



Cisco IP Transfer Point (ITP)

For Cisco IOS Release 12.4(15)SW9
November 2014

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Turn the television or radio antenna until the interference stops.
- Move the equipment to one side or the other of the television or radio.
- Move the equipment farther away from the television or radio.
- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

IP Transfer Point

© 2012-2014 Cisco Systems, Inc. All rights reserved.



CONTENTS

About this Book iii-xv

- Audience xv
- Documentation Organization xvi
- Documentation Conventions xviii
- Obtaining Documentation, Obtaining Support, and Security Guidelines xix

Using Cisco IOS Software iv-xxi

- Understanding Command Modes iv-xxi
- Getting Help iv-xxii
 - Example: How to Find Command Options iv-xxiii
- Using the no and default Forms of Commands iv-xxv
- Filtering Output from the show and more Commands iv-xxvi
- Finding Additional Feature Support Information iv-xxvi

Overview of ITP 1-1

- SS7oIP Technology Overview 1-1
 - Introduction to SS7oIP 1-1
 - Stream Control Transmission Protocol (RFC2960) 1-1
 - Sigtran M2PA - SS7 MTP2-User Peer-to-Peer Adaptation Layer 1-2
 - Sigtran M3UA - SS7 MTP3-User Adaptation Layer 1-2
 - Sigtran SUA - SS7 SCCP-User Adaptation Layer 1-3
- Benefits 1-4

Planning to Configure ITP 2-5

- Supported Platforms 2-5
- Supported Standards, MIBs, and RFCs 2-5
 - Standards 2-5
 - MIBs 2-5

Performing IOS ITP Software Upgrade 3-9

- Performing ITP IOS Software Upgrade 3-9
- Performing ITP Group Software Upgrade 3-10

Configuring ITP Basic Functionality 4-13

- Contents 4-14
- Enabling Secure Shell 4-14

Specifying the SS7 Variant, National Option, and Network Indicator	4-15
Specifying the Point Code	4-18
Specifying the Point Code Representation	4-18
Specifying the Primary Local Point Code	4-19
Specifying a Secondary Point Code	4-19
Specifying the Capability Point Code	4-19
Specifying the Interface and Encapsulation	4-20
Clocking on the SS7 Port Adapter and SS7 Q.703 High Speed Port Adapter	4-21
Configuring a Serial Interface and SS7 High-Speed MTP2 Encapsulation (Q.703 Annex A) on the SS7 Q.703 High Speed Port Adapter	4-21
Configuring a Serial Interface and MTP2 Encapsulation on the SS7 Port Adapter	4-23
Configuring SS7 over ATM High Speed Links (HSL)	4-25
Configuring BITS Network Clocking	4-27
Configuring SS7 ATM High Speed Links with BITS Network Clocking	4-29
Configuring Local Peers	4-32
Configuring Linksets	4-32
Configuring Circular Route Direction (CRD)	4-34
Configuring CRD for the ANSI Variant	4-34
Configuring CRD for the ITU and ITU-like Variants	4-35
Configuring Multiple Linksets to Adjacent Nodes	4-37
Specifying the Cisco ITP Route Table	4-38
Specifying the Default Route Table	4-39
Loading the Route Table Contents	4-39
Adding Routes to the Route Table	4-39
Saving the Route Table	4-40
Assigning Links to Linksets	4-40
Traditional SS7 Links	4-40
High-Speed Signaling Links	4-41
SS7 Over IP Links (Peers)	4-41
Shutting Down and Restarting Linksets and Links	4-42
Configuration Example of ITP Basic Functionality	4-43

Probeless Monitoring 5-53

Contents	5-53
Information About Probeless Monitoring	5-54
How to Configure Probeless Monitoring	5-54
Configuring Global Probeless Monitoring	5-55
Configuring Hold Queue and Congestion Timer	5-56
Configuring a DCS Node	5-56
Restrictions	5-57

Configuring a DCS Group	5-59
Restrictions	5-59
Configuring Probeless Monitoring for a Specific Linkset	5-60
Configuring Probeless Monitoring for a Specific AS	5-61
Verifying the Probeless Monitoring Configuration	5-62
Configuration Example for Probeless Monitoring	5-62
Multiple Instances and Instance Translation	6-67
Contents	6-67
Information About Multiple Instances and Instance Translation	6-67
Understanding Virtual Linksets	6-68
How to Configure Multiple Instances	6-69
How to Configure Instance Translation	6-69
Configuring Point Code Conversion	6-69
Configuring Global Title Conversion	6-70
Configuring Instance Conversion After Global Title Translation	6-73
Verifying the Multiple Instances Configuration	6-74
Configuration Example for Multiple Instance	6-74
Configuration Examples for Instance Translation	6-75
ITP Group	7-79
Contents	7-79
Prerequisites for ITP Group Operation	7-80
Restrictions for ITP Group Operation	7-80
Information about ITP Group Operation	7-80
How to Configure the ITP Group Feature	7-81
Configuring the Inter-Device Redundancy Parameters	7-82
What to Do Next	7-83
Enabling the ITP Group Feature	7-83
Prerequisites	7-84
What to Do Next	7-85
Configuring the Group SCTP Parameters	7-85
Commands for Configuring SCTP Parameters	7-85
What to Do Next	7-86
Defining Linksets that Span Group Peers	7-86
Prerequisites	7-86
Configuration Example for ITP Group	7-88
Performing ITP Group Software Upgrade	7-90

Global Title Translation	8-91
Contents	8-91
Overview of GTT Components	8-92
GTT Selectors	8-93
GTT Global Title Address Entries	8-93
GTT Application Groups	8-94
GTT Mated Application Entries	8-95
Storing and Loading GTT Configuration Data	8-96
Loading a GTT Table from a Remote File Server or Flash (No existing GTT Data)	8-96
Loading a GTT Table from a Remote File Server or Flash (Existing GTT Data)	8-97
Bulk Loading/Replacing GTT Database	8-98
Syntax and Format Rules for Creating a GTT Database Download File	8-98
Command Identifiers in a GTT Database Download File	8-98
Parameter Values in GTT Database Download Files	8-99
Examples of Entries in a GTT Database Download File	8-100
Modifying and Verifying the GTT Selector	8-104
Configuring GTT: 6 Scenarios	8-105
Configuring Intermediate GTT To Route MSUs to a Single Point Code	8-105
Configuring Intermediate GTT To Load Balance MSUs Across Two Or More Point Codes	8-107
Configuring Final GTT To Route MSUs to a Solitary Point Code	8-110
Configuring Final GTT To Route MSUs to a Primary and Backup Point Code and SSN (Dominant Mode)	8-113
Configuring Final GTT To Load Balance MSUs Across a Group of Point Codes and Subsystems	8-116
Configuring Final GTT to an SUA AS with a Backup Point Code (Dominant Mode)	8-118
Configuring the GTT Application Group	8-119
Configuring Global Title Address Conversion	8-121
Verifying Global Title Translations	8-123
GTT Measurements	8-123
SCCP Accounting	8-123
Subsystem Status	8-124
Logging GTT Errors with the ITP Logging Facility	8-124
GTT Error Log	8-125
GTT Configuration Examples	8-126
ITP GTT Configuration for ITPA Example	8-128
ITP GTT Configuration for ITPB Example	8-130
ITP GTT Configuration for ITPC Example	8-133
ITP GTT Configuration for ITPD Example	8-135

M3UA and SUA SS7 Over IP Signaling Gateways 9-137

Contents 9-137

Information About M3UA and SUA ITP Signaling Gateways 9-138

M3UA 9-138

SUA 9-139

SGMP 9-140

C-Link Backup Routing of M3UA/SUA Traffic 9-141

Application Server (AS) 9-142

Application Server Process (ASP) 9-142

Point Code Assignment and Management 9-142

AS Load-sharing Support 9-143

AS Fail-over support 9-144

SCCP Traffic Processing for M3UA 9-144

ITP SG Quality Of Service (QoS) 9-145

How to Configure Signaling Gateways 9-145

Performing Basic ITP Configuration 9-145

Enabling and Disabling M3UA and SUA 9-146

Enabling M3UA 9-146

Disabling M3UA 9-146

Enabling SUA 9-146

Disabling SUA 9-147

Enabling SGMP 9-147

Enabling SGMP Offloading 9-149

Examples 9-150

Defining an Application Server Process (ASP) 9-150

Defining Application Servers (AS) and Routing Keys 9-152

Enabling M3UA Extended User Part Unavailable (UPU) Operation 9-153

ITP Signaling Gateway Configuration Examples 9-153

M3UA Configuration Example 9-154

SUA Configuration Example 9-155

ITP Signaling Gateway: ASPs with Unique Point Codes Configuration Example 9-155

ITP SG Mated-SG Configuration Example 9-156

ITP SG GTT Configuration Example 9-158

ITP SG QoS Configuration Examples 9-159

Gateway Screening (GWS) 10-163

Contents 10-163

Information About GWS 10-164

GWS Tables 10-164

GWS Table Matching Order for Incoming Packets	10-175
How GWS Works with Access Lists	10-175
How to Configure GWS	10-178
Defining GWS Access Lists	10-179
Defining GWS Action Sets	10-180
Defining GWS Tables	10-182
Defining Entries in GWS Tables	10-184
What to Do Next	10-186
Defining Gateway Linkset Tables	10-187
What to Do Next	10-189
Defining an AS Table for GWS	10-189
What to Do Next	10-191
Saving a GWS Table or a GWS Configuration to a Remote or Local File	10-192
Loading a GWS Table and GWS Configuration from a Remote or Local File	10-192
Replacing a Running GWS Configuration or Existing GWS Table with a Remote or Local File	10-194
Validating and Auditing the Consistency of the GWS Files in the Line Card and Main Processor	10-194
Monitoring GWS	10-195
Message Logging	10-195
Verifying GWS Configuration	10-197
Configuration Examples for GWS	10-198
GWS Scenario: Linkset with Allowed DPC	10-199
GWS Scenario: XUA AS with Allowed DPC	10-200
GWS Scenario with CgPA, CdPA	10-200
Additional References	10-202
Standards	10-202
MLR Routing and Screening	11-203
Contents	11-203
Information About MLR Routing and Screening	11-204
Trigger Search Order	11-204
Destination Selection	11-205
How to Configure MLR-Based Routing	11-205
Define MLR Global Options	11-206
Define the MLR Group	11-207
Defining the MLR Modify-Profile	11-211
Creating and Managing Address Tables	11-214
Creating and Loading an Address Table File Using the CLI	11-215
Creating and Loading a Stored Address Table File	11-218

Replacing an Address Table File	11-219
Examples	11-220
Saving an MLR Configuration to a File	11-221
Loading an MLR Configuration from a File	11-221
Replacing a Running MLR Configuration with a File	11-222
Validating and Auditing the Consistency of the MLR Files in the Line Card and Main Processor	11-223
Define One or More MLR Rulesets	11-224
Define the MLR Triggers	11-240
Define the MLR Triggers with GWS	11-240
Information About MLR Triggers with GWS	11-240
Define MLR Triggers with Proprietary Method	11-242
How to Configure MLR-Based Screening	11-244
Blocking Based on SCCP cdPa and cgPa	11-244
Define GTT Entries for cdPa and cgPa digits to Screen	11-244
Define MLR table and Blocking Based on SCCP cdPa or cgPa	11-246
Define MLR Table and Blocking on Combination of SCCP cdPa and cgPa	11-246
Blocking Based on cgPa, cdPa, and SMS MAP Operation Code	11-247
Blocking Based on cgPa, cdPa and SMS MO/MT Routing Parameters	11-247
Verifying and Monitoring MLR Routing	11-247
Configuration Examples of MLR	11-249
Configuration Example of Address Modification, page 257	
Configuration Example for MLR: ITP Receives All SMS-MO Traffic in GT-Routed Network	11-249
Configuration Example for MLR: Legacy SMSC Retains Point Code in PC-Routed Network	11-252
Configuration Example for MLR: MLR Distribution to MTP3-Based SMSCs	11-254
Examples of Configuring Routing Based on Operation Types	11-256
Example of Routing with B-Address Binding	11-257
Configuration Example of Address Modification	11-257
How to Configure Packet Address Modification (PAM)	11-259
PAM CdPA and CgPA Modifications	11-259
PAM in GWS	11-260
PAM in MLR	11-260
PAM Modify Failure	11-260
PAM Limitations	11-260
Configuring PAM	11-261
Configuration Examples of PAM	11-264
IP Security	12-265
Contents	12-265
Information About IPSec	12-265

How to Configure IPSec	12-266
Create an IPSEC Tunnel	12-266
What to Do Next	12-268
Configure a CS7 Peer Link over the Tunnel	12-269
Configuration Examples for IPSec	12-269

MAP Proxy: GSM Authentication Service MMSC Gateway Service

Contents	13-271
Information About MAP Proxy	13-272
GSM MAP Authentication	13-272
Multimedia Message Service Center Gateway	13-273
PGW SIP MAP Gateway	13-273
How to Configure MAP Proxy	13-274
Performing Basic ITP Configuration	13-274
Implementing a GSM MAP Authentication Service	13-274
Implementing a PGW SIP MAP Gateway	13-277
Example	13-281
Provisioning MAP Proxy Parameters for GSM MAP Authentication Service	13-281
Example	13-282
Implementing an MMSC Gateway Service	13-282
Provisioning MAP Proxy Parameters for An MMSC Gateway Service	13-284
Example	13-285
Enabling and Disabling MAPUA	13-285

ITP QoS

Contents	14-287
Information About ITP QoS	14-287
ITP QoS Components	14-288
ITP QoS Functionality	14-288
How to Configure ITP QoS	14-289
Specifying Packet Classification	14-290
Verifying ITP QoS	14-297
QOS Configuration Example	14-299

Load Sharing

Contents	15-315
Information About SCCP Load Sharing	15-316
Scenarios for SCCP Load Sharing	15-316

Configuring SCCP Load Sharing	15-318
Configuring GTT Application Group Overflow Load Sharing for SCCP Class 0	15-319
Restrictions and Considerations	15-319
Example	15-321
Verifying and Monitoring	15-321
Configuring the MTP Overflow Load Sharing	15-323
Configuring GTT Application Group Load Balancing for SCCP Traffic	15-326
Example	15-327
Configuring GTT Application Group Load Balancing for SCCP Traffic at the Global Level	15-327
Example	15-328
Configuring GTT Application Groups with the WRR Algorithm for Processing SCCP Class 1 Traffic	15-329
Example	15-329
Configuring SCCP Class 0 Load Sharing to Ignore Class and Sequencing	15-330
Example	15-330
Configuring SCCP Class 1 Load Sharing to Ignore Class and Sequencing	15-330
Example	15-331
Configuring MTP3 Enhanced Load Sharing For ITU	15-331
Verifying and Monitoring MTP3 Load Sharing	15-333
Inter-Carrier Accounting	16-335
Contents	16-335
Information About Inter-Carrier Accounting	16-335
MTP3 Accounting	16-336
SCCP Accounting	16-336
SMS Traffic Accounting	16-337
Service Data Records	16-337
Data Collection and Backup Options	16-338
Configuring Inter-Carrier Accounting	16-338
Configuring an MTP3 Inter-Carrier Accounting Billing Account	16-338
Inter-Carrier Accounting Billing Account Configured for MTP3 Example	16-341
Inter-Carrier Accounting Billing Account Configured for Both MTP3 and SCCP Example	16-341
Configuring an SCCP Inter-Carrier Accounting Billing Account	16-341
Example	16-344
Configuring Inter-Carrier Accounting Data Collection	16-345
Example	16-345
Saving and Loading Inter-Carrier Accounting Configurations	16-346
Example	16-346
Verifying and Monitoring	16-346

Summary Routing and ANSI Cluster Routing 17-349

Contents 17-349

Information About Summary Routing and ANSI Cluster Routing 17-350

How Point Codes Are Used in Summary Routing 17-350

Summary Routes and the Routing Table 17-352

How to Configure Summary Routes 17-353

How to Configure ANSI Cluster Routing 17-355

Verifying, Monitoring, and Tuning the ITP 18-357

Verifying ITP 18-357

Monitoring ITP 18-369

Configuring ITP for Event Logging to an External Server 18-369

Enabling Simple Network Management Protocol 18-370

Monitoring the Cisco ITP 18-372

Monitoring CPU/Memory 18-372

Monitoring Linksets and Links 18-373

Monitoring MTP2 Links/Interfaces 18-375

Monitoring M2PA Links/Interfaces 18-380

Monitoring GTT Measurements 18-383

Monitoring M3UA or SUA 18-384

Monitoring AS, ASP, Mated-SG 18-385

Monitoring Routes 18-391

Monitoring Gateway Screening Violations 18-392

Monitoring System Messages 18-392

Monitoring Accounting 18-393

Summary of Commands to Monitor Cisco ITP 18-393

Tuning ITP 18-394

Tuning HSL Parameters 18-394

Create a Profile to Support HSL 18-394

Specify HSL Parameters on a Link 18-397

Tuning MTP3 Timers 18-397

Tuning MTP2 Parameters 18-398

Understanding the MTP2 Parameters 18-398

Specifying MTP2 Parameters in a CS7 Profile 18-399

Specifying MTP2 Parameters Individually 18-401

Tuning SCTP Parameters 18-402

How SCTP Parameters Work 18-402

Tuning SCTP Parameters for M2PA 18-404

Tuning SCTP Parameters for M3UA and SUA 18-407

Tuning SCTP Parameters for an ASP	18-408
Tuning AS Options	18-408
Tuning SCTP Parameters for a Mated SG	18-409
Tuning SCTP Parameters for Satellite Channels	18-410
ITP Command Set: A - D	19-415
ITP Command Set: E - R	20-754
ITP Command Set: S - Z	21-1062
ITP Debug Commands	22-1387
ITP System Messages	23-1411
How This Manual Is Organized	23-1411
How to Read System Messages	23-1412
CS7ADDRTBL Messages	23-1412
CS7CDR Messages	23-1413
CS7CHKPT Messages	23-1414
CS7GROUP Messages	23-1415
CS7HSL Messages	23-1417
CS7M2PA Messages	23-1418
CS7MLR Messages	23-1420
CS7MTP2 Messages	23-1421
CS7MTP3 Messages	23-1424
CS7NSO Messages	23-1442
CS7PING Messages	23-1444
CS7RF Messages	23-1446
CS7ROUTE Messages	23-1447
CS7SCCP Messages	23-1450
CS7SMS Messages	23-1458
CS7TCAP Messages	23-1459
CS7XUA Messages	23-1460
DCS7 Messages	23-1465



About this Book

This preface describes the audience, organization, and conventions of *IP Transfer Point*. It also lists documentation revision history, sources for obtaining related documentation, technical assistance, and additional publications and information from Cisco Systems.



Note

This publication does not contain the instructions to install router. For information on installing the router, see the installation guide that came with your router.

This preface contains the following sections:

- [Audience, page xv](#)
- [Documentation Organization, page xvi](#)
- [Documentation Conventions, page xviii](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page xix](#)

Audience

This publication is intended for users who are responsible for configuring and maintaining the Cisco IP Transfer Point software. It is intended for users who are responsible for migrating Signaling System 7 (SS7) to the mobile wireless SS7-over-IP (SS7oIP) environment but who may not be familiar with the configuration and maintenance tasks, the relationship among tasks, or the Cisco IOS software commands necessary to perform particular tasks. This publication is also intended for those users experienced with the Cisco ITP software who need to know about new features, new configuration options, and new software characteristics in the current software release.

Documentation Organization

This publication is organized as follows:

Chapter	Description
About This Book	This preface describes the audience, organization, and conventions of <i>IP Transfer Point</i> . It also lists documentation revision history, sources for obtaining related documentation, technical assistance, and additional publications and information from Cisco Systems.
Using Cisco IOS Software	This chapter provides helpful tips for understanding and configuring the Cisco IOS software using the command-line interface (CLI). The chapter discusses command modes, show commands, and using the CLI to get command syntax help.
Overview of ITP	Provides an overview of the ITP, SS7, and SS7oIP
Planning to Configure ITP	Describes the prerequisites to installing the Cisco ITP, including supported hardware and software. The chapter includes references to related documentation.
Performing ITP Software Upgrade	Describes the ITP software upgrade procedure
Configuring ITP Basic Functionality	Describes the tasks and commands to configure basic Cisco ITP functionality.
Multiple Instances and Instance Translation	Describes the tasks and commands to configure the Multiple Instances feature to connect the ITP to different networks with specific variant and network indicators. Describes the tasks and commands to configure Instance Translation, which enables the conversion and transfer of MSUs between different instances.
ITP Group	Describes the tasks and commands to configure two ITPs to appear as a single network entity. The two ITPs share the same local point codes and support SS7 linksets that span both ITPs. This feature provides inter-device redundancy, high availability, and reduced point code usage.
Global Title Translation	Describes the tasks and commands to configure Global Title Translation (GTT), the process by which the SCCP translates a global title into the point code and subsystem number of the destination SSP where the higher-layer protocol processing occurs.
M3UA and SUA Over IP Signaling Gateways	Describes the tasks and commands to configure the Cisco ITP Signaling Gateway (ITP SG) feature which provides open-standards-based SS7 over IP solutions through the implementation of SIGTRAN MTP3-User Adaptation (M3UA) and SCCP User Adaptation (SUA) protocols.
Gateway Screening	Describes the tasks and commands to configure the ITP Gateway Screening feature (GWS) which prevents unauthorized use of the ITP and controls the flow of messages into or through the ITP.

Chapter	Description
Multi-Layer SMS Routing and Screening	Describes the tasks and commands to configure the ITP Multi-Layer Routing (MLR) feature which implements the routing of SMS messages based on information found in the Transaction Capability Application Part (TCAP), Mobile Application Part (MAP), and SMS layers.
ANSI-41 SMS Notification	Describes the tasks and commands to perform a broadcast of incoming ANSI-41 SMS Notifications to a bank of short message Messaging Centers (MC) and to provide a reply to the HLR after receiving the first positive acknowledgement message from any of the MCs in the distribution.
IP Security	Describes the tasks and commands to configure IP Security (IPSec).
MAP Proxy: GSM Authentication Service; MMSC Gateway Service	Describes the tasks and commands to enable the ITP to deliver Mobile Application Part (MAP) functionality.
MTP3 Offload	Describes the tasks and commands to enable message forwarding and Global Title Translation (GTT) to be performed on the FlexWANs.
Non-Stop Operation	Describes the tasks and commands to configure the Non-Stop Operation feature which enables the ITP to continue operation in the event of a Supervisor 720 failure.
ITP QoS	Describes the tasks and commands to configure the ITP QoS feature which provides the framework that allows end-to-end Quality of Service (QoS) for SS7 packet flow through SS7 over IP (SS7oIP) networks.
SCCP Load Sharing	Describes the configuration options for SCCP load sharing as well as address guidelines for when to use the different methods provided.
Summary Routing and ANSI Cluster Routing	Describes the tasks and commands to configure the Summary Routing feature. This feature allows routing of MSUs to groups of DPCs by specifying one or more routes to a summary destination in the route table rather than individual route table entries for each destination.
Verifying, Monitoring, and Tuning the ITP	Describes how to verify proper configuration of the RPR+ feature and the ITP, monitor status and traffic, and tune the ITP.
ITP Command Set: A - D	Command Reference describes command syntax, usage guidelines, etc., for each command.
ITP Command Set: E - R	Command Reference describes command syntax, usage guidelines, etc., for each command.
ITP Command Set: S - Z	Command Reference describes command syntax, usage guidelines, etc., for each command.
ITP Debug Commands	Debug command reference.
ITP System Messages	Describes system messages and provides recommended actions.

Documentation Conventions

This publication uses the following conventions:

Convention	Description
^ or Ctrl	The ^ and Ctrl symbols represent the Control key. For example, the key combination ^D or Ctrl-D means hold down the Control key while you press the D key. Keys are indicated in capital letters but are not case sensitive.
<i>string</i>	A string is a nonquoted set of characters shown in italics. For example, when setting an SNMP community string to <i>public</i> , do not use quotation marks around the string or the string will include the quotation marks.

Command syntax descriptions use the following conventions:

Convention	Description
bold	Bold text indicates commands and keywords that you enter literally as shown.
<i>italics</i>	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional element (keyword or argument).
	A vertical line indicates a choice within an optional or required set of keywords or arguments.
[x y]	Square brackets enclosing keywords or arguments separated by a vertical line indicate an optional choice.
{x y}	Braces enclosing keywords or arguments separated by a vertical line indicate a required choice.

Nested sets of square brackets or braces indicate optional or required choices within optional or required elements. For example:

Convention	Description
[x {y z}]	Braces and a vertical line within square brackets indicate a required choice within an optional element.

Examples use the following conventions:

Convention	Description
screen	Examples of information displayed on the screen are set in Courier font.
bold screen	Examples of text that you must enter are set in Courier bold font.
< >	Angle brackets enclose text that is not printed to the screen, such as passwords, and are used in contexts in which the italic document convention is not available, such as ASCII text.
!	An exclamation point at the beginning of a line indicates a comment line. (Exclamation points are also displayed by the Cisco IOS software for certain processes.)
[]	Square brackets enclose default responses to system prompts.

The following conventions are used to attract the attention of the reader:

Caution

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Note

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>



Using Cisco IOS Software

This chapter provides helpful tips for understanding and configuring the Cisco IOS software on the ITP using the command-line interface (CLI). It contains the following sections:

- [Understanding Command Modes, page xxi](#)
- [Getting Help, page xxii](#)
- [Using the no and default Forms of Commands, page xxv](#)
- [Filtering Output from the show and more Commands, page xxvi](#)
- [Finding Additional Feature Support Information, page xxvi](#)

Understanding Command Modes

You use the CLI to configure the Cisco IOS software that runs on the ITP. Because the CLI is divided into many different modes, the commands available to you at any given time depend on the mode that you are currently in. Entering a question mark (?) at the CLI prompt allows you to obtain a list of commands available for each command mode.

When you log in to the CLI, you are in user EXEC mode. User EXEC mode contains only a limited subset of commands. To have access to all commands, you must enter privileged EXEC mode, normally by using a password. From privileged EXEC mode you can issue any EXEC command—user or privileged mode—or you can enter global configuration mode. Most EXEC commands are one-time commands. For example, **show** commands show important status information, and **clear** commands clear counters or interfaces. The EXEC commands are not saved when the software reboots.

Configuration modes allow you to make changes to the running configuration. If you later save the running configuration to the startup configuration, these changed commands are stored when the software is rebooted. To enter specific configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and a variety of other modes, such as protocol-specific modes.

ROM monitor mode is a separate mode used when the Cisco IOS software cannot load properly. If a valid software image is not found when the software boots or if the configuration file is corrupted at startup, the software might enter ROM monitor mode.

Table 1 describes how to access and exit the most common command modes of the Cisco IOS software. It also shows examples of the prompts displayed for each mode. As you configure the Cisco IOS software for your ITP, you will access many other command modes, depending on the ITP features that you are configuring.

Table 1 **Accessing and Exiting Command Modes**

Command Mode	Access Method	Prompt	Exit Method
User EXEC	Log in.	Router>	Use the logout command.
Privileged EXEC	From user EXEC mode, use the enable command.	Router#	To return to user EXEC mode, use the disable command.
Global configuration	From privileged EXEC mode, use the configure terminal command.	Router(config)#	To return to privileged EXEC mode from global configuration mode, use the exit or end command.
Interface configuration	From global configuration mode, specify an interface using an interface command.	Router(config-if)#	To return to global configuration mode, use the exit command. To return to privileged EXEC mode, use the end command.
ROM monitor	From privileged EXEC mode, use the reload command. Press the Break key during the first 60 seconds while the system is booting.	>	To exit ROM monitor mode, use the continue command.

Getting Help

Entering a question mark (?) at the CLI prompt displays a list of commands available for each command mode. You can also get a list of keywords and arguments associated with any command by using the context-sensitive help feature.

To get help specific to a command mode, a command, a keyword, or an argument, use one of the following commands:

Command	Purpose
help	Provides a brief description of the help system in any command mode.
<i>abbreviated-command-entry?</i>	Provides a list of commands that begin with a particular character string. (No space between command and question mark.)
<i>abbreviated-command-entry<Tab></i>	Completes a partial command name.
?	Lists all commands available for a particular command mode.
<i>command ?</i>	Lists the keywords or arguments that you must enter next on the command line. (Space between command and question mark.)

Example: How to Find Command Options

This section provides an example of how to display syntax for a command. The syntax can consist of optional or required keywords and arguments. To display keywords and arguments for a command, enter a question mark (?) at the configuration prompt or after entering part of a command followed by a space. The Cisco IOS software displays a list and brief description of available keywords and arguments. For example, if you were in global configuration mode and wanted to see all the keywords or arguments for the **arap** command, you would type **arap ?**.

The <cr> symbol in command help output stands for “carriage return.” On older keyboards, the carriage return key is the Return key. On most modern keyboards, the carriage return key is the Enter key. The <cr> symbol at the end of command help output indicates that you have the option to press **Enter** to complete the command and that the arguments and keywords in the list preceding the <cr> symbol are optional. The <cr> symbol by itself indicates that no more arguments or keywords are available and that you must press **Enter** to complete the command.

Table 2 shows examples of how you can use the question mark (?) to assist you in entering commands. The table steps you through configuring an IP address on a serial interface.

Table 2 *How to Find Command Options*

Command	Comment
Router> enable Password: <password> Router#	Enter the enable command and password to access privileged EXEC commands. You are in privileged EXEC mode when the prompt changes to Router#.
Router# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#	Enter the configure terminal privileged EXEC command to enter global configuration mode. You are in global configuration mode when the prompt changes to Router(config)#.
Router(config)# interface serial ? <0-6> Serial interface number Router(config)# interface serial 4 ? / Router(config)# interface serial 4/ ? <0-3> Serial interface number Router(config)# interface serial 4/0 ? <cr> Router(config)# interface serial 4/0 Router(config-if)#	Enter interface configuration mode by specifying the serial interface that you want to configure using the interface serial global configuration command. Enter ? to display what you must enter next on the command line. In this example, you must enter the serial interface slot number and port number, separated by a forward slash. When the <cr> symbol is displayed, you can press Enter to complete the command. You are in interface configuration mode when the prompt changes to Router(config-if)#.

Table 2 **How to Find Command Options (continued)**

Command	Comment
Router(config-if)# ? Interface configuration commands: . . . ip Interface Internet Protocol config commands keepalive Enable keepalive lan-name LAN Name command llc2 LLC2 Interface Subcommands load-interval Specify interval for load calculation for an interface locaddr-priority Assign a priority group logging Configure logging for interface loopback Configure internal loopback on an interface mac-address Manually set interface MAC address mls mls router sub/interface commands mpoa MPOA interface configuration commands mtu Set the interface Maximum Transmission Unit (MTU) netbios Use a defined NETBIOS access list or enable name-caching no Negate a command or set its defaults nrzi-encoding Enable use of NRZI encoding ntp Configure NTP . . . Router(config-if)#	Enter ? to display a list of all the interface configuration commands available for the serial interface. This example shows only some of the available interface configuration commands.
Router(config-if)# ip ? Interface IP configuration subcommands: access-group Specify access control for packets accounting Enable IP accounting on this interface address Set the IP address of an interface authentication authentication subcommands bandwidth-percent Set EIGRP bandwidth limit broadcast-address Set the broadcast address of an interface cgmp Enable/disable CGMP directed-broadcast Enable forwarding of directed broadcasts dvmrp DVMRP interface commands hello-interval Configures IP-EIGRP hello interval helper-address Specify a destination address for UDP broadcasts hold-time Configures IP-EIGRP hold time . . . Router(config-if)# ip	Enter the command that you want to configure for the interface. This example uses the ip command. Enter ? to display what you must enter next on the command line. This example shows only some of the available interface IP configuration commands.

Table 2 *How to Find Command Options (continued)*

Command	Comment
<pre>Router(config-if)# ip address ? A.B.C.D IP address negotiated IP Address negotiated over PPP Router(config-if)# ip address</pre>	Enter the command that you want to configure for the interface. This example uses the ip address command. Enter ? to display what you must enter next on the command line. In this example, you must enter an IP address or the negotiated keyword. A carriage return (<cr>) is not displayed; therefore, you must enter additional keywords or arguments to complete the command.
<pre>Router(config-if)# ip address 172.16.0.1 ? A.B.C.D IP subnet mask Router(config-if)# ip address 172.16.0.1</pre>	Enter the keyword or argument that you want to use. This example uses the 172.16.0.1 IP address. Enter ? to display what you must enter next on the command line. In this example, you must enter an IP subnet mask. A <cr> is not displayed; therefore, you must enter additional keywords or arguments to complete the command.
<pre>Router(config-if)# ip address 172.16.0.1 255.255.255.0 ? secondary Make this IP address a secondary address <cr> Router(config-if)# ip address 172.16.0.1 255.255.255.0</pre>	Enter the IP subnet mask. This example uses the 255.255.255.0 IP subnet mask. Enter ? to display what you must enter next on the command line. In this example, you can enter the secondary keyword, or you can press Enter. A <cr> is displayed; you can press Enter to complete the command, or you can enter another keyword.
<pre>Router(config-if)# ip address 172.16.0.1 255.255.255.0 Router(config-if)#</pre>	In this example, Enter is pressed to complete the command.

Using the no and default Forms of Commands

Almost every configuration command has a **no** form. In general, use the **no** form to disable a function. Use the command without the **no** keyword to reenable a disabled function or to enable a function that is disabled by default. For example, IP routing is enabled by default. To disable IP routing, use the **no ip routing** command; to reenable IP routing, use the **ip routing** command. The Cisco IOS software command reference publications provide the complete syntax for the configuration commands and describe what the **no** form of a command does.

Configuration commands can also have a **default** form, which returns the command settings to the default values. Most commands are disabled by default, so in such cases using the **default** form has the same result as using the **no** form of the command. However, some commands are enabled by default and

have variables set to certain default values. In these cases, the **default** form of the command enables the command and sets the variables to their default values. The Cisco IOS software command reference publications describe the effect of the **default** form of a command if the command functions differently than the **no** form.

Filtering Output from the show and more Commands

You can search and filter the output of **show** and **more** commands. This functionality is useful if you need to sort through large amounts of output or if you want to exclude output that you need not see.

To use this functionality, enter a **show** or **more** command followed by the “pipe” character (`|`); one of the keywords **begin**, **include**, or **exclude**; and a regular expression on which you want to search or filter (the expression is case-sensitive):

command | { **begin** | **include** | **exclude** } *regular-expression*

The output matches certain lines of information in the configuration file. The following example illustrates how to use output modifiers with the **show interface** command when you want the output to include only lines in which the expression “protocol” appears:

```
Router# show interface | include protocol

FastEthernet0/0 is up, line protocol is up
Serial4/0 is up, line protocol is up
Serial4/1 is up, line protocol is up
Serial4/2 is administratively down, line protocol is down
Serial4/3 is administratively down, line protocol is down
```

Finding Additional Feature Support Information

If you want to use a specific Cisco IOS software feature, you will need to determine in which Cisco IOS software images that feature is supported. Feature support in Cisco IOS software images is dependent on three main factors: the software version (called the “Release”), the hardware model (the “Platform” or “Series”), and the “Feature Set” (collection of specific features designed for a certain network environment). Although the Cisco IOS software documentation set documents feature support information for Release 12.4 as a whole, it does not generally provide specific hardware and feature set information.

To determine the correct combination of Release (software version), Platform (hardware version), and Feature Set needed to run a particular feature (or any combination of features), use Feature Navigator.

Feature Navigator is a web-based tool available on Cisco.com at <http://www.cisco.com/go/fn>. Feature Navigator is available only for registered users of Cisco.com. If you do not have an account or have forgotten your username or password, click Cancel at the login dialog box and follow the instructions that appear.

Software features may also have additional limitations or restrictions. For example, a minimum amount of system memory may be required. Or there may be known issues for features on certain platforms that have not yet been resolved (called “Caveats”). For the latest information about these limitations, see the release notes for the appropriate Cisco IOS software release. Release notes provide detailed installation instructions, new feature descriptions, system requirements, limitations and restrictions, caveats, and troubleshooting information for a particular software release.



Overview of ITP

Cisco IP Transfer Point (ITP) is a hardware and software SS7-over-IP (SS7oIP) solution. ITP provides a highly reliable, cost effective medium for migrating Signaling System 7 (SS7), the telecommunications network signaling technology, to the mobile wireless IP environment.

By leveraging its leadership in high-end switches and routers, Cisco has created a carrier class router with a transparent SS7oIP convergence solution. Cisco ITP is managed identically to other Cisco routers and leverages the Cisco skill sets already existing within the service provider, including provisioning, management, and tools training.

Short Message Peer-to-Peer (SMPP) protocol is not supported. Some DSMR functionality is also not supported. It is recommended that commands pertaining to these features are not configured.

This chapter introduces the Signaling System 7 (SS7) protocol and Cisco ITP technology. This chapter includes the following sections:

- [SS7oIP Technology Overview, page 1](#)
- [Benefits, page 4](#)

SS7oIP Technology Overview

Introduction to SS7oIP

The IETF Signaling Transport (Sigtran) Working Group is a multi-vendor organization that is developing and standardizing protocols to transport SS7 over IP. The primary purpose of this working group is to address the transport of packet-based mobile/PSTN signaling over IP networks, while also accounting for functional and performance requirements of mobile/PSTN signaling. For internetworking with a mobile/PSTN network, IP networks need to transport signaling such as Q.931 or SS7 ISDN User Part (ISUP) messages. To view the IETF Sigtran standards, refer to the following URL:
<http://www.ietf.org/html.charters/sigtran-charter.html>.

Stream Control Transmission Protocol (RFC2960)

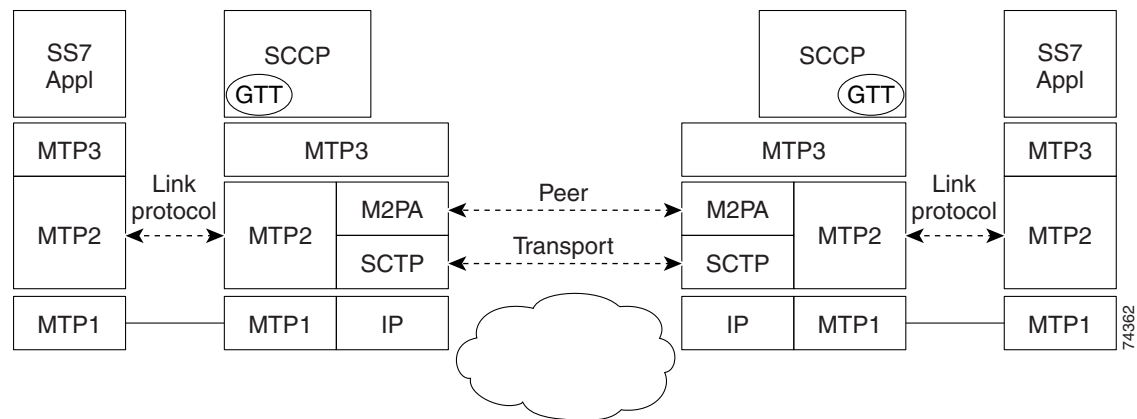
The Stream Control Transmission Protocol (SCTP) is a reliable transport protocol that operates on top of an unreliable connectionless packet service such as IP. It offers acknowledged error-free, non-duplicated transfer of MSUs. SCTP uses checksums and sequence numbers to detect data

corruption, loss, or duplication, and corrects loss or corruption of data with a selective retransmission mechanism. SCTP provides the function and measurements in an architecturally identical manner to MTP2. To view the SCTP standards, refer to the following URL: <http://www.ietf.org/rfc/rfc2960.txt>.

Sigtran M2PA - SS7 MTP2-User Peer-to-Peer Adaptation Layer

M2PA is designed for peer-to-peer signaling gateway (SG) communications. The analogy in legacy networks is STP-to-STP communication. Figure 1 provides a protocol architecture diagram.

Figure 1 M2PA Protocol Architecture

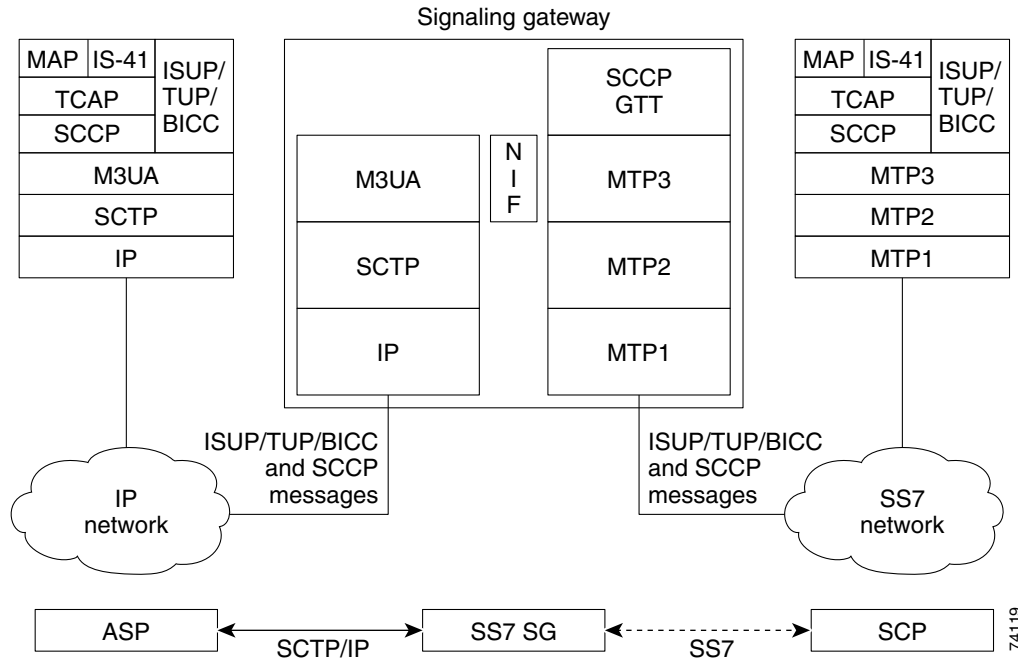


M2PA offers a protocol high availability similar to an STP. The MTP3 implementation layer in an M2PA SG is unaware of whether a link is time-division multiplexing (TDM) or IP and run equally well over either. This preserves congestion, Layer 2 failure detection, changeover, change-back, load balancing via SLS, screening, and other MTP3 features.

Sigtran M3UA - SS7 MTP3-User Adaptation Layer

Message Transfer Part, Level 3, User Adaptation Layer protocol (M3UA) describes a transport mechanism for delivering SS7 Message Transfer Part, Level 3 (MTP3) User Part messages as well as certain MTP network management events over Stream Control Transmission Protocol (SCTP) transport to IP-based application processors or databases. The M3UA SG terminates the SS7 MTP2 and MTP3 protocol layers and delivers ISDN User Part (ISUP), Signaling Connection Control Part (SCCP) and/or any other MTP3-User protocol messages. The Application Server Process (ASP) is the IP-based instance of an application process or database such as Call Agents, Home Location Registers (HLRs), etc.

Figure 2 depicts the relationship between the legacy SS7 Service Control Point, the M3UA SG, the IP-based Application Server Process (ASP), and the protocol stacks.

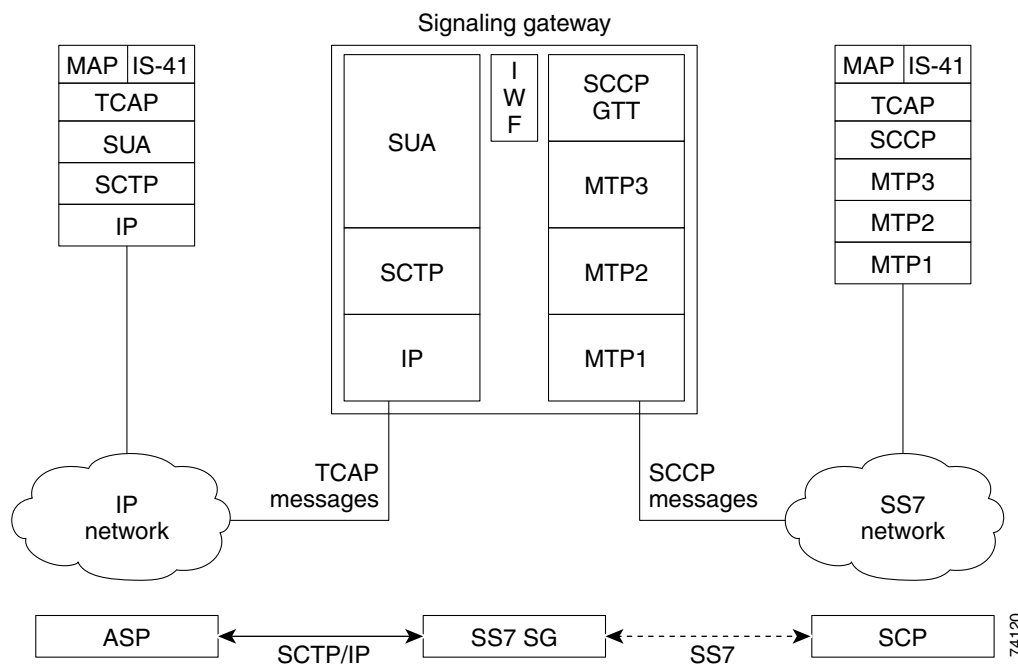
Figure 2 M3UA Signaling Gateway Protocol Stacks

In [Figure 2](#), the legacy SS7 SCP on the far right uses MTP1, MTP2, and MTP3 for transporting SCCP and ISUP messages into the network. The SG terminates the SS7 links, translates the MTP3 messages into M3UA messages, and transports them to the ASP over SCTP/IP. M3UA at the ASP delivers SCCP and ISUP messages.

Sigtran SUA - SS7 SCCP-User Adaptation Layer

SUA describes a transport mechanism for delivering SS7 SCCP-User Part messages and certain SCCP network management events over SCTP transport to IP-based application processors or databases. The SUA SG terminates the SS7 MTP2, MTP3, and SCCP protocol layers and delivers TCAP, RANAP and/or any other SCCP-User protocol messages. The Application Server Process (ASP) is the IP-based instance of an application process or database (e.g. HLRs, SMSCs, etc.).

[Figure 3](#) depicts the relationship between the legacy SS7 Service Control Point, the SUA SG, the IP-based Application Server Process (ASP), and the protocol stacks.

Figure 3 *SUA Signaling Gateway Protocol Stacks*

In Figure 3, the legacy SS7 SCP on the far right uses MTP1, MTP2, and MTP3 for transporting SCCP messages into the network. The SG terminates the SS7 links, translates the SCCP messages into SUA messages, and transports them to the ASP over SCTP/IP. SUA at the ASP delivers TCAP messages.

Benefits

The Cisco ITP Router provides the following benefits:

- Lower incremental investment from using a cost-effective IP network
- Reduced number of links
- Reduced STP ports
- Reduced processor occupancy for STP
- Support for the full suite of Cisco routing protocols and QoS technologies
- Non-intrusive, end-point devices transparent to the SS7 network
- Full set of high-end routing protocols and IP media
- Integrated SS7 and IP management using IP-based industry standard tools
- High Availability and increased link density for SS7 line cards via an SS7 Port Adapter



Planning to Configure ITP

This chapter describes the prerequisites to installing the Cisco ITP product, including supported hardware and software. The chapter includes references to related documentation.

Supported Platforms

- Cisco 2811 Integrated Services Router
- Cisco 7204 Router
- Cisco 7206 Router
- Cisco 7301 Router



Note

ATM HSL is supported on the Cisco 7301 routers. ATM is supported on the Loki 8 port T1/E1 port adapter with IMA support (PA-A3-8T1IMA and PA-A3-8E1IMA). We recommend that you do not mix link types (low speed links, high speed links, M2PA/XUA) on the same FlexWAN.

Supported Standards, MIBs, and RFCs

Standards

- ANSI 1996
- ITU white 1996
- SS7 MTP2-User Peer-to-Peer Adaptation Layer RFC 4165
- SS7 MTP3-User Adaptation Layer (M3UA) Sigtran M3UA RFC number 3332
- SS7 SCCP-User Adaptation Layer (SUA) Sigtran SUA draft version 14

MIBs

- CISCO-BITS-CLOCK-MIB.my
MIB provides information on Building Integrated Timing Supply (BITS) clocking sources and modes of operations. It is used to generate notifications to indicate when clocking sources change roles or become unavailable.

NOTIFICATIONS

- ciscoBitsClockFreerun
 - ciscoBitsClockHoldover
 - ciscoBitsClockSource
- CISCO-IETF-SCTP-MIB.my
Cisco Systems implementation of Stream Control Transmission Protocol MIB (RFC 2960). This MIB is based on the IETF document draft-ietf-sigtran-sctp-mib-04.txt.
- CISCO-IETF-SCTP-EXT-MIB.my
Cisco Systems extensions for the Stream Control Transmission Protocol MIB (RFC 2960). This MIB is based on the IETF document draft-ietf-sigtran-sctp-mib-04.txt.

NOTIFICATIONS

- cSctpExtDestAddressStateChange
- CISCO-ITP-ACL-MIB.my
MIB for managing access lists that control messages transported over the SS7 network via Cisco ITP.
- CISCO-ITP-ACT-MIB.my
Deprecated and replaced by CISCO-ITP-GACT-MIB.my
- CISCO-ITP-GACT-MIB.my
MIB for providing information specified in ITU Q752 Monitoring and Measurements for the SS7 network. This management information base replaces CISCO-ITP-ACT-MIB.my and provides support for multiple instances of signaling points on the same device.
- CISCO-ITP-GRT-MIB.my
MIB for managing the route table used to control messages transported over the SS7 network via Cisco ITP. This management information base replaces CISCO-ITP-RT-MIB.my and provides support for multiple instances of signaling points on the same device.

NOTIFICATIONS

- ciscoGrtDestStateChange
 - ciscoGrtMgmtStateChange
 - ciscoGrtRouteTableLoad
- CISCO-ITP-GSCCP-MIB.my
MIB for Signalling Connection Control Part (SCCP) messages transported over the SS7 network via Cisco ITP. This management information base replaces CISCO-ITP-SCCP-MIB.my and provides support for multiple instances of signaling points on the same device.

NOTIFICATIONS

- ciscoGsccpGttErrors
 - ciscoGsccpGttLoadTable
 - ciscoGsccpGttMapStateChange
- CISCO-ITP-GSP-MIB.my
MIB for managing signalling points and associated messages transported over SS7 via Cisco ITP. This management information base replaces CISCO-ITP-SP-MIB.my and provides support for multiple instances of signaling points on the same device.

NOTIFICATIONS

- ciscoGspCongestionChange
- ciscoGspIsolation
- ciscoGspLinkRcvdUtilChange
- ciscoGspLinkSentUtilChange
- ciscoGspLinksetStateChange
- ciscoGspLinkStateChange
- CISCO-ITP-GSP2-MIB.my

MIB for providing Quality of Service (QOS) information for the ITP environment. Also, provides event history for SS7 events. This management information base replaces CISCO-ITP-SP-MIB.my and provides support for multiple instances of signaling points on the same device.
- CISCO-ITP-MLR-MIB.my

The MIB for providing information about Multi-layer Routing (MLR). This MIB will provide information used to control and measure SS7 messages signalling units in a SS7 Network. Message Signalling Units are routed based on information found in the SCCP, TCAP, MAP, and MAP-user layers.

NOTIFICATIONS

- ciscoMlrTableLoad
- CISCO-ITP-MONITOR-MIB.my

The MIB for providing information related to monitoring SS7 links. This information can be used to manage the state of software used to collect all packets transported and received over a SS7 link.

NOTIFICATIONS:

- ciscoItpMonitorCongestion
- ciscoItpMonitorState
- CISCO-ITP-RT-MIB.my

Deprecated and replaced by CISCO-ITP-GRT-MIB.my
- CISCO-ITP-SCCP-MIB.my

Deprecated and replaced by CISCO-ITP-GSCCP-MIB.my
- CISCO-ITP-SP-MIB.my

Deprecated and replaced by CISCO-ITP-GSP-MIB.my
- CISCO-ITP-SP2-MIB.my

Deprecated and replaced by CISCO-ITP-GSP2-MIB.my
- CISCO-ITP-TC-MIB.my

MIB defining textual conventions used to manage devices related to the SS7 network. The relevant ITU documents describing this technology are the ITU Q series, including ITU Q.700: Introduction to CCITT Signalling System No. 7 and ITU Q.701: Functional Description of the Message Transfer Part (MTP) of Signalling System 7.

- CISCO-ITP-XUA-MIB.my

MIB for managing ASPs, ASs, Mated Pair Signaling Gateways for M3UA and SUA.

NOTIFICATIONS

- ciscoItpXuaAspCongChange
- ciscoItpXuaAspStateChange
- ciscoItpXuaAsStateChange
- ciscoItpXuaSgmCongChange
- ciscoItpXuaSgmStateChange

- CISCO-RF-MIB.my

This MIB provides configuration control and status for the Redundancy Framework (RF) subsystem.

NOTIFICATIONS

- ciscoRFProgressionNotif
- ciscoRFSwactNotif

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB web site on Cisco.com at

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

RFCs

- BSD Syslog Protocol (RFC 3164)
- Remote Authentication Dial-In User Service (RADIUS) (RFC 2865)
- Stream Control Transmission Protocol (RFC 2960) User Datagram Protocol, STD 6 (RFC 768)



Performing IOS ITP Software Upgrade



Note

Configuration Mode Restrictions: Simultaneous changes to the configuration from multiple CLI sessions are not supported. Only one configuration session is allowed to enter in configuration mode at a time; other sessions should not enter in configuration mode. The **show line** or **show users EXEC** command may be used to determine the active user sessions on an ITP, and the **clear line EXEC** command may be used to ensure that only a single active session exists.

This chapter includes the following software upgrade procedures:

- [Performing ITP IOS Software Upgrade, page 9](#)
- [Performing ITP Group Software Upgrade, page 10](#)

Performing ITP IOS Software Upgrade

To upgrade the ITP IOS software, perform following steps, beginning in Privileged user mode:

	Command	Purpose
Step 1	<pre>Router# copy tftp slot slot-number: Address or name of remote host []? ip-address Name of file to copy []? imagename <Return> writing filename!! Destination file name? [imagename1] <Return> Accessing file 'imagename' on ip-address.. found ! Loading imagename from ip-address (via Ethernet1/0/0): !</pre>	Uses TFTP to copy the new Cisco IOS image onto the Flash memory card of the active RSP. • slotslot-number—Specifies the Flash memory card of the active RSP. The router prompts you for the IP address of the TFTP server. • ip-address—Specifies the IP address of the TFTP server that contains the new image. The router prompts you for the name of the image file you are copying to the Flash memory card. • imagename—Indicates the name of the image to be loaded onto the Flash memory card. The router prompts you to enter the name under which you want the file to appear at the destination. • imagename1—Indicates the name of the image as it appears at the destination.

Step 2	Router# configure terminal	Enters global configuration mode.
Step 3	Router(config)# no boot system disk:image	Removes the existing boot statements from the running-config file.
Step 4	Router(config)# boot system disk:image	Specifies the new image to be loaded at startup.
Step 5	Router(config)# copy running-config startup-config	Saves the running configuration as the startup configuration.
Step 6	Issue the shutdown command for all linksets. This redirects all traffic through alternate routes. The updated running-config that includes the shutdown commands for the linksets does not have to be saved.	
Step 7	Router# reload	Reloads the IOS image.

Performing ITP Group Software Upgrade

This procedure describes the steps to upgrade the ITP IOS software if you have implemented ITP Group.

1. Determine the ITP Group state of the two ITPs in the group being upgraded. This can be accomplished by issuing the **show cs7 group state** command. The ITP with a group state of *Manager* will be referred to as the Manager throughout this procedure. The ITP with a group state of *Alternate* will be referred to as the Alternate throughout this procedure.
2. If the ITPs are to be loaded from flash or disk, transfer the new ITP images to the flash/disk on both the Manager and Alternate.

Steps 3 - 5 are performed on the Manager.

3. On the Manager issue a **shutdown** command for all MTP2 links that physically reside on the Manager. This will redirect all traffic handled by the ITP Group through the Alternate.
4. On the Manager issue a **shutdown** command for all Ethernet interfaces that are configured with IP addresses used by the group control transport and the redundancy state transport. These IP addresses appear on the **local-ip** statements under the **cs7 group** command and the **ipc zone default/association** commands. Both the Manager and Alternate will transition to a group state of *ManagerIsolated*. This can be verified by issuing the **show cs7 group state** command.
5. Immediately save the Manager configuration and reload the Manager with the new ITP image.
6. When the Manager reloads and achieves a group state of *ManagerIsolated*, reactivate (with the **no shutdown** command) all MTP2 links that physically reside on the Manager and verify that the traffic is being forwarded by the Manager.

Steps 7 - 10 are performed on the Alternate.

7. On the Alternate, save any configuration changes to the startup-config that are required for the upgraded image (such as the name and location of the new image to be loaded). Then shutdown all MTP2 links that physically reside on the Alternate. This will redirect all traffic handled by the ITP Group through the Manager.
8. Immediately reload the Alternate with the new ITP image. The updated running-config that contains the **shutdown** commands for the MTP2 links does not have to be saved.
9. While the Alternate is reloading reactivate (with the **no shutdown** command) the Ethernet interfaces on the Manager that were shutdown in Step 4). Ensure that this step is performed before the Alternate is fully initialized.

10. The Alternate will resume its role as the Alternate when it initializes and will begin forwarding traffic on its MTP2 links when it has received its state information from the Manager.



Configuring ITP Basic Functionality

This chapter describes the specific tasks and commands to configure basic Cisco ITP functionality.

For information about configuring the IOS software, beyond the specific ITP configuration instructions that are included in this document, refer to the Cisco IOS Release 12.2 documentation at the following URLs:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/finter_c/index.htm



Note

Cisco ITP on the Cisco 7600 Series Routers requires that the default MAC address is used on all FlexWAN interfaces. The ITP does not support alternate MAC addresses on FlexWAN interfaces.



Note

Cisco ITP on the Cisco 7600 Series Routers requires traffic to be transmitted and received using only FlexWAN interfaces.



Note

Cisco ITP on the Cisco 7600 Series Routers requires specifying a numerical next hop when configuring a default route 0.0.0.0 0.0.0.0.



Note

IP routing is enabled on the ITP by default, and must not be disabled. Disabling IP routing can result in connection errors.



Note

You must perform ITP CLI configuration only on the active supervisor module of the Cisco 7600 Series Routers. We recommended you not perform configuration on a SAMI. Because the active supervisor module is the controller card, the configuration is synced from the supervisor to the linecards.



Note

Configuration Mode Restrictions: Simultaneous changes to the configuration from multiple CLI sessions are not supported. Only one configuration session is allowed to enter in configuration mode at a time; other sessions should not enter in configuration mode. The **show line** or **show users EXEC** command may be used to determine the active user sessions on an ITP, and the **clear line EXEC** command may be used to ensure that only a single active session exists.

Contents

This chapter discusses the following topics and describes the associated configuration tasks:

- [Enabling Secure Shell, page 14](#)
- [Specifying the SS7 Variant, National Option, and Network Indicator, page 15](#)
- [Specifying the Point Code, page 18](#)
- [Specifying the Point Code, page 18](#)
- [Specifying the Interface and Encapsulation, page 20](#)
- [Configuring Local Peers, page 32](#)
- [Configuring Linksets, page 32](#)
- [Configuring Circular Route Direction \(CRD\), page 34](#)
- [Configuring Multiple Linksets to Adjacent Nodes, page 37](#)
- [Specifying the Cisco ITP Route Table, page 38](#)
- [Assigning Links to Linksets, page 40](#)
- [Shutting Down and Restarting Linksets and Links, page 42](#)
- [Configuration Example of ITP Basic Functionality, page 43](#)

Enabling Secure Shell

The Secure Shell (SSH) feature enables secure sessions by establishing an encrypted connection between an SSH client and an SSH server.

For information about configuring the Secure Shell feature, beyond the basic instructions below, please refer to the *Cisco IOS Release 12.4 Security Configuration Guide* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hsec_c/index.htm

and to the *Cisco IOS Release 12.4 Security Command Reference* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cr/hsec_r/index.htm

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **username *username* password *password***
4. **aaa new-model**
5. **ip domain-name *domain-name***
6. **ip ssh authentication-retries *num***
7. **crypto key generate rsa modulus *size***
8. **ssh -I *userID* {*ip-address* | *hostname*}** (Enter this command from an Xterm window.)
9. **show ssh** (Enter this command from the ITP.)

	Command	Purpose
Step 1	enable Example: ITP> enable	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	configure {terminal memory network} Example: ITP# configure terminal	Enters configuration mode, selecting the terminal option.
Step 3	username username password password Example: ITP(config)# username admin password jo4fhe	Specifies the username and password.
Step 4	aaa new-model Example: ITP(config)# aaa new-model	Enables the authentication, authorization, and accounting (AAA) access control model.
Step 5	ip domain-name domain-name Example: ITP(config)# ip domain-name cisco	Specifies the domain.
Step 6	ip ssh authentication-retries num Example: ITP(config)# ip ssh authentication-retries 3	Specifies the number of attempts after which the interface is reset.
Step 7	crypto key generate rsa modulus size Example: ITP(config)# crypto key generate rsa modulus 768	Generates Rivest, Shamir, and Adelman (RSA) key pairs.
Step 8	ssh -I userID {ip-address hostname} Example: ITP# ssh -I adminHQ HQhost	(Enter this EXEC command from an xterm window.) Starts an encrypted session with a remote networking device,
Step 9	show ssh Example: ITP# show ssh	(Enter this EXEC command from the ITP) Displays the status of the SSH connections. Use this command to verify your SSH connectivity.

Specifying the SS7 Variant, National Option, and Network Indicator

The SS7 variant specifies which variation of SS7 the router is running. The variant configured on the ITP must match the variant of the connected SS7 network.

**Note**

If you change the variant after you have completed ITP configuration, you must first remove all linksets and the local point-code. After reconfiguring the variant, you must first reconfigure the point code and then the linkset.

To specify one of these variants, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cs7 variant {ansi | itu | china | ttc}**
4. **cs7 national-options {TFR | multiple-congestion | route-set-congestion-test | combined-linkset-loadsharing}**
5. **cs7 network-indicator {international | national | reserved | spare}**
6. **cs7 [instance *instance-number*] local-sccp-addr-ind {national | international}**

	Command	Purpose
Step 1	enable Example: ITP> enable	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	configure {terminal memory network} Example: ITP# configure terminal	Enters configuration mode, selecting the terminal option.
Step 3	cs7 variant {ansi itu china ttc} Example: ITP(config)# cs7 variant ansi	Specifies which SS7 variant the router is running.

	Command	Purpose
Step 4	cs7 national-options {TFR multiple-congestion signaling-route-congestion-test combined-linkset-loadsharing} Example: ITP(config)# cs7 national-options TFR	Specifies national options. The national options apply to the variants as follows: • TFR—ITU and China SS7 Variants • multiple-congestion—ITU and China SS7 Variants • signaling-route-congestion-test—TTC SS7 Variant • combined-linkset-loadsharing—Configures the TTC variant to use the enhanced loadsharing algorithm Note All SS7 variants, except TTC, use the enhanced loadsharing algorithm for distributing messages across the available links within a linkset and combined linkset. By default, the TTC variant uses the A/B linkset selection bit that exists as part of the SLS in the MSU routing label. Note Configure national option as combined-linkset-loadsharing in TTC variant to use the enhanced loadsharing algorithm at the configuration time of variant. If you do not want to use the enhanced loadsharing algorithm, do not configure national option as combined-linkset-loadsharing. If already configured, unconfigure national option and reload the router for the change to take effect.
Step 5	cs7 network-indicator {international national reserved spare} Example: ITP(config)# cs7 network-indicator international	(Optional) Specifies the network indicator. The network indicator on the ITP must match the network indicator in use in the rest of the SS7 network. The default is national.
Step 6	cs7 [instance <i>instance-number</i>] local-sccp-addr-ind {national international} Example: ITP(config)# cs7 local-sccp-addr-ind international	(Optional) Customizes the setting of the national use field within SCCP management calling and called party addresses. The default value for instances configured with the ANSI variant is national ('1'b value), and the default for all other variants is international ('0'b value).

Specifying the Point Code

Each signaling point (also called an SS7 node) in the SS7 network is identified with a unique address called a point code (PC). PCs are carried in signaling messages exchanged between signaling points to identify the source and destination of each message. Operators can assign their own PCs in private SS7 networks.

Specifying the Point Code Representation

The format of the point code can be represented according to either the ANSI, ITU, China or Japan TTC standard. The ANSI and China standard for point code representation is 24 bits partitioned into 3 components that specify network.cluster.member, with a default representation of 8.8.8. The ITU standard for point code representation is 14 bits partitioned into 3 components that specify zone.region.signaling point (sp), with a default point code representation of 3.8.3. The TTC standard for point code representation is 16 bits partitioned into 3 fields with a default representation of 5.4.7. The delimiter that will appear between each segment (when you show output of the configuration) can be either a dot or a dash. You can modify the default point code bit format and the default delimiter at any time during configuration, without prior removal of links and linksets.

You can change the partitioning of the bits to any configuration of 1, 2, or 3 components that total the 24-bit ANSI and China standard or 14-bit ITU standard. To modify the ANSI or ITU point code format, or to return to either standard's default format, use one of the following commands in global configuration mode:

Command	Purpose
cs7 [instance <i>instance-number</i>] point-code format <i>1-24</i> [<i>1-23</i> [<i>1-22</i>]] [description <i>string</i>] Example: ITP(config)# cs7 instance 1 point-code format 2 6 6 description network cluster member	Specifies the point code representation.
cs7 point-code format default Example: ITP(config)# cs7 point-code format default	Resets the point-code format to the default 8.8.8 (ANSI and China), 3.8.3 (ITU), or 5.4.7 (TTC).

The default delimiter between components of the point code is a dot. To change the delimiter to a dash, or to return to the default delimiter (dot), use one of the following commands in global configuration mode:

Command	Purpose
<code>cs7 point-code delimiter [default dash]</code>	Specifies the delimiter between bits as either dots or dashes.
Example: <pre>ITP(config)# cs7 point-code delimiter dash</pre>	
<code>cs7 point-code delimiter default</code>	Resets the delimiter to dots.
Example: <pre>ITP(config)# cs7 point-code delimiter default</pre>	

Specifying the Primary Local Point Code



Note

You must specify the SS7 variant before you can specify the local point code.

Each Cisco ITP must have a unique local point code that is used to send management messages to adjacent signaling points. To specify the point code, use the following command in global configuration mode:

Command	Purpose
<code>cs7 point-code point-code</code>	Specifies the primary point code for the ITP.
Example: <pre>ITP(config)# cs7 point-code 5.100.1</pre>	

Specifying a Secondary Point Code

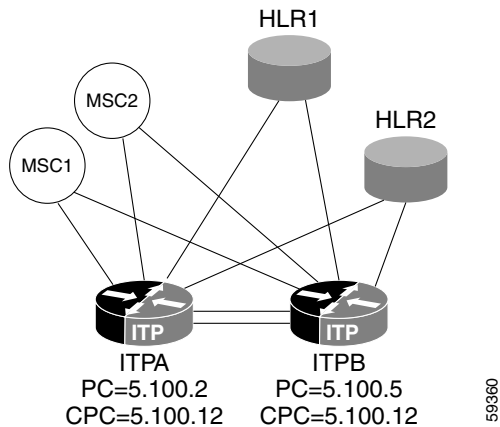
If you intend to configure a second linkset between the ITP and an adjacent node, you must specify a secondary local point code. You cannot exceed a maximum of 40 secondary point codes per chassis. To specify the secondary point code, use the following command in global configuration mode:

Command	Purpose
<code>cs7 secondary-pc point-code</code>	Specifies a secondary point code for the ITP.
Example: <pre>ITP(config)# cs7 secondary-pc 5.100.2</pre>	

Specifying the Capability Point Code

The ITP supports configuration of up to 200 capability point-codes (CPC) per instance. CPC configuration is optional, but recommended for certain networks. The prime example for use of a CPC is when a mated pair of ITP nodes shares the same GTT database for redundancy purposes. In this configuration, all SCCP messages are directed to a single “capable” point-code; either ITP can handle the SCCP processing. The figure below shows a mated pair of ITPs with identical capability point-codes and a common GTT database for selecting the appropriate HLR.

Figure 4 Mated Pair of ITPs With the Same Capability Point Codes



In Figure 4, each of the MSCs have two routes to the mated pair of ITPs. The MSCs can either load-share all GTT messages between the mated pair of ITPs, or use one ITP as a backup should the primary fail. All messages requiring GTT can be routed to the same destination point-code. In this case the DPC is the CPC, which is 5.100.12. The benefit of CPC usage in this case is that if a single ITP is unreachable, the MSCs are unaware of this event.

To specify the capability point code, use the following command in global configuration mode:

Command	Purpose
<code>cs7 capability-pc point-code</code>	Specifies the capability point code for the ITP. ITP supports the configuration of up to 200 capability point codes per instance.
Example: <code>ITP(config)# cs7 capability-pc 5.100.12</code>	



Note

The previously defined point code format must be used to enter the capability point-code.

All messages requiring GTT processing can be routed to either the local point-code or the capability point-code.

Specifying the Interface and Encapsulation



Note

To avoid unnecessary CPU load, we recommend that you shut down interfaces that are configured but not provisioned as part of a linkset.

The following sections provide information and tasks for various interface and encapsulation configurations:

- [Clocking on the SS7 Port Adapter and SS7 Q.703 High Speed Port Adapter, page 21](#)
- [Configuring a Serial Interface and SS7 High-Speed MTP2 Encapsulation \(Q.703 Annex A\) on the SS7 Q.703 High Speed Port Adapter, page 21](#)
- [Configuring a Serial Interface and MTP2 Encapsulation on the SS7 Port Adapter, page 23](#)

- [Configuring SS7 over ATM High Speed Links \(HSL\), page 25](#)
- [Configuring BITS Network Clocking, page 27](#)
- [Configuring SS7 ATM High Speed Links with BITS Network Clocking, page 29](#)

Clocking on the SS7 Port Adapter and SS7 Q.703 High Speed Port Adapter

Each SS7 Port Adapter in the ITP shares a clocking source for all T1s and E1s serviced on that card. The clocking options and commands are listed here and shown in the configuration tasks that follow this section:

- Clocking source is internally generated.
clock source internal
This option imposes the requirements that all devices connected to the ITP must derive their clock from the T1/E1 by which they are connected to the ITP.
- Clocking source is derived from a T1/E1 that is terminated on the card.
clock source line {primary | secondary priority}
The SS7 Port Adapter on the ITP derives its clock from an adjacent node. All other T1s or E1s on the card are clocked with this derived source. This option imposes the restrictions that all adjacent nodes connected to T1s or E1s on that card must either derive the clock from the T1/E1 to which they are connected or are derive the clock from the same source as the ITP.
- Clocking source is provided through a dedicated port on that card via BITS (a common source received via satellite and used to synchronize all clocks across a CO and between COs)
clock source bits {primary | secondary priority}
A common dedicated clock source is wired to all devices and used by each device for all T1/E1 timing.
A controller that is configured for BITS clocking cannot be used to carry data.



Note

It is recommended that any controller that is not used for SS7 links or BITS clocking should be shut down.

Configuring a Serial Interface and SS7 High-Speed MTP2 Encapsulation (Q.703 Annex A) on the SS7 Q.703 High Speed Port Adapter

The SS7 Q.703 High Speed Port Adapter for the Cisco ITP (PA-MCX-4TE1-Q) is a single-width, high speed port adapter that supports enhanced Message Transfer Part Level 2 (MTP2) functions and procedures that are suitable for the operation and control of signaling links at data rates of 1.5 and 2.0 Mb. For the complete instructions for installing and configuring the SS7 Q.703 high speed port adapter, see the *SS7 Q.703 High Speed Port Adapter Installation and Configuration Guide* at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7507/portadp/multicha/mcx4te1q/index.htm>.

To perform the basic configuration for the SS7 Q.703 High Speed Port Adapter, you specify the card type as E1, configure the controller, configure a channel group on the port adapter to use all the time slots, and configure the interface for SS7 high-speed MTP2 encapsulation. Perform these tasks, beginning in global configuration mode:

	Command	Purpose
Step 1	card type e1 slot bay Example: ITP(config)# card type e1 6 0	Configures the card type.
Step 2	controller e1 slot/bay/port Example: ITP(config)# controller e1 6/0/0	Configures an E1 controller.
Step 3	framing crc4 Example: ITP(config-controller)# framing crc4	Specifies the framing format for E1 controller.
Step 4	linestate debounce Example: ITP(config-controller)# linestate debounce	Suppresses rapid linestate transitions that may occur due to brief interruption of the framing on an E1 controller.
Step 5	clock source {bits {primary secondary priority} internal line {primary secondary priority}} Example: ITP(config-controller)# clock source internal	Specifies the clock source as internal.
Step 6	linecode hdb3 Example: ITP(config-controller)#	Specifies high-density bipolar 3 (hdb3) as the line-code type. Valid for E1 controller only. This is the default for E1 lines.
Step 7	channel-group channel-number timeslots 1-31 Example: ITP(config-controller)# channel-group 0 timeslots 1-31	Configures the channel group and timeslots 1-31. Note High-speed MTP2 links must use timeslots 1-31 on an E1.
Step 8	exit Example: ITP(config-controller)# exit	Exit controller configuration mode and return to global configuration mode.
Step 9	ITP(config)# interface serial number Example: ITP(config)# interface serial 6/0/0:0	Configures a serial interface in global configuration mode and enters interface configuration mode.
Step 10	encapsulation hs-mtp2 Example: ITP(config-if)# encapsulation hs-mtp2	Configures the serial interface to use SS7 high-speed MTP2 encapsulation.

Configuring a Serial Interface and MTP2 Encapsulation on the SS7 Port Adapter

**Note**

The ITP supports SS7 links over T1/E1 router interfaces. These are router interfaces where the CSU/DSU functionality is integrated into the port adapter. Multiple SS7 links can be configured per T1/E1 interface in this configuration.

The SS7 Port Adapter is a single-width, eight-port T1/E1 port adapter with a custom hardware-assist engine to support SS7 signaling. The SS7 Port Adapter features full channelization of up to 126 HDLC-encoded SS7 (or DS0) channels at 56 Kbps or 64 Kbps. This feature requires the SS7 Port Adapter (PA-MCX-8TE1-M=) with the controller configured for BITS clock.

For more information on the SS7 Port Adapter, refer to the SS7 guide, *SS7 Port Adapter Installation and Configuration* on Cisco.com:

<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7507/portadp/multicha/mcx8te1/index.htm>

To configure a serial interface and MTP2 encapsulation for the SS7 Port Adapter, you specify the card type, configure the controller, configure a channel group on the port adapter to use all the time slots, and specify the interface for MTP2 encapsulation.

A separate channel group statement is necessary for each traditional SS7 link to be mapped to the specific T1/E1 link.

**Note**

An SS7 port adapter that is configured to be E1 cannot use port 7 timeslot 31.

**Note**

MTP2 low speed links support only 1 timeslot per serial link.

**Note**

If you use a T1/E1 card for your SS7 connectivity, each channel group statement under the controller automatically produces a serial subinterface for that channel. To complete connectivity over the T1/E1 interface, you must enable MTP2 encapsulation on those serial sub-interfaces.

The scenario for the configuration task that follows assumes a T1 interface with T1 cross over cable to an STP. The framing and linecode are set to match the STP values. For this configuration, the T1/E1 controller parameters must be set appropriately with the device on the other side of the T1/E1 link. Here, two SS7 links are being configured over the same T1 interface, one on timeslot 1 and the other on timeslot 2.

To configure the T1 interface as indicated in the above scenario, use the following commands beginning in global configuration mode:

■ Specifying the Interface and Encapsulation

	Command	Purpose
Step 1	card type {t1 e1} slot bay Example: ITP(config)# card type t1 1 1	Configures the card type.
Step 2	controller {t1 e1} slot/port-adapter-num/port Example: ITP(config)# controller t1 1/1/1	Specifies the controller and enters controller configuration mode.
Step 3	linestate debounce Example: ITP(config-controller)# linestate debounce	(Optional for E1 controller configuration.) Supresses rapid linestate transitions that may occur due to brief interruption of the framing on an E1 controller.
Step 4	variant jt1 Example: ITP(config-controller)# variant jt1	(Optional) Applies to T1 interface only. Enables Japanese variations of the standard framing formats.
Step 5	framing {sf esf} Example: ITP(config-controller)# framing esf	Specifies the framing format for T1.
Step 6	clock source {bits {primary secondary priority} internal line {primary secondary priority}} Example: ITP(config-controller)# clock source internal	Specifies the clock source as internal.
Step 7	linecode {ami b8zs hdb3} Example: ITP(config-controller)# linecode b8zs	Specifies the line code type as B8ZS.
Step 8	channel-group channel-group-num timeslots range Example: ITP(config-controller)# channel-group 0 timeslots 1	Specifies the channel group.
Step 9	channel-group channel-group-num timeslots range Example: ITP(config-controller)# channel-group 1 timeslots 2	Specifies the channel group.
Step 10	exit Example: ITP(config-controller)# channel-group 1 timeslots 2	Exits controller configuration mode and returns to global configuration mode.

	Command	Purpose
Step 11	<pre>ITP(config)# interface serial number</pre> Example: <pre>ITP(config)# interface serial 1</pre>	Configures a serial interface in global configuration mode and enters interface configuration mode.
Step 12	<pre>ITP(config-if)# encapsulation mtp2</pre> Example: <pre>ITP(config)# encapsulation mtp2</pre>	Configures the serial interface to use MTP2 encapsulation.

Configuring SS7 over ATM High Speed Links (HSL)



Note

ITP HSL is compliant with both ANSI per Telcordia GR-2878-CORE and ITU per Q.2100, and includes the following protocol stack components: AAL5, SSCOP, SSCF-NNI and MTP3b. On the Cisco 7301 and Cisco 7200 routers, ATM is supported on the following IMA capable port adapters: PA-A3-8T1IMA, PA-A3-8E1IMA, PA-A3-OC3-MM, PA-A3-OC3-SMI, PA-A3-OC3-SML, PA-A6-OC3-MM, PA-A6-OC3-SMI, and PA-A6-OC3-SML.

ITP ATM HSL allows high-speed SS7 connectivity over ATM links. HSL capability can replace the traditional MTP1 and MTP2 layers of the SS7 protocol stack with SAAL. The following sections describe the required tasks for configuring an ITP for ATM HSL support:

- [Enabling an ATM Interface, page 25](#) (Required)
- [Configuring a Permanent Virtual Circuit \(PVC\), page 27](#) (Required)

Enabling an ATM Interface

To enable an ATM interface for HSL, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	<pre>interface atm interface-number[.subinterface-number]</pre> Example: <pre>ITP(config)# interface atm 2/0.1</pre>	Enters the configure ATM interface or configure ATM subinterface mode.
Step 2	<pre>no shutdown</pre>	Enables the interface.

Specifying the Interface and Encapsulation

	Command	Purpose
Step 3	framing esfadm -OR- framing crc4adm	Specifies frame type (T1 only). -or- Specifies frame type (E1 only).
	For OC3 use the following: atm framing sdh -OR- atm framing sonet	Specifies SDH framing mode (OC3 only). -or- Specifies SONET framing mode (OC3 only).
	Example: ITP(config-if)# framing crc4adm	
Step 4	clock source {common internal line} Example: ITP(config-if)# clock source internal	(Optional) Specifies the clock source (T1/E1 only).

Enabling an OC3 ATM Interface

To enable an OC3 ATM interface for HSL, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	interface atm <i>interface-num</i> Example: ITP(config)#	Specifies an ATM interface and enters interface configuration mode.
Step 2	no shutdown Example: ITP(config-if)# no shutdown	Enables the interface.
Step 3	atm sonet stm-1 Example: ITP(config-if)# atm sonet stm-1	Specifies SDH (STM-1) framing.

Configuring a Permanent Virtual Circuit (PVC)

You must configure a permanent virtual circuit (PVC) on the ATM interface or subinterface before you can define the interface as a link. To configure the PVC, use the following commands, beginning in interface configuration mode:

	Command	Purpose
Step 1	atm nni	Selects service specific coordination function for Network Node Interface.
	Example: ITP(config-if)# atm nni	
Step 2	pvc [name] {vpi/vci} [qsaal]	Specifies the PVC. The default/recommended PVC number is 0/5.
	Example: ITP(config-if)# pvc 0/5 qsaal	qsaal is a signaling type PVC used to communicate between SS7 nodes.
		Note ces , ilmi , smds , and l2transport are not supported.



Note

Only one qsaal is permitted for each ATM interface or subinterface. To allow more qssals, you must create an additional subinterface for each additional qsaal, and add these subinterfaces to the linkset.

To configure the linkset, see the [“Configuring Linksets” section on page 32](#). To specify or tune optional HSL bundling, SSCF-NNI, or SSCOP parameters, see the [“Tuning HSL Parameters” section on page 394](#) of the [“Verifying, Monitoring, and Tuning the ITP” chapter](#).

For details about the above commands, refer to the Cisco IOS Wide-Area Networking Command Reference, Release 12.2, ATM Commands, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fwan_r/atmcmds/index.htm

Configuring BITS Network Clocking

Building Integrated Timing Supply (BITS) is a method of ensuring network synchronization. With BITS, a single master timing source supplies the clock reference for all nodes.



Note

A controller that is configured for BITS clocking cannot be used to carry data. If BITS clocking has been set, no channel groups can be configured. If channel groups have been configured, BITS cannot be configured.

To configure BITS network clocking, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	controller { t1 e1 } <i>slot/port-adapter-num/port</i> Example: ITP(config)# controller t1 1/1/1	Specifies the controller and enters Controller configuration mode.
Step 2	framing { sf esf } Example: ITP(config)# framing esf	Specifies the framing format for T1.
Step 3	clock source { bits { primary secondary <i>priority</i> } internal line { primary secondary <i>priority</i> }} Example: ITP(config-controller)# clock source bits primary	Specifies the clock source as BITS primary source.
Step 4	linecode { ami b8zs hdb3 } Example: ITP(config-controller)# linecode b8zs	Specifies the line code type as B8ZS.

Configuring SS7 ATM High Speed Links with BITS Network Clocking

If you prefer to use a common, reliable clock source over several links, you can deliver a BITS clock to the SS7 ATM high speed links. To do so, you must configure BITS clocking on the SS7 port adapter controller. Then, connect a T1 crossover cable from the SS7 port adapter controller to a T1 Inverse Multiplexing for ATM (IMA) port adapter interface. The IMA port adapter interface receives the BITS clock source for all other interfaces on that IMA port adapter. All other interfaces on the IMA port adapter accept the BITS clock by specifying **clock source common interface-number**, where *interface-number* is the IMA port adapter interface that is crossover cabled to the SS7 port adapter.

This feature requires the SS7 Port Adapter (PA-MCX-8TE1-M=) with the controller configured for BITS clock. For more information on the SS7 Port Adapter, refer to the SS7 guide, *SS7 Port Adapter Installation and Configuration* on Cisco.com:

To provide a BITS clock source to the SS7 ATM high speed links, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	controller t1 slot/port-adapter-num/port Example: ITP(config)# controller t1 2/0/0	Specifies controller 0 on the SS7 port adapter and enters controller configuration mode.
Step 2	clock source {bits {primary secondary priority} internal line {primary secondary priority}} Example: ITP(config-controller)# clock source bits primary	Specifies controller 0 on the SS7 port adapter as the the primary source of the BITS clock.
Step 3	exit Example: ITP(config-controller)# exit	Exits from controller configuration mode to global configuration mode.
Step 4	controller t1 slot/port-adapter-num/port Example: ITP(config)# controller t1 2/0/1	Specifies controller 1 on the SS7 port adapter and enters controller configuration mode.
Step 5	clock source {bits {primary secondary priority} internal line {primary secondary priority}} Example: ITP(config-controller)# clock source bits secondary 1	Specifies controller 1 on the SS7 port adapter as the first secondary source of the BITS clock.
Step 6	exit Example: ITP(config-controller)# exit	Exits from controller configuration mode to global configuration mode.
Step 7	controller t1 slot/port-adapter-num/port Example: ITP(config)# controller t1 2/0/2	Specifies controller 2 on the SS7 port adapter and enters controller configuration mode.

	Command	Purpose
Step 8	clock source {bits {primary secondary priority} internal line {primary secondary priority}} Example: ITP(config-controller)# clock source internal	Specifies controller 2 internal clocking. Note This controller will provide BITS clock to the high speed links via the T1 crossover cable to the SS7 ATM port adapter.
Step 9	exit Example: ITP(config-controller)# exit	Exits from controller configuration mode to global configuration mode.

The following task enables an ATM interface to receive BITS clocking for HSLs.

After you configure BITS clocking on the SS7 port adapter controllers and connect the primary BITS clock from the SS7 port adapter to the IMA port adapter, you configure the ATM interfaces on the IMA port adapter to receive the BITS clock.


Note

A T1 crossover cable delivers the BITS clock from the configured SS7 port adapter controller to this interface. This interface will relay the BITS clock to every other ATM interface that is configured with **clock source common interface-num**, where *interface-num* is the interface physically connected to the SS7 PA. Because this interface is receiving the BITS clock from the SS7 PA, it cannot be used as an SS7 link to send or receive traffic. It is reserved for receiving and distributing the BITS clock to the other interfaces on the IMA PA. Also, the clock source on this interface must be configured as **clock source line**. This is the default, so you do not need to add this command unless it was previously set to some other value. If you are not sure, the output of the **show running-config** command will indicate if the clock source for this interface is configured for a value other than line. (Default states are not shown in the show run output.)

To enable an ATM interface to receive BITS clocking for HSLs, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	<code>interface atm interface-num</code>	Specifies ATM interface 12/0/0 and enters interface configuration mode.
Step 2	Example: <pre>ITP(config)# interface atm 12/0/0</pre> <pre>no ip address no ima-group no atm ilmi-keepalive exit</pre> Example: <pre>ITP(config-if)# no ip address ITP(config-if)# no ima-group ITP(config-if)# no atm ilmi-keepalive ITP(config-if)# exit</pre>	Disables IP addressing. Disables inverse multiplexing over ATM (IMA) group. Disables ILMI keepalives. Exits from interface configuration mode to global configuration mode.
Step 3	<code>interface atm interface-num</code>	Specifies ATM interface 12/0/1 and enters interface configuration mode.
Step 4	<code>clock source {common [interface-num] internal line}</code> Example: <pre>ITP(config-if)# clock source common 0</pre>	Specifies that this interface will receive the common BITS clock resource. Note Steps 3 - 4 can be repeated as needed to configure ATM interfaces. The ATM physically connected to the SS7 PA (in this case atm 12/0/0 will relay the BITS clock to every ATM interface that is configured with clock source common interface-num, where <i>interface-num</i> is the interface physically connected to the SS7 PA).

**Caution**

You cannot configure the clock source for an ATM interface when the interface is in the administratively down state. The clock source may revert to the original clock source when the interface becomes active.

**Caution**

The Cisco VWIC-2T1/E1-RAN is required for SS7 low-speed links. SS7 low-speed links are not supported using any other VWIC.

Configuring Local Peers

A Cisco ITP peer has two end-points: a local end-point and a remote end-point. (Peer end-points are also referred to as *instances*.) A local peer is the local end-point for SS7 over IP with Stream Control Transmission Protocol (SCTP) connections¹.

A local peer is identified by its local-port-number. You must configure one (and may configure up to four) local IP address for each local-peer. Cisco ITP will use one of the four local IP addresses for a primary local end-point instance and use the other three IP addresses as backups.

The M2PA/SCTP protocol can be offloaded onto a enabling management of peer links on the and freeing the CPU for MTP3 management and routing.

To configure the local peer, and, optionally, configure M2PA/SCTP offload, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	cs7 local-peer <i>local-port-number</i> offload <i>slot bay</i>	Specifies the local peer and puts you in local-peer submenu.
	Example: ITP(config)# cs7 local-peer 7000	
Step 2	local-ip <i>address</i>	Configures the IP address for this local peer instance. You can repeat this step to configure backup IP addresses for this local end-point.
	Example: ITP(config-cs7-lp)# local-ip 172.18.44.242	

Configuring Linksets

A link is either a serial or ATM interface or a peer (virtual link) to a remote Cisco ITP node. Multiple links are grouped into a linkset. Each link must be assigned to one linkset, and multiple links can be assigned to a linkset. Links within the same linkset must be parallel between the same nodes.

To configure a linkset you must name the linkset and specify the point code of the adjacent signaling point.



Note

You must specify the SS7 variant and the point code before you can configure linksets.



Note

To avoid unnecessary CPU load, we recommend that you shut down interfaces that are configured but not provisioned as part of a linkset.



Note

Avoid manual configuration of linksets when a MTP3 restart is in progress.

1. For more information, refer to Stream Control Transmission Protocol, RFC 2690.

To specify a linkset, use the following command in global configuration mode:

Command	Purpose
cs7 [instance <i>instance-number</i>] linkset <i>ls-name adj-pc</i> [local-pc [<i>pc</i>]] Example: ITP(config)# cs7 linkset LINKSET1 2.2.2	To specify a linkset and enter CS7 linkset submode.

Configuring Circular Route Direction (CRD)

Circular routing is when an MSU flows through an SS7 network and ends up back at the originating point code (OPC). Circular routes can quickly lead to congestion of links and degrade network performance. SS7 messages do not have time-to-live or hop counter features, which help stop circular routing in some other protocols, so another way is needed to detect and stop the problem. If the problem is not detected and stopped, a MSU can continue on indefinitely. The CRD feature detects circular routing and disables these problematic routes. These problematic routes are usually caused by an incorrect router configuration.

Configuring CRD for the ANSI Variant

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no cs7 mtp3 crd**
4. **cs7 linkset**
5. **c-link-linkset**
6. **cs7 mtp3 crd**
7. **cs7 mtp3 timer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: ITP> enable	Enables privileged EXEC mode.
Step 2	configure terminal Example: ITP# configure terminal	Enters global configuration mode.
Step 3	no cs7 [instance <i>instance-number</i>] mtp3 crd Example: ITP(config)# no cs7 mtp3 crd	Turns off CRD.
Step 4	cs7 [instance <i>instance-number</i>] linkset <i>ls-name</i> <i>adj-pc</i> [local-pc [<i>pc</i>]] Example: ITP(config)# cs7 linkset LINKSET1 2.2.2	(Optional) Specifies a linkset and puts you in linkset configuration mode.  Note This step is not necessary if there are no C-links in the ITP.

	Command or Action	Purpose
Step 5	c-link-linkset [secondary] Example: ITP(config-cs7-ls)# c-link-linkset	(Optional) Tags a linkset as a C-link linkset. secondary —(Optional) C-link linkset to the connected secondary PC.  Note This step is not necessary if there are no C-links in the ITP.  Note CRD also controls OPC Verification. One of the checks done during OPC Verification is if an MSU with OPC equal to the mate's PC arrives on a linkset that is not the C-link linkset, then that MSU is discarded. That makes it necessary to identify the linksets as C-link linksets before the CRD feature is turned on. This step accomplishes that.
Step 6	exit Example: ITP(config-cs7-ls)# exit	Returns to the global configuration mode.
Step 7	cs7 [instance <i>instance-number</i>] mtp3 crd Example: ITP(config)# cs7 mtp3 crd	Turns on CRD and OPC verification. The default for the ANSI variant is CRD on. The default for all other variants is CRD off.
Step 8	cs7 [instance <i>instance-number</i>] mtp3 timer tloop msec Example: ITP(config)# cs7 mtp3 timer tloop 10000	Globally configures the ITP MTP3 management timers. tloop msec —The loop detection timer. The timer value is in the range 10000-20000 msec. The default value is 10000 msec.

Configuring CRD for the ITU and ITU-like Variants

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cs7 national-options multiple-congestion**
4. **cs7 linkset**
5. **c-link-linkset**
6. **cs7 mtp3 crd**
7. **cs7 mtp3 timer**

DETAILED STEPS

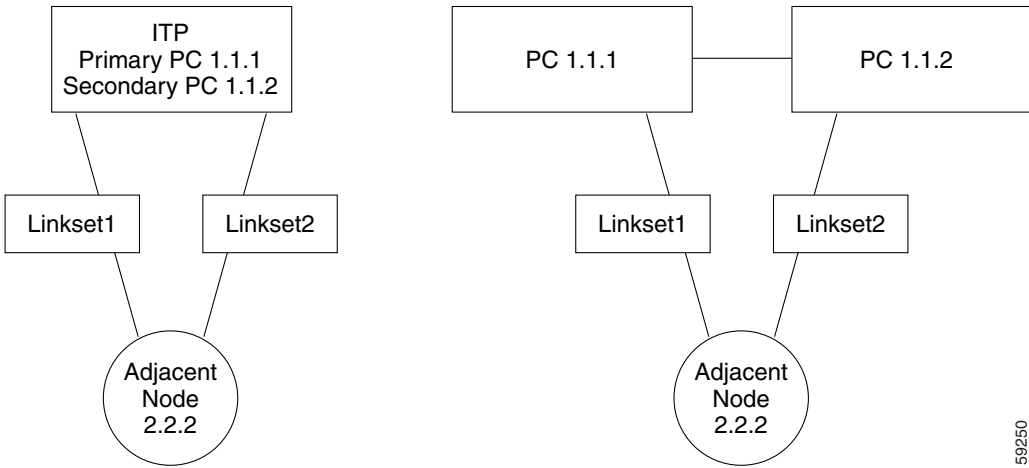
	Command or Action	Purpose
Step 1	enable Example: ITP> enable	Enables privileged EXEC mode.
Step 2	configure terminal Example: ITP# configure terminal	Enters global configuration mode.
Step 3	cs7 [instance instance-number] national-options multiple-congestion Example: ITP(config)#cs7 national-options multiple-congestion	Specifies the national option. There must be support for multiple congestion levels in the network for CRD and OPC Verification to work.
Step 4	no cs7 [instance instance-number] mtp3 crd Example: ITP(config)# no cs7 mtp3 crd	Turns off CRD.
Step 5	cs7 [instance instance-number] linkset ls-name adj-pc [local-pc [pc]] Example: ITP(config)# cs7 linkset LINKSET1 2.2.2	(Optional) Specifies a linkset and puts you in linkset configuration mode.  Note This step is not necessary if there are no C-links in the ITP.
Step 6	c-link-linkset [secondary] Example: ITP(config-cs7-ls)# c-link-linkset	(Optional) Tags a linkset as a C-link linkset. secondary —(Optional) C-link linkset to the connected secondary PC.  Note This step is not necessary if there are no C-links in the ITP.
Step 7	exit Example: ITP(config-cs7-ls)# exit	Returns to the global configuration mode.

	Command or Action	Purpose
Step 8	cs7 [instance <i>instance-number</i>] mtp3 crd Example: ITP(config)# cs7 mtp3 crd	Turns on CRD and OPC verification. The default for the ANSI variant is CRD on. The default for all other variants is CRD off.
Step 9	cs7 [instance <i>instance-number</i>] mtp3 timer tloop msec Example: ITP(config)# cs7 mtp3 timer tloop 10000	Globally configures the ITP MTP3 management timers. tloop msec —The loop detection timer. The timer value is in the range 10000-20000 msec. The default value is 10000 msec.

Configuring Multiple Linksets to Adjacent Nodes

This optional feature allows you to configure 2 linksets between the ITP and an adjacent node. Each linkset can have 16 links, so a total of 32 links can be configured between an ITP and an adjacent node. To the adjacent node, it appears that it is connected to two different ITPs. Figure 5 represents the actual network on the left and the adjacent node’s view of the network on the right. Point codes 1.1.1 and 1.1.2 appear to be two separate nodes, but they are actually the same ITP.

Figure 5 Multiple Linksets



Before you can configure multiple linksets to an adjacent node, you must add a secondary local point code to the ITP. (This was discussed in an earlier section.) If you have not already done so, configure a secondary point code using the following command in global configuration mode:

Command	Purpose
cs7 secondary-pc <i>point-code</i> Example: ITP(config)# cs7 secondary-pc 1.1.2	Specifies a second point code for the ITP.

Configure two linksets between the ITP and the adjacent node, using the following commands in global configuration mode:

Command	Purpose
<code>cs7 linkset ls-name adjacent-point-code [local-pc primary-point-code]</code>	Specifies a linkset between the adjacent point code and the ITP primary point code and enters linkset configuration mode. If the [local-pc primary-point-code] option is omitted, the primary local point code is used on this linkset. If the [local-pc primary-point-code] is specified, either primary or secondary point code can be explicitly assigned to the linkset.
Example: ITP(config)# cs7 linkset LINKSET1 2.2.2 ITP(config-cs7-ls)exit ITP(config)# cs7 linkset LINKSET2 2.2.2	

The combination of adjacent point code and local point code must be unique. So for any adjacent point code, the user can configure two linksets - one using the primary local pc, and one using the secondary pc. An example of configuring this is:

```
cs7 linkset LINKSET1 2.2.2 local-pc 1.1.1
  link 0 serial 1/1/1:0
  ..
  link 15 serial 1/1/1:15

cs7 linkset LINKSET2 2.2.2 local-pc 1.1.2
  link 0 serial 1/1/2:0
  ..
  link 15 serial 1/1/2:15
```

The two linksets to the adjacent node are automatically entered as a combined route to the adjacent node. Traffic going to the adjacent node will be divided between the two linksets based on SLS.



Note

In ANSI, if the two linksets each have 16 links, traffic is automatically distributed across all 32 links based on SLS. In ITU, because there are only 16 SLS combinations, only half the links would carry traffic in the default configuration. If the traffic is SCCP unsequenced, you can configure the **cs7 distribute-sccp-unsequenced** command, and the ITP will then use all 32 links.

Specifying the Cisco ITP Route Table

The Cisco ITP uses a route table to select the appropriate signaling path for each message, or signal unit, that it must forward. The route table maps the destination point code (DPC) of the message to an output linkset name that is used to forward the packet.

Specifying the Default Route Table

On the Cisco ITP router, a route table named “system” is configured by default. The system route table keeps a record of routes to all adjacent signaling points. To specify the Cisco ITP route table, use this command in global configuration mode:

Command	Purpose
cs7 route-table <i>rt-name</i>	Specifies the name of the route table and enters route table mode.
Example: ITP(config)# cs7 route-table system	



Note You must specify **system** as the route table name (*rt-name*).

Loading the Route Table Contents

Route table contents can be loaded from a URL where a binary version of the route table is located. To add route table contents, use this command in route table configuration mode:

Command	Purpose
load { flash ftp rtp tftp } <i>URL</i>	Loads the contents of the route table.
Example: ITP(config-cs7-rt)# load tftp://64.102.16.25/route.txt	



Note Whenever any change is made in the routing configuration of an instance, save the routing configuration and perform any load operation for only that particular instance.

Adding Routes to the Route Table

Additional routes can be added to the system route table. To update a Cisco ITP route table, use the **update route** command in CS7 route table configuration mode:

Command	Purpose
update route <i>point-code</i> [<i>mask</i> <i>length</i>] linkset <i>ls-name</i> [priority <i>priority-value</i> ¹] [qos-class { <i>class</i> default }] [load_balance]	Updates a route in the routing table.
Example: ITP(config-cs7-rt)# update route 1.50.2 255.255.255 linkset nyc	

1. The smaller the number, the higher the priority. See the **update route** ITP Command Set entry for an example.

Saving the Route Table

You can save an active route table into a file. The newly created file can be used with the **load** route-table sub-command to populate the route table upon ITP startup. Note that all **update route** or **remove route** route-table sub-commands are removed from the system configuration after the save is completed. This is done because those commands have been applied to the actual route-table *before* the save, and are therefore included in the saved file.

We recommend that you save the router configuration to non-volatile memory after generating a new route-table file because the configuration has changed (update/remove route commands may have been removed from the configuration).

Update/remove routes are saved in the system configuration. Therefore, to load a file from disk, it is recommended to save the current route-configuration to disk so that the current update/remove commands are not reapplied on file load.



Note

If the routing table configuration is loaded using a file, ensure this file exists on both Active and Standby supervisor modules before reloading the ITP.

To save an active route table to a file, use the following command in privileged EXEC mode:

Command	Purpose
<code>cs7 save route-table name url</code>	Save the route table to a file.
Example: <pre>ITP# cs7 save route-table testtable flash:testtable</pre>	

Assigning Links to Linksets

After specifying linksets, you can assign links to the linkset. You will assign links to adjacent legacy SS7 devices as well as links to adjacent Cisco ITP peer nodes.

Traditional SS7 Links

You must configure a link to the legacy SS7 devices. To configure an SS7 link within a linkset, make sure that the interface encapsulation is MTP2, then use the following command in linkset configuration mode:

Command	Purpose
<code>link slc serial number</code>	Configures an SS7 link within a linkset and enters CS7 link configuration mode.
Example: <pre>ITP(config-cs7-ls)#</pre>	

High-Speed Signaling Links

You must configure a link to HSL devices. To configure an HSL link within a linkset, make sure that the ATM interface has NNI selected and a QSAAL PVC defined, then use the following command in linkset configuration mode:

Command	Purpose
link slc atm interface-number[.subinterface-number]	Configures a link to an HSL device and enters CS7 link configuration mode.
Example: ITP(config-cs7-ls)#	

SS7 Over IP Links (Peers)

A Cisco ITP peer has two end-points: a local and a remote end-point.

The local end-point is identified by the local-port-number, which you specified earlier with the **cs7 local-peer** *local-port-number* command.

The remote end-point is simply the local-peer on a remote router. In the link definition shown in the following task table, the remote router's *local-port-number* is the *remote-port-number* and the (up to) four IP addresses of the remote router's local-peer are the *remote-ip-addrs*.

The **passive** keyword (which is optional) can be used to indicate that the remote router must establish the peer connection.



Note

IP routing is automatically enabled in the ITP and should not be disabled. If IP routing has been disabled, process suspending behavior can occur in M2PA, M3UA, or SUA configurations. To re-enable IP routing if it has been disabled, use the **ip routing** command in global configuration mode.

To configure an SS7 link within a linkset, use the following command in linkset configuration mode:

Command	Purpose
link slc sctp remote-ip-addr [backup-remote-ip-addr ...] remote-port-num ¹ local-port-num [passive]	Configures SS7 over IP peers for a linkset and enters Cisco CS7 link configuration mode.
Example: ITP(config-cs7-ls)#	

1. remote-port-num is the local port number of the adjacent Cisco ITP peer.

There are several SCTP parameters that you can adjust, such as tuning SCTP parameters for satellite channels. Tasks and commands to tune timers and SCTP parameters are described in the [“Tuning ITP” section on page 394](#) of the “Verifying, Monitor, and Tuning ITP” chapter.

Shutting Down and Restarting Linksets and Links

To inhibit a link, use the following commands in EXEC mode:

Command	Purpose
cs7 inhibit linkset link Example: ITP# cs7 inhibit nyc 3	Takes a link out of service without risking loss of connectivity.
cs7 uninhibit linkset link Example: ITP# cs7 uninhibit nyc 3	Returns the link to service.

To disable or reactivate a linkset, use one of the following commands, beginning in global configuration mode:

Command	Purpose
cs7 linkset ls-name point-code Example: ITP(config)# cs7 linkset nyc 1.1.0	Specifies a linkset and puts you in linkset configuration mode.
shutdown Example: ITP(config-cs7-ls)# shutdown	Disables the linkset.
ITP(config-ls)# no shutdown Example: ITP(config-cs7-ls)# no shutdown	Brings the linkset back into the active state.

To disable or reactivate a link, use the following commands, beginning in global configuration mode:

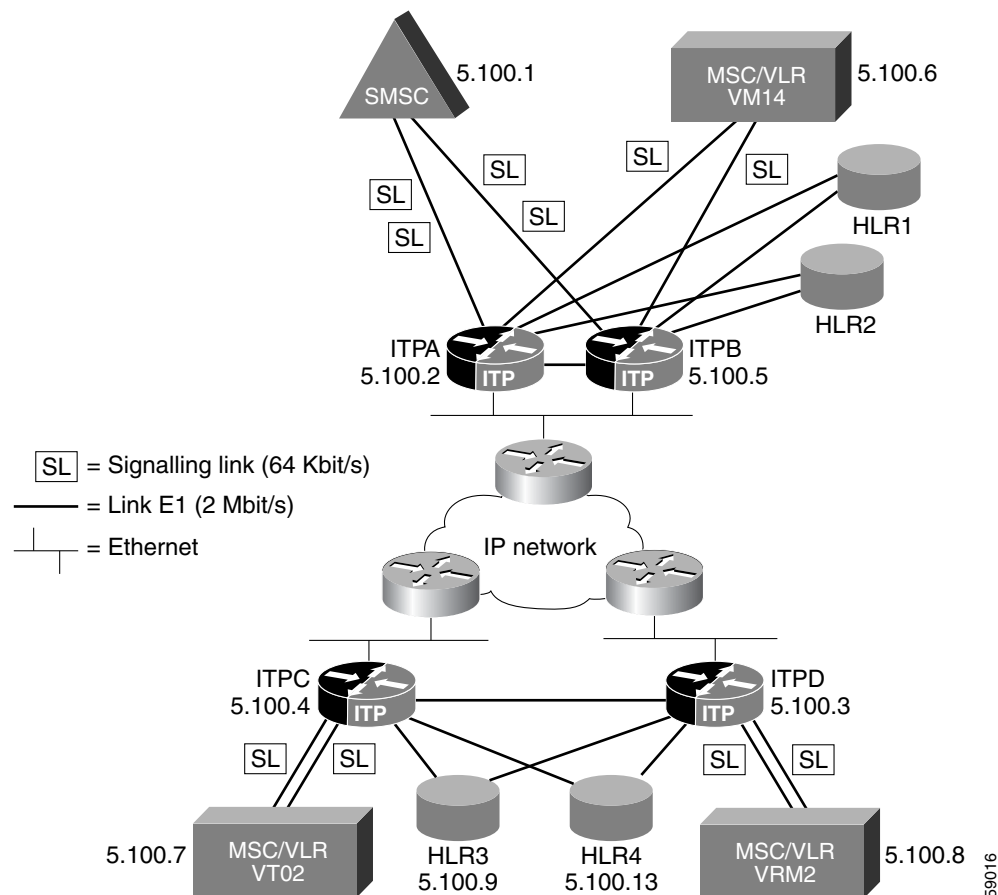
Command	Purpose
cs7 linkset ls-name point-code Example: ITP(config)# cs7 nyc 1.1.0	Specifies a linkset and puts you in linkset configuration mode.
link slc -OR- link slc sctp remote-peer remote-instance local-instance [passive] Example: ITP(config-cs7-ls)# link 3	Specifies a link and puts you in link configuration mode.

Command	Purpose
shutdown	Disables the link.
Example: ITP(config-cs7-ls)# shutdown	
no shutdown	Brings the link back into the active state.
Example: ITP(config-cs7-ls)# no shutdown	

Configuration Example of ITP Basic Functionality

This configuration example describes the basic ITP functions. Four Cisco ITPs are configured. The network configuration is illustrated in [Figure 6](#).

Figure 6 ITPs as STPs in an SS7oIP Topology



Assumptions:

All routers have redundant ethernet connectivity and therefore all SCTP associations use two IP addresses (multi-homing).

Point codes and IP addresses for ITP routers:

```
ITPA  5.100.2  172.18.44.242 117.117.117.2
ITPB  5.100.5  172.18.44.243 117.117.117.3
ITPC  5.100.4  172.18.45.1  117.117.119.4
ITPD  5.100.3  172.18.46.1  117.117.118.4
```

Point codes for SS7 SSPs:

```
SMSC  5.100.1
VMI4   5.100.6
VT02   5.100.7
VRM2   5.100.8
```

ITP Basic Configuration for ITPA

```
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ITPA
!
enable secret 5 $1$iBmo$AF1H6u2CVGDRM5BMeuGmx/
enable password lab
!
!
no ip cef
no ip finger
no ip domain-lookup
!
cs7 variant itu
cs7 point-code 5.100.2
!
!
controller E1 1/0/0
    channel-group 0 timeslots 1
!
controller E1 1/0/1
    channel-group 0 timeslots 1
!
controller E1 2/0/0
    channel-group 0 timeslots 1
!
!
interface FastEthernet0/0/0
    ip address 172.18.44.242 255.255.255.128
    no ip route-cache distributed
    no ip route-cache
    no ip mroute-cache
!
interface FastEthernet0/0/1
    ip address 117.117.117.2 255.255.255.0
    no ip route-cache distributed
    no ip route-cache
    no ip mroute-cache
!
interface Serial1/0/0:0
    no ip address
```

```
encapsulation mtp2
no ip route-cache distributed
no ip route-cache
load-interval 30
!
interface Serial1/0/1:0
no ip address
encapsulation mtp2
no ip route-cache distributed
no ip route-cache
load-interval 30
!
interface Serial2/0/0:0
no ip address
encapsulation mtp2
no ip route-cache distributed
no ip route-cache
load-interval 30
!
cs7 local-peer 7000
local-ip 172.18.44.242
local-ip 117.117.117.2
!
!
! Routes using linksets to ITPC and ITPD have a default
! priority of 5. Routes to adjacent node SMS-C and VMI4
! are inserted by the systems with priority 5 and when
! the linkset is configured. They don't have to be defined
! here. Backup-routes to SMS-C and VMI4 are inserted with
! priority 9 using the "C-Link".
!
cs7 route-table system
update route 5.100.7 7.255.7 linkset ITPc
update route 5.100.8 7.255.7 linkset ITPd
update route 5.100.1 7.255.7 linkset ITPb priority 9
update route 5.100.6 7.255.7 linkset ITPb priority 9
!
cs7 linkset ITPc 5.100.4
accounting
link 0 sctp 172.18.45.1 117.117.119.4 7000 7000

!
cs7 linkset ITPd 5.100.3
accounting
link 0 sctp 172.18.46.1 117.117.118.4 7000 7000

!
cs7 linkset smsc 5.100.1
accounting
link 0 Serial1/0/0:0
link 1 Serial2/0/0:0

!
cs7 linkset vmi4 5.100.6
accounting
link 0 Serial1/0/1:0

!
cs7 linkset ITPb 5.100.5
accounting
link 0 sctp 172.18.44.243 117.117.117.3 7000 7000

!
ip classless
```

```
no ip http server
!  
!  
!  
line con 0  
  transport input none  
line aux 0  
line vty 0 4  
  password lab  
  login  
!  
end
```

ITP Basic Configuration for ITPB

```
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ITPB
!
enable secret 5 $1$iBmo$AFlH6u2CVGDRM5BMeuGmx/
enable password lab
!
!
!
!
!
no ip cef
no ip finger
no ip domain-lookup
!
cs7 variant itu
cs7 point-code 5.100.3
!
!
controller E1 1/0/0
    channel-group 0 timeslots 1
!
controller E1 1/0/1
    channel-group 0 timeslots 1
!
controller E1 2/0/0
    channel-group 0 timeslots 1
!
!
interface FastEthernet0/0/0
    ip address 172.18.44.243 255.255.255.128
    no ip route-cache distributed
    no ip route-cache
    no ip mroute-cache
!
interface FastEthernet0/0/1
    ip address 117.117.117.3 255.255.255.0
    no ip route-cache distributed
    no ip route-cache
    no ip mroute-cache
!
interface Serial1/0/0:0
    no ip address
    encapsulation mtp2
    no ip route-cache distributed
    no ip route-cache
    load-interval 30
!
interface Serial1/0/1:0
    no ip address
    encapsulation mtp2
    no ip route-cache distributed
    no ip route-cache
    load-interval 30
!
interface Serial2/0/0:0
    no ip address
    encapsulation mtp2
```

```

no ip route-cache distributed
no ip route-cache
load-interval 30
!
cs7 local-peer 7000
local-ip 172.18.44.243
local-ip 117.117.117.3
!
! Routes using linksets to ITPC and ITPD have a default
! priority of 5. Routes to adjacent node SMS-C and VMI4
! are inserted by the systems with priority 5 and when
! the linkset is configured. They don't have to be defined
! here. Backup-routes to SMS-C and VMI4 are inserted with
! priority 9 using the "C-Link".
!
cs7 route-table system
update route 5.100.7 7.255.7 linkset ITPc
update route 5.100.8 7.255.7 linkset ITPd
update route 5.100.1 7.255.7 linkset ITPa priority 9
update route 5.100.6 7.255.7 linkset ITPa priority 9
!
cs7 linkset ITPc 5.100.4
accounting
link 0 sctp 172.18.45.1 117.117.119.4 7000 7000

!
cs7 linkset ITPd 5.100.3
accounting
link 0 sctp 172.18.46.1 117.117.118.4 7000 7000

!
cs7 linkset smsc 5.100.1
accounting
link 0 Serial11/0/0:0
link 1 Serial2/0/0:0

!
cs7 linkset vmi4 5.100.6
accounting
link 0 Serial11/0/1:0

!
cs7 linkset ITPa 5.100.2
accounting
link 0 sctp 172.18.44.242 117.117.117.2 7000 7000

!
ip classless
no ip http server
!
!
!
line con 0
transport input none
line aux 0
line vty 0 4
password lab
login
!
end
!

```

ITP Basic Configuration for ITPC

```
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ITPC
!
enable secret 5 $1$iBmo$AFlH6u2CVGDRM5BMeuGmx/
enable password lab
!
!
!
!
!
no ip cef
no ip finger
no ip domain-lookup
!
cs7 variant itu
cs7 point-code 5.100.4
!
!
controller E1 1/0/0
    channel-group 0 timeslots 1
!
controller E1 2/0/0
    channel-group 0 timeslots 1
!
!
interface FastEthernet0/0/0
    ip address 172.18.45.1 255.255.255.128
    no ip route-cache distributed
    no ip route-cache
    no ip mroute-cache
!
interface FastEthernet0/0/1
    ip address 117.117.119.4 255.255.255.0
    no ip route-cache distributed
    no ip route-cache
    no ip mroute-cache
!
interface Serial1/0/0:0
    no ip address
    encapsulation mtp2
    no ip route-cache distributed
    no ip route-cache
    load-interval 30
!
interface Serial2/0/0:0
    no ip address
    encapsulation mtp2
    no ip route-cache distributed
    no ip route-cache
    load-interval 30
!
cs7 local-peer 7000
    local-ip 172.18.45.1
    local-ip 117.117.119.4
!
!
! Routes to SMS-C and VMI4 use a combined linkset.
```

```

! This is defined by inserting two routes with
! identical priority (5 is default).
!
cs7 route-table system
  update route 5.100.1 7.255.7 linkset ITPa
  update route 5.100.1 7.255.7 linkset ITPb
  update route 5.100.6 7.255.7 linkset ITPa
  update route 5.100.6 7.255.7 linkset ITPb
  update route 5.100.8 7.255.7 linkset ITPd
!
cs7 linkset ITPa 5.100.2
  accounting
  link 0 sctp 172.18.44.242 117.117.117.2 7000 7000

!
cs7 linkset ITPb 5.100.5
  accounting
  link 0 sctp 172.18.44.243 117.117.117.3 7000 7000

!
cs7 linkset ITPd 5.100.3
  accounting
  link 0 sctp 172.18.46.1 117.117.118.4 7000 7000

!
cs7 linkset vt02 5.100.7
  accounting
  link 0 Serial11/0/0:0
  link 1 Serial12/0/0:0

!
ip classless
no ip http server
!
!
!
line con 0
  transport input none
line aux 0
line vty 0 4
  password lab
  login
!
end

```


ITP Basic Configuration for ITPD

```
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ITPD
!
enable secret 5 $1$iBmo$AFlH6u2CVGDRM5BMeuGmx/
enable password lab
!
!
!
!
!
no ip cef
no ip finger
no ip domain-lookup
!
cs7 variant itu
cs7 point-code 5.100.3
!
!
controller E1 1/0/0
    channel-group 0 timeslots 1
!
controller E1 2/0/0
    channel-group 0 timeslots 1
!
!
interface FastEthernet0/0/0
    ip address 172.18.46.1 255.255.255.128
    no ip route-cache distributed
    no ip route-cache
    no ip mroute-cache
!
interface FastEthernet0/0/1
    ip address 117.117.118.4 255.255.255.0
    no ip route-cache distributed
    no ip route-cache
    no ip mroute-cache
!
interface Serial1/0/0:0
    no ip address
    encapsulation mtp2
    no ip route-cache distributed
    no ip route-cache
    load-interval 30
!
interface Serial2/0/0:0
    no ip address
    encapsulation mtp2
    no ip route-cache distributed
    no ip route-cache
    load-interval 30
!
cs7 local-peer 7000
    local-ip 172.18.46.1
    local-ip 117.117.118.4
!
!
! Routes to SMS-C and VMI4 use a combined linkset.
```

```

! This is defined by inserting two routes with
! identical priority (5 is default).
!
cs7 route-table system
  update route 5.100.1 7.255.7 linkset ITPa
  update route 5.100.1 7.255.7 linkset ITPb
  update route 5.100.6 7.255.7 linkset ITPa
  update route 5.100.6 7.255.7 linkset ITPb
  update route 5.100.7 7.255.7 linkset ITPc
!
cs7 linkset ITPa 5.100.2
  accounting
  link 0 sctp 172.18.44.242 117.117.117.2 7000 7000

!
cs7 linkset ITPb 5.100.5
  accounting
  link 0 sctp 172.18.44.243 117.117.117.3 7000 7000

!
cs7 linkset ITPd 5.100.4
  accounting
  link 0 sctp 172.18.45.1 117.117.119.4 7000 7000

!
cs7 linkset vrm2 5.100.8
  accounting
  link 0 Serial1/0/0:0
  link 1 Serial2/0/0:0

!
ip classless
no ip http server
!
!
!
line con 0
  transport input none
line aux 0
line vty 0 4
  password lab
  login
!
end

```



Probeless Monitoring

With Probeless Monitoring enabled, the ITP sends packets to an external server. The packets sent to this server contain copies of any MSUs received or sent by the ITP.

Feature History for Probeless Monitoring

Release	Modification
12.2(33)IRC	This feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



Note

Configuration Mode Restrictions: Simultaneous changes to the configuration from multiple CLI sessions are not supported. Only one configuration session is allowed to enter in configuration mode at a time; other sessions should not enter in configuration mode. The **show line** or **show users EXEC** command may be used to determine the active user sessions on an ITP, and the **clear line EXEC** command may be used to ensure that only a single active session exists.

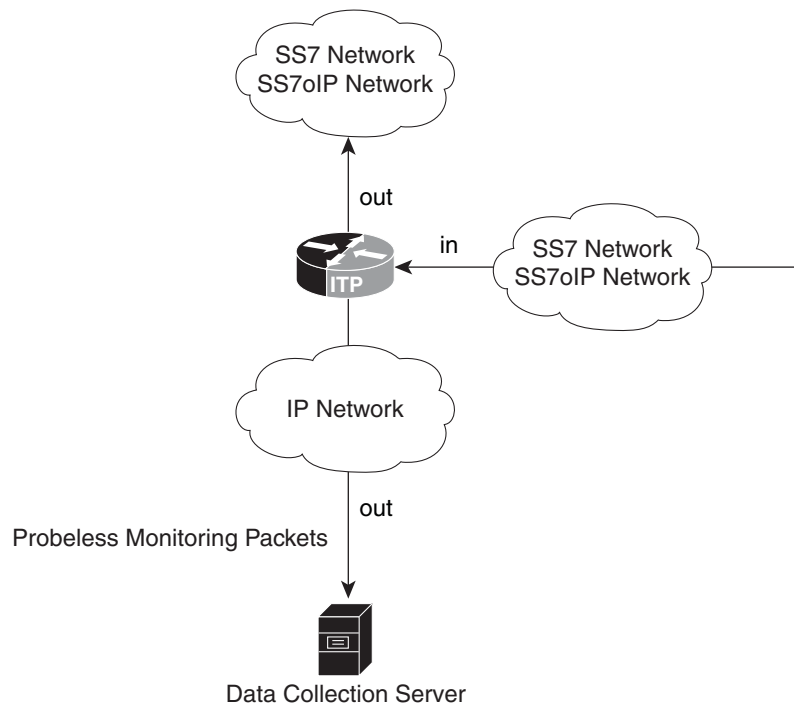
Contents

- [Information About Probeless Monitoring, page 54](#)
- [How to Configure Probeless Monitoring, page 54](#)
- [Verifying the Probeless Monitoring Configuration, page 62](#)
- [Configuration Example for Probeless Monitoring, page 62](#)

Information About Probeless Monitoring

The basics of Probeless Monitoring are shown in [Figure 7](#), where the ITP performs its normal role and Probeless Monitoring uses the IP network to send packets to a data collection server (DCS). The packets contain copies of the MSUs from the linksets and ASs of an SS7oIP network and/or copies of the MSUs from the linksets of an SS7 network. These MSU copies are encapsulated in a proprietary Probeless Monitoring protocol (PMP), which is stacked on UDP and transmitted over a non-reliable IP stream.

Figure 7 *Probeless Monitoring*



The DCS servers are also known as DCS nodes and serve as endpoints in the IP network that carries the PMP packets. These DCS nodes may have up to two unique IP addresses and/or ports assigned. The DCS nodes make up a DCS group, which contains a maximum of eight of these DCS nodes. Sixteen DCS groups are the maximum for an ITP.

Other characteristics of Probeless Monitoring are that ITP monitors the path to the remote DCS IP address with Internet Control Message Protocol (ICMP) echo packets, and that the loadsharing algorithm among DCS nodes of a DCS group is least cost according to round-robin scheduling. The congestion avoidance algorithm is based on Java remote method invocation (RMI). You can also enable Probeless Monitoring globally or specifically for a particular linkset or application server (AS).

How to Configure Probeless Monitoring

This section include the following tasks and information:

- [Configuring Global Probeless Monitoring, page 55](#)
- [Configuring Hold Queue and Congestion Timer, page 56](#)
- [Configuring a DCS Node, page 56](#)

- [Configuring a DCS Group, page 59](#)
- [Configuring Probeless Monitoring for a Specific Linkset, page 60](#)
- [Configuring Probeless Monitoring for a Specific AS, page 61](#)

Configuring Global Probeless Monitoring

When global Probeless Monitoring is off (default), it disables copying at a system level and overrides all provisioned linkset and AS pmp settings. You need to manually enable Probeless Monitoring at the system level to activate all sub-tending linkset and AS pmp settings. [Table 3](#) below defines this behavior:

Table 3 Global Probeless Monitoring Behavior for Linkset and AS PMP Settings

CS7 PMP	Linkset/AS PMP	Result
On	On	On
On	Off	Off
Off	On or Off	Off

To enable Probeless Monitoring globally, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cs7 pmp**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: ITP> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: ITP# configure terminal	Enters global configuration mode.
Step 3	cs7 pmp Example: ITP(config)# cs7 pmp	Turns Probeless Monitoring on for all linksets and AS.

Configuring Hold Queue and Congestion Timer

The congestion timer is used in conjunction with the hold queue to control the congestion of PMP packets. When PMP packets in the hold queue hit the congestion onset threshold, a congestion timer with a range of 0 to 60 seconds starts. Before the timer expires, the receiving side of PMP will be disabled. When the timer expires, the congestion status is checked based on the queue length against the abate threshold.

To enable the hold queue and congestion timer, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cs7 pmp hold-queue**
4. **cs7 pmp congestion-timer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: ITP> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: ITP# configure terminal	Enters global configuration mode.
Step 3	cs7 pmp hold-queue <i>abate-threshold onset-threshold</i> Example: ITP(config)# cs7 pmp hold-queue 256 512	(Optional) Controls the congestion of PMP packets.
Step 4	cs7 pmp congestion-timer <i>timer</i> Example: ITP(config)# cs7 pmp congestion-timer 60	(Optional) Set the integer range of the PMP congestion timer.

Configuring a DCS Node

A DCS node represents a PMP endpoint and is uniquely identified by name, IP address, and port number. Each DCS node may contain up to two IP addresses and port combinations. You can also configure other characteristics of the DCS node, including:

- The interval between two consecutive ICMP Echo requests
- The number of times the ITP will retry the ping before marking the DCS node as unavailable
- The optional calculation of a UDP checksum sent in the PMP stream

- The encapsulation MSU data format of the egress PMP packets
- The sending of PMP packets and pings to the DCS

Restrictions

The following list identifies restrictions to a DCS Node:

- The remote IP address must be unique for the DCS node.
- The local IP address must be reachable.
- The local/remote IP addresses can only change when the DCS is not part of any DCS group.
- You cannot delete a DCS node referenced by a DCS group.
- You need to shut down the DCS node before deleting its local/remote IP addresses.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cs7 dcs** *name*
4. **remote-ip** *ip_addr1* [*ip_addr2*] *port*
5. **local-ip** *ip_addr* *port*
6. **ping-interval** *sec*
7. **timeout-count** *count*
8. **udp-checksum**
9. **emdt** [*emdt1* | *emdt2*]
10. **shutdown**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: ITP> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: ITP# configure terminal	Enters global configuration mode.
Step 3	cs7 dcs <i>name</i> Example: ITP(config)# cs7 dcs dcs1	Identifies a name to be associated with this DCS and enters cs7 dcs configuration submenu.

	Command or Action	Purpose
Step 4	remote-ip <i>ip_addr1</i> [<i>ip_addr2</i>] <i>port</i> Example: <pre>ITP(config-cs7-dcs)# remote-ip 209.165.201.31 209.165.201.28 33500</pre>	Configures an IP address(s) and a port(s) for a DCS node. • <i>addr1</i>—A v4 IP address in the form xxx.xxx.xxx.xxx. It is the primary IP address used when sending PMP traffic. • <i>addr2</i>(Optional)—A v4 IP address in the form xxx.xxx.xxx.xxx. It is a redundant IP address used when the primary IP address fails. • <i>port</i>—IP address port with an integer range of 1-65535 for remote port and 1024-65535 for local port.
Step 5	local-ip <i>ip_addr</i> <i>port</i> <pre>ITP(config-cs7-dcs)# local-ip 209.165.201.28 33500</pre>	Configures a local IP address used to send PMP or UDP to DCS nodes.  Note Multiple DCS nodes may have the same local IP address and port combination.
Step 6	ping-interval <i>sec</i> Example: <pre>ITP(config-cs7-dcs)# ping-interval 5</pre>	(Optional) Sets the interval between pings to the DCS nodes' IP addresses. • <i>sec</i>—Length of time in seconds.
Step 7	timeout-count <i>count</i> Example: <pre>ITP(config-cs7-dcs)# timeout-count 3</pre>	(Optional) Sets the number of times the ITP will retry the ping before marking the DCS node as unavailable. • <i>count</i>—Number of times the ITP will retry the ping.
Step 8	udp-checksum Example: <pre>ITP(config-cs7-dcs)# udp-checksum</pre>	(Optional) Turns on the optional calculation of a UDP checksum sent in the PMP stream.
Step 9	emdt [<i>emdt1</i> <i>emdt2</i>] Example: <pre>ITP(config-cs7-dcs)# emdt2</pre>	(Optional) Specifies the MSU data format encapsulation of the egress PMP packets. • emdt1—Encapsulated MSU Data Type 1, which takes advantage of an SNMP MIB to reduce the overhead of the MSU encapsulation header. • emdt2—(default) Encapsulated MSU Data Type 2, which includes all the context information with the MSU.
Step 10	shutdown Example: <pre>ITP(config-cs7-dcs)# shutdown</pre>	Stops sending PMP packets and pings to this DCS node. The DCS node is shut down by default.

Configuring a DCS Group

A DCS group represents a group of one or more DCS nodes and contains a maximum of eight. You identify a DCS group with a unique name.

Restrictions

The following list identifies restrictions to a DCS group:

- You cannot delete a DCS group that is referenced by a linkset or AS.
- You cannot delete a DCS node that is referenced by a DCS group.
- You cannot add more than eight DCS nodes to group.
- You cannot add a DCS node that is not configured to a DCS group.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cs7 dcs-group *name***
4. **dcs *name cost***

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: ITP> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: ITP# configure terminal	Enters global configuration mode.
Step 3	cs7 dcs-group <i>name</i> Example: ITP(config)# cs7 dcs-group dcsGroup1	Defines a DCS group and associates a name.
Step 4	[no] dcs <i>name cost</i> Example: ITP(config)# dcs dcs1 2	Adds or removes a DCS node to a DCS group.

Configuring Probeless Monitoring for a Specific Linkset

You can assign a DCS group to a specific linkset.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cs7** [**instance** *instance-number*] **linkset** *ls-name* *adj-pc* [**local-pc** [*pc*]]
4. **pmp**
5. **dcs-group** *dcs-group-name* { **in** | **out** | **all** }

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: ITP> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: ITP# configure terminal	Enters global configuration mode.
Step 3	cs7 [instance <i>instance-number</i>] linkset <i>ls-name</i> <i>adj-pc</i> [local-pc [<i>pc</i>]] Example: ITP(config)# cs7 linkset vt02 5.100.7	Specifies a linkset and enter CS7 linkset submenu.
Step 4	pmp Example: ITP(config-cs7-ls)# pmp	Turn on Probeless Monitoring for the linkset. Probeless Monitoring is off by default.
Step 5	dcs-group <i>dcs-group-name</i> { in out all } Example: ITP(config-cs7-ls)# dcs-group group_pmp_01 all	Associates a DCS group with a linkset. • <i>dcs-group-name</i>—Identifies the name of the DCS group. • in—Specifies inbound traffic will be copied to the specified group. • out—Specifies outbound traffic will be copied to the specified group. • all—Specifies both inbound and outbound traffic will be copied to the specified group.

Configuring Probeless Monitoring for a Specific AS

You can assign a DSC group to a specific AS.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cs7** [*instance instance-number*] **as** *as-name* { **m3ua** | **sua** }
4. **pmp**
5. **dcs-group** *dcs-group-name* { **in** | **out** | **all** }

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: ITP> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: ITP# configure terminal	Enters global configuration mode.
Step 3	cs7 [<i>instance instance-number</i>] as <i>as-name</i> { m3ua sua } Example: cs7 instance 4 as as1 m3ua	Specifies an AS and enter CS7 AS submode. instance—(Optional) Associate an Application Server (AS) with a defined instance. <i>instance-number</i> —Instance number. The valid range is 0 through 7. The default instance is instance 0. <i>as-name</i> —The AS name is a unique name used to identify an AS for configuration and monitoring. This name may be up to 12 characters long. The first character must be alphabetic. The AS name cannot duplicate an AS Route name, and cannot match the following reserved keywords: m3ua, sua, all, operational, active, statistics, bindings, or detail. m3ua —The m3ua keyword indicates that this is an M3UA AS. sua —The sua keyword indicates that this is an SUA AS.

	Command or Action	Purpose
Step 4	pmp Example: ITP(config-cs7-as)# pmp	Turn on Probeless Monitoring for the AS. Probeless Monitoring is off by default.
Step 5	dcsgroup dcs-group-name { in out all } Example: ITP(config-cs7-as)# dcs-group group_pmp_01 all	Associates a DCS group with a AS. <i>dcs-group-name</i>—Identifies the name of the DCS group. in—Specifies inbound traffic that will be copied to the specified group. out—Specifies outbound traffic that will be copied to the specified group. all—Specifies both inbound and outbound traffic that will be copied to the specified group.

Verifying the Probeless Monitoring Configuration

To verify the Probeless Monitoring configuration, use the following commands in Privileged EXEC mode:

Command	Purpose
Router# show cs7 dcs	Displays information about the dcs node.
Router# show cs7 dcs-group	Displays information about the dcs group.
Router# show cs7 pmp [errors context {as asname linkset lname}]	Displays information about PMP related errors or PMP packets.
Router# show cs7 linkset [instance-number] linkset [ls-name routes sls statistics statel timers tmap] [brief detailed]	Displays information about the linkset, including the PMP status and the assigned dcs-groups in the detailed information.
Router# show cs7 [instance-number] as [[m3ua [include-gtt exclude-gtt only-gtt]] [sua [include-gtt exclude-gtt only-gtt]] [all [include-gtt exclude-gtt only-gtt]] [name as-name]] [operational active all]] [statistics detail brief]	Displays information about the AS, including the PMP status and the assigned dcs-groups in the detailed information.

Configuration Example for Probeless Monitoring

The following configuration example shows a Probeless Monitoring configuration where the pmp feature is turned on globally. The copying occurs on the linkset ITPa, ITPd, vt02, and also occurs on the AS as1:

```
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
```

```
hostname ITPC
!
enable secret *****
enable password *****
!
!
!
!
!
no ip cef
no ip finger
no ip domain-lookup
!
cs7 variant itu
cs7 point-code 5.100.4
cs7 capability-pc 5.100.14
cs7 pmp
!
controller E1 1/0/0
    channel-group 0 timeslots 1
!
controller E1 2/0/0
    channel-group 0 timeslots 1
!
interface FastEthernet4/0/0
    ip address 10.74.50.33 255.255.255.0
    no ip route-cache distributed
    no ip route-cache
    no ip mroute-cache
!
interface FastEthernet4/0/1
    ip address 10.74.48.7 255.255.255.0
    no ip route-cache distributed
    no ip route-cache
    no ip mroute-cache
!
interface FastEthernet3/0/0
    ip address 172.18.45.1 255.255.255.128
    no ip route-cache distributed
    no ip route-cache
    no ip mroute-cache
!
interface FastEthernet3/0/1
    ip address 117.117.119.4 255.255.255.0
    no ip route-cache distributed
    no ip route-cache
    no ip mroute-cache
!
interface Serial1/0/0:0
    no ip address
    encapsulation mtp2
    no ip route-cache distributed
    no ip route-cache
    load-interval 30
!
interface Serial2/0/0:0
    no ip address
    encapsulation mtp2
    no ip route-cache distributed
    no ip route-cache
    load-interval 30
!
cs7 local-peer 7000
    local-ip 172.18.45.1
```

```

local-ip 117.117.119.4
!
!
cs7 route-table system
update route 5.100.1 7.255.7 linkset ITPa
update route 5.100.1 7.255.7 linkset ITPb
update route 5.100.6 7.255.7 linkset ITPa
update route 5.100.6 7.255.7 linkset ITPb
update route 5.100.8 7.255.7 linkset ITPd
!
!
cs7 dcs dcs1
remote-ip 10.74.50.22 10.74.48.33 3033
local-ip 10.74.50.33 3033
ping-interval 5
timeout-count 3
udp-checksum
!
cs7 dcs dcs2
remote-ip 10.74.50.27 10.74.48.39 3033
local-ip 10.74.50.33 3033
ping-interval 5
timeout-count 3
udp-checksum
!
cs7 dcs dcs3
remote-ip 10.74.50.20 10.74.48.32 3033
local-ip 10.74.50.33 3033
ping-interval 5
timeout-count 3
udp-checksum
!
cs7 dcs dcs4
remote-ip 10.74.50.29 10.74.48.35 3033
local-ip 10.74.50.33 3033
ping-interval 5
timeout-count 3
udp-checksum
!
cs7 dcs dcs5
remote-ip 10.74.50.23 10.74.48.38 3033
local-ip 10.74.50.33 3033
ping-interval 5
timeout-count 3
udp-checksum
!
cs7 dcs-group dcs-group1
dcs dcs1 cost 0
dcs dcs2 cost 0
dcs dcs3 cost 1
!
cs7 dcs-group dcs-group2
dcs dcs4 cost 0
dcs dcs5 cost 1
!
cs7 linkset ITPa 5.100.2
accounting
pmp
link 0 sctp 172.18.44.242 117.117.117.2 7000 7000
dcs-group dcs-group1 all
route all table system
!
cs7 linkset ITPb 5.100.5
accounting

```

```
link 0 sctp 172.18.44.243 117.117.117.3 7000 7000
route all table system
!
cs7 linkset ITPd 5.100.3
accounting
pmp
link 0 sctp 172.18.46.1 117.117.118.4 7000 7000
dcs-group dcs-group1 in
dcs-group dcs-group2 out
route all table system
!
cs7 linkset vt02 5.100.7
accounting
pmp
link 0 Serial1/0/0:0
link 1 Serial2/0/0:0
dcs-group dcs-group1 in
dcs-group dcs-group2 out
route all table system
!
cs7 m3ua 2910 offload 3 0
local-ip 117.117.118.4
!
cs7 m3ua 2911 offload 3 0
local-ip 117.117.118.4
!
cs7 m3ua 2912 offload 3 0
local-ip 117.117.118.4
!
cs7 m3ua 2913 offload 3 0
local-ip 117.117.118.4
!
cs7 asp asp1 2910 2910 m3ua
remote-ip 117.117.118.16
!
cs7 asp asp2 2911 2911 m3ua
remote-ip 117.117.118.17
!
cs7 asp asp3 2912 2912 m3ua
remote-ip 117.117.118.18
!
cs7 asp asp4 2913 2912 m3ua
remote-ip 117.117.118.19
!
cs7 instance 4 as as1 m3ua
pmp
routing-key 2333 444
asp asp1
asp asp2
dcs-group dcs-group1 in
dcs-group dcs-group2 out
!
cs7 instance 4 as as2 m3ua
routing-key 2333 444
asp asp3
asp asp4
!
ip classless
no ip http server
```




Multiple Instances and Instance Translation

The Multiple Instances feature makes it possible to connect Cisco ITP to different networks with specific variant and network indicators. Instance translation enables the conversion and transfer of MSUs between different instances.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



Note

Configuration Mode Restrictions: Simultaneous changes to the configuration from multiple CLI sessions are not supported. Only one configuration session is allowed to enter in configuration mode at a time; other sessions should not enter in configuration mode. The **show line** or **show users EXEC** command may be used to determine the active user sessions on an ITP, and the **clear line EXEC** command may be used to ensure that only a single active session exists.

Contents

- [Information About Multiple Instances and Instance Translation, page 67](#)
- [How to Configure Multiple Instances, page 69](#)
- [How to Configure Instance Translation, page 69](#)
- [Verifying the Multiple Instances Configuration, page 74](#)
- [Configuration Example for Multiple Instance, page 74](#)
- [Configuration Examples for Instance Translation, page 75](#)

Information About Multiple Instances and Instance Translation

The ITP Multiple Instance feature makes it possible to connect the ITP to different networks at one time, each with specific variant and network indicator values. The ITP treats each combination of variant and network indicator as a separate “instance.” Each instance acts as a separate logical ITP. Each instance is

a separate domain with a defined variant, network indicator, ITP point code, optional capability point code, and optional secondary point code. Each instance also has its own routing table and Global Title Translation (GTT) table

You can configure up to 8 different instances on the ITP. Instances are numbered 0 to 7.

Instance translation is the conversion of packets between instances of ANSI or ITU variants.

Understanding Virtual Linksets

A virtual linkset is a connection from one instance to another. There are two virtual linksets between any two instances in the ITP. For example, between instance X and instance Y, there are virtual linksets VirtualLSx-y and VirtualLSy-x. VirtualLSx-y appears to be a linkset in Instance x, and it will appear in Instance x's route table, for alias destinations whose true point code exists in Instance y. VirtualLSy-x appears to be a linkset in Instance y, and it will appear in Instance Y's route table, for alias destinations whose true point code exists in Instance x.

Virtual linksets are not the same as real linksets. Virtual linksets do not have queues, and are not bandwidth limited.

Virtual linkset are created automatically when a new instance is created. When an alias point code is defined, the alias point code is automatically entered in the alias instance's routing table using the virtual linkset. For example, the following command enters an alias point code in instance 5 for a real point code in instance 6:

```
cs7 instance 6 pc-conversion 3.4.5 alias-pc 5 5.6.7
```

This creates a route in instance 5 for the alias point code 5.6.7. The linkset shown in the Virtual Linkset that goes from Instance 5 to Instance 6.

```
#show cs7 5 route 5.6.7 detailed
Routing table = system5 Instance = 5
Destination      C Q P Linkset Name      Linkset Non-adj Route
-----
5.6.7/14         acces  1 VirtualLS5-6         avail  allowed avail
```

Virtual linksets are available if the destination Instance has completed MTP Restart. They are Unavailable when the destination instance is doing an MTP Restart. For example, when instance 6 is isolated or going through an MTP Restart, here is the output of show cs7 route for the alias point code.

```
#show cs7 5 route 5.6.7 detailed
Routing table = system5 Instance = 5
Destination      C Q P Linkset Name      Linkset Non-adj Route
-----
5.6.7/14         INACC  1 VirtualLS5-6         UNAVAIL allowed UNAVAIL
```

How to Configure Multiple Instances

To enable Multiple Instances, use the following command in global configuration mode:

Command	Purpose
Router(config)# cs7 multi-instance	Enable the Multiple Instance feature.

For the commands that require an instance number, anything configured before Multiple Instances is turned on (such as variant, point-code, linksets, routes) is considered to be in the default instance (instance 0) once Multiple Instances is turned on.

Also, after you turn on Multiple Instances, the ITP begins displaying the instance number when it displays a point code. The ITP displays the point code, then a colon, then the instance number. For example, 1.2.3:0 means point code 1.2.3 in instance 0.

To configure an additional instance (after the default) specify the instance, the variant, and the instance network name, using the following commands in interface configuration mode:

Command	Purpose
Router(config)# cs7 instance <i>instance-number</i> variant { ansi china itu ttc }	Identify an instance and indicate which of the SS7 variations the ITP is running on the instance. Instance numbers are used only to configure the information specific to each instance and do not need to match across devices.
Router(config)# cs7 instance <i>instance-number</i> network-name <i>network-name</i>	Specify a network name for the instance The network-name is used to qualify information per signaling point in related management information bases. It is used to correlate instances into the same network by network management applications. In order for instances in the same network to be properly managed they must be assigned the same network name.

How to Configure Instance Translation

This section include the following tasks and information:

- [Configuring Point Code Conversion, page 69](#)
- [Configuring Global Title Conversion, page 70](#)
- [Configuring Instance Conversion After Global Title Translation, page 73](#)

Configuring Point Code Conversion



Note

In the case of variant conversions among ANSI/CHINA/ITU/TTC, the MSU size may change as a result of the different point codes size.



Note

Point code conversion is not supported for SCCP Class 2 traffic.

The ITP performs point code conversion for the following point codes:

- DPC
- OPC
- Concerned Point Code
- SCCP Called Party PC
- SCCP Calling Party PC
- SCMG Concerned PC

To configure point code conversion, use the following command in global configuration mode:

Command	Purpose
Router(config)# cs7 instance <i>instance-number</i> pc-conversion <i>pc</i> alias-pc <i>alias-instance</i> <i>alias-pc</i>	Configures a mapping between <i>pc</i> in instance <i>instance-number</i> , and <i>alias-pc</i> in <i>alias-instance</i> . If an MSU arrives destined for <i>alias-pc</i> in instance <i>alias-instance</i> , it will be sent to instance <i>instance</i> and the DPC converted to <i>pc</i> .

To configure default point code conversion, use the following command in global configuration mode:

Command	Purpose
Router(config)# cs7 instance <i>instance-number</i> pc-conversion default <i>alias-instance</i> [no-route]	Allows MSUs with unknown point codes in one instance to be another instance. Enables default conversion for point codes between instance <i>orig-instance</i> and <i>dest-instance</i> . If point code conversion between the two instances is required, and the point code does not match a specified <i>pc</i> conversion, or the ITP's point code, then the point code is unchanged in the new instance and conversion still succeeds

Configuring Global Title Conversion



Note

This section describes specifying changes to Global Title fields when configuring the Instance Translation feature. If you are looking for information about specifying Global Title Address (GTA) conversion mapping, see the [“Configuring Global Title Address Conversion” section on page 121](#) of the [“Global Title Translation”](#) chapter.

The following sections describe the purpose of Global Title conversion, three methods of converting the SCCP Global Title information, and how to assign a conversion table from one instance to another. These methods are optional, and can be used separately, combined, or not at all. The methods are applied to both the Calling and Called Party Addresses.

- [Overview of Global Title Conversion, page 71](#)
- [Creating a GTI Conversion Table, page 71](#)
- [Creating a Subsystem Mapping Table, page 72](#)

- [Creating a GTA Prefix Conversion Table, page 72](#)
- [Assigning a Conversion Table to an Instance, page 72](#)

Overview of Global Title Conversion

The optional Global Title Conversion feature enables you to specify changes to SCCP Global Title fields when performing conversion between instances. Two typical scenarios for Global Title Conversion are:

GTT is required, MSUs are destined for local point-code. The result of GTT is an application group including other instance's PC or xUA AS.

- MSUs are destined for an alias point-code in a different instance.

If the Global Title Conversion feature is not configured, the MSUs going from one instance to another will have no change in the global title data. However, Calling and Called Party point codes will be converted, if they exist.

The fields that can be changed are:

- Global Title Indicator (GTI) - ANSI networks normally use GTI 2. ITU networks typically use GTI 4.
- Translation Type (TT)
- Subsystem Number (SSN)
- Global Title Address (GTA) - This field uses the existing ITP GTA prefix conversion feature.
- Encoding Scheme - This field is used if GTI is 4, does not exist for GTI 2.
- Numbering Plan - This field is used if GTI is 4, does not exist for GTI 2.
- Nature of Address - This field is used if GTI is 4, does not exist for GTI 2.



Note

Global Title conversion is supported for SCCP UDT, XUDT, UDTs, XUDTS message types only.

Creating a GTI Conversion Table

The GTI conversion method can be used to update the GTI, TT, SSN, Encoding Scheme (ES), Numbering Plan (NP), and Nature of Address Indicator (NAI) in an SCCP address. You name the table, and then specify sets of input parameters and output parameters. When an MSU comes in, the ITP finds the most specific match. If no match is found, the fields in the MSU are unchanged. For ANSI, GTI 2 is supported. For ITU, GTI 2 and 4 are supported.

To create a GTI Conversion Table perform the following tasks, beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# cs7 sccp gti-conversion <i>tablename</i>	Names the GTI Conversion table and enables CS7 SCCP GTI conversion mode.
Step 2	Router(config-cs7-sccp-gticonv)# update [gti-in <i>gti-in</i>] [tt-in <i>tt-in</i>] [ssn-in <i>ssn-in</i>] [es-in <i>es-in</i>] [np-in <i>np-in</i>] [nai-in <i>nai-in</i>] [gti-out <i>gti-out</i>] [tt-out <i>tt-out</i>] [ssn-out <i>ssn-out</i>] [es-out <i>es-out</i>] [np-out <i>np-out</i>] [nai-out <i>nai-out</i>] [addr-conv <i>addr</i>]	Specifies the input and output parameters for the table. If the addr-conv keyword is specified, this GTT conversion takes precedence over any GTT address conversion table specified per instance conversion rule.

Creating a Subsystem Mapping Table

The subsystem mapping method converts a subsystem in one instance to a different subsystem in another instance. To create a subsystem mapping table, use the following command in global configuration mode:

Command	Purpose
Router(config)# cs7 sccp ssn-conversion <i>tablename</i> in-ssn <i>in-ssn</i> out-ssn <i>out-ssn</i>	Creates a subsystem mapping table, specifying input and output SSN values.

If no match is found in the SSN conversion table, the SSN in the MSU is unchanged. If both GTI Conversion and Subsystem Mapping are used, and a GTI conversion specifies a new subsystem for the MSU, the subsystem specified by the GTI conversion is used.

Creating a GTA Prefix Conversion Table

The GTA prefix conversion method uses the existing ITP address-conversion feature. This feature allows for conversion of addresses that use different prefixes or codes, such as converting between E212 and E214 addressing schemes. Address conversion is an optional part of GTT conversion and will only be applied when configured.



Note

Both the address conversion command here and the GTI conversion command described earlier, allow the user to specify a numbering plan and nature of address values. Any NP or NAI specified by address conversion overrides those specified by GTI conversion.

To define a address conversion table and enter GTT address conversion submode, use the following commands, beginning in global configuration mode:

Command	Purpose
Router(config)# cs7 instance <i>instance-number</i> gtt address-conversion <i>tablename</i>	Specifies a GTT address conversion table name (1-12 characters) and enables CS7 GTT address conversion table submode.
Router(config-cs7-gtt-conv-tbl)# update in-address <i>input-address</i> [out-address <i>output-address</i>] [np <i>newnp</i>] [nai <i>newnai</i>] [es <i>es</i>]	Defines input and (optionally) output address entries.

Assigning a Conversion Table to an Instance

This task assigns gti-conversion, subsystem mapping, and address-conversion tables for conversion from one instance to another. All three conversion methods can be used, or just one or two. If no conversion methods are assigned, the GTT in the MSUs will not be changed.

To assign a conversion table for conversion, use the following commands, beginning in global configuration mode:

Command	Purpose
Router(config)# cs7 sccp instance-conversion in-instance <i>instance</i> out-instance <i>instance</i>	Specifies the input and output instances.
Router(config-cs7-sccp-insconv)# set gti-conversion <i>tablename</i>	Assigns GTI conversion table to be assigned from one instance to another.
Router(config-cs7-sccp-insconv)# set ssn-conversion <i>tablename</i>	Assigns subsystem mapping table to be assigned from one instance to another.
Router(config-cs7-sccp-insconv)# set address-conversion <i>tablename</i>	Assigns address-conversion table to be assigned from one instance to another.
Router(config-cs7-sccp-insconv)# set message-handling <i>option</i>	Specifies the message handling option to be used. The following are valid options: 0 no special options 1-7 spare values (ie unassigned) 9-15 additional spare values (ie unassigned) no change leave field unchanged return-on-error return [x]udts on error
Router(config-cs7-sccp-insconv)# set national-indicator <i>natl-ind</i>	Specifies the SCCP national indicator to be used. The following are valid options: 0 international 1 national no change leave field unchanged

Configuring Instance Conversion After Global Title Translation

To enable Instance Conversion with global title, configure an application group in an instance and then assign point codes in other instances to the application group.

The application group has an optional parameter **instance**. If you do not specify an instance, a point code that is entered has the same instance as the application group. By using the instance parameter, you can specify a point code in a different instance. The specified point code must represent a real point code, not an alias point code.

To configure instance translation with GTT use the following command in global configuration mode:

Command	Purpose
Router(config)# cs7 instance <i>instance-number</i> gtt application-group <i>application-group</i>	Configures an application group in an instance.
Router(config-cs7-gtt-app-grp)# instance <i>instance-number</i> { pc <i>pc</i> asname <i>asname</i> } ssn <i>ssn cost</i> { pcssn gt }	Assign point codes in other instances to the application group.

The following example creates a GTT entry for instance 0 that will convert the MSU to instance 1. If the ITP receives an SCCP MSU in instance 0, destined for the ITP, route on global title with TT 250 and GTA 919, the ITP will convert the MSU to instance 1 and send the MSU to point code 1.1.1 in instance 1 if 1.1.1/10 is available.

```
Router(config)#cs7 instance 0 gtt application-group app-group0
Router(config-cs7-gtt-app-grp)#instance 1 pc 1.1.1 ssn 10 1 pcssn
Router(config-cs7-gtt-app-grp)#pc 2.2.2 ssn 20 2 pcssn
Router(config-cs7-gtt-app-grp)#exit
Router(config)#cs7 instance 0 gtt selector selector0 tt 250
Router(config-cs7-gtt-selector)#gta 919 app-grp app-group0
Router(config-cs7-gtt-selector)#
```

The following example creates a GTT entry for the converted instance 1. Instead of sending the MSU directly to point code 1.1.1, you configure the pc to match instance 1's local pc with the RI set to gt. Assuming instance 1 has a local pc of 3.3.3, the MSU performs gtt again in instance 1 and routes the MSU based on the GTT configuration of instance 1.

```
Router(config)#cs7 instance 0 gtt application-group app-group0
Router(config-cs7-gtt-app-grp)#instance 1 pc 3.3.3 1 gt
Router(config-cs7-gtt-app-grp)#exit
Router(config)#cs7 instance 0 gtt selector selector0 tt 250
Router(config-cs7-gtt-selector)#gta 910 app-grp
Router(config-cs7-gtt-selector)#
```

You can also configure an application group that contains an asname that is in a different instance. In this case, the ITP will convert the MSU to the new instance, then send the MSU to the as.

```
dancer(config)#cs7 instance 1 gtt application-group as-app1
dance(config-cs7-gtt-app-grp)#asname as-0 1 pcssn
dance(config-cs7-gtt-app-grp)#exit
dancer(config)#cs7 instance 1 gtt selector selector0 tt 10
danc(config-cs7-gtt-selector)#gta 336 app-grp as-app1
```

Verifying the Multiple Instances Configuration

To verify the Multiple Instances configuration, use the following command in Privileged EXEC mode:

Command	Purpose
Router# show cs7 virtual-linkset [<i>linkset-name</i>] [brief] [routes] [statistics] [utilization]	Displays information about virtual linksets.

Configuration Example for Multiple Instance

In the following example, the Multiple Instances feature is used to configure STPs in two SS7 networks. Network 1 has variant ANSI and network indicator national. All instances in this network will have network name specified as ANSI-NAT. Network 2 has variant ANSI and network indicator international. All instances in this network will have network name specified as ANSI-INT.

Configuration for ITP1

```

cs7 multi-instance
cs7 instance 0 variant ANSI
cs7 instance 0 network-name ANSI-NAT
cs7 instance 0 point-code 5.5.1
cs7 instance 1 variant ANSI
cs7 instance 1 network-name ANSI-INT
cs7 instance 1 network-indicator international
cs7 instance 1 point-code 15.5.1

```

Configuration for ITP2

```

cs7 multi-instance
cs7 instance 0 variant ANSI
cs7 instance 0 network-name ANSI-INT
cs7 instance 0 network-indicator international
cs7 instance 0 point-code 7.3.2
cs7 instance 1 variant ANSI
cs7 instance 1 network-name ANSI-NAT
cs7 instance 1 point-code 11.6.2

```

Configuration Examples for Instance Translation

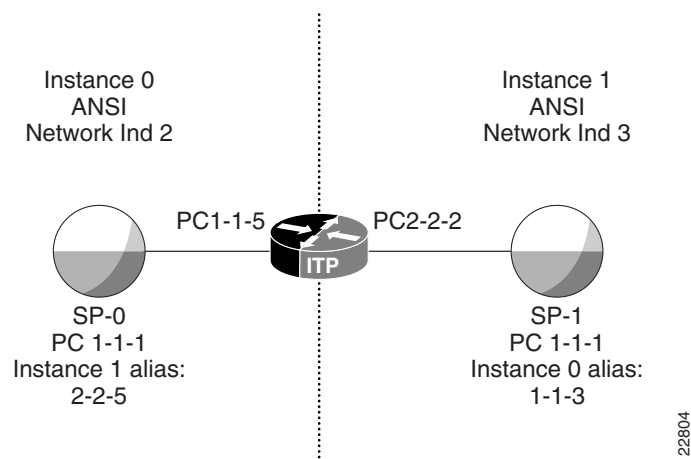
This section includes two examples:

- [Instance Translation: Instances with the Same Variant, page 75](#)
- [Instance Translation: Conversion from ANSI to ITU, page 77](#)
- [Instance Translation: Conversion from TTC to ITU, page 77](#)

Instance Translation: Instances with the Same Variant

The following example configuration is illustrated in [Figure 8](#).

Figure 8 Instance Translation Configuration Example



In the network above, SP-0 sees the ITP with PC 1-1-5, and also sees a remote SP with PC 1-1-3. SP1 sees the ITP with PC 2-2-2, and also sees a remote SP with PC 2-2-5. The CLI to configure the alias point codes is shown below:

```

ITP#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ITP(config)#cs7 instance 0 pc-conversion 1.1.1 alias-pc 1 2.2.5
ITP(config)#cs7 instance 1 pc-conversion 1.1.1 alias-pc 0 1.1.3

```

When SP-0 sends an MSU to SP-1, it sets:

- DPC: 1-1-3
- OPC: 1-1-1
- Network Indicator: 2

When the ITP receives the MSU, it determines that 1-1-3 in Instance 0 is an alias for 1-1-1 in Instance 1, so it converts the MSU to Instance 1. Since Instance 1 uses Network Indicator 3, the MSU's Network Indicator is changed to 3. The converted MSU has:

- DPC 1-1-1
- OPC 2-2-5
- Network Indicator: 3

If the MSU is SCCP and contains a Calling Party PC, this PC is converted using the alias PC table. If the Calling Party PC is 1-1-1, this is converted to 2-2-5

The following show command output sections show the status before and after the configuration of Instance Translation:

```

ITP#show cs7 linkset brief
lsn=SP-0          apc=1.1.1:0      state=avail      avail/links=1/1
lsn=SP-1          apc=1.1.1:1      state=avail      avail/links=1/1

```

```
ITP#show cs7 route
```

```
Routing table = system Instance = 0
```

Destination	Prio	Linkset Name	Route
1.1.1/24	acces 1	SP-0	avail

```
Routing table = system1 Instance = 1
```

Destination	Prio	Linkset Name	Route
1.1.1/24	acces 1	SP-1	avail

```
ITP#show cs7 route
```

```
Routing table = system Instance = 0
```

Destination	Prio	Linkset Name	Route
1.1.1/24	acces 1	SP-0	avail
1.1.3/24	acces 1	VirtualLS0-1	avail

```
Routing table = system1 Instance = 1
```

Destination	Prio	Linkset Name	Route
1.1.1/24	acces 1	SP-1	avail
2.2.5/24	acces 1	VirtualLS1-0	avail

```

ITP#show cs7 linkset brief
lsn=SP-0          apc=1.1.1:0      state=avail      avail/links=1/1
lsn=SP-1          apc=1.1.1:1      state=avail      avail/links=1/1

ITP#show cs7 pc-conversion

PC          ALIAS  PCs
1.1.1:0     2.2.5:1
1.1.1:1     1.1.3:0

ITP#show cs7 0 pc-conversion 1.1.1

PC          ALIAS  PCs
1.1.1:0     2.2.5:1

ITP#show cs7 1 pc-conversion 1.1.1

PC          ALIAS  PCs
1.1.1:1     1.1.3:0

```

Instance Translation: Conversion from ANSI to ITU

The following GTI conversion and instance conversion tables convert E.164 global title addresses from ANSI to ITU and ITU to ANSI:

```

cs7 sccp gti-conversion ANSI2ITU
  update gti-in 2 tt-in 10 gti-out 4 tt-out 0 np-out 1 nai-out 4 es-out 2
cs7 sccp gti-conversion ITU2ANSI
  update gti-in 4 tt-in 0 np-in 1 nai-in 4 gti-out 2 tt-out 10
cs7 sccp instance-conversion in-instance 0 out-instance 2
  set gti-conversion ITU2ANSI

cs7 sccp instance-conversion in-instance 2 out-instance 0
  set gti-conversion ANSI2ITU

```

Default conversion is not allowed between different variants. The following command will be rejected and will generate a console error if *instance* and *alias-instance* have different variants:

```
cs7 instance <instance> pc-conversion default <alias-instance>
```

Instance Translation: Conversion from TTC to ITU

The following GTI conversion and instance conversion tables convert E.164 global title addresses from TTC to ITU:

```

cs7 sccp gti-conversion gti-conv0
(config-cs7-sccp-gticonv)#update in-gti 4 in-tt 0 in-ssn 6 out-gti 2 out-tt 240
(config-cs7-sccp-gticonv)#update in-gti 4 in-tt 0 in-ssn 8 out-gti 2 out-tt 10

```

For subsystem mapping, enter the following commands:

```

(config)#cs7 sccp ssn-conversion ss-conv0 in-ssn 11 out-ssn 13
(config)#cs7 sccp ssn-conversion ss-conv0 in-ssn 200 out-ssn 6

```

For address conversion, enter the following commands:

```

cs7 instance 1 gtt address-conversion gta-conv0
update in-address 919522 out-address 1919522

```

For conversion, enter the following commands:

```
cs7 sccp instance-conversion input-instance 0 output-instance 1
set gti-conversion gti-conv0
set ssr-conversion ssr ss-conv0
set address-conversion gta-conv0
```

**Note**

The above conversion types are optional when performing instance conversion and they can be used separately or together.



ITP Group



Note

Configuration Mode Restrictions: Simultaneous changes to the configuration from multiple CLI sessions are not supported. Only one configuration session is allowed to enter in configuration mode at a time; other sessions should not enter in configuration mode. The **show line** or **show users EXEC** command may be used to determine the active user sessions on an ITP, and the **clear line EXEC** command may be used to ensure that only a single active session exists.

The ITP Group feature allows two ITPs to appear as a single network entity. The two ITPs share the same local point codes and support SS7 linksets that span both ITPs. In the event of a failure of one of the ITPs, the other is capable of maintaining the availability of the local point codes and linksets and continuing with message forwarding. This feature provides inter-device redundancy, high availability, and reduced point code usage.

Feature History for ITP Group

Release	Modification
12.4(11)SW	This feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for ITP Group Operation, page 80](#)
- [Restrictions for ITP Group Operation, page 80](#)
- [Information about ITP Group Operation, page 80](#)
- [How to Configure the ITP Group Feature, page 81](#)
- [Configuration Example for ITP Group, page 88](#)
- [Performing ITP Group Software Upgrade, page 90](#)

Prerequisites for ITP Group Operation

Proper ITP Group operation requires that both group members have a consistent ITP configuration such that each has the same understanding of the group point code(s) and linkset membership.

Each peer must be configured independently with the parameters necessary to participate in a group.

Restrictions for ITP Group Operation

The ITP Group feature is not supported on the Cisco 7500 Router.

When two ITPs are interacting as ITP Group peers the physical communication link between them is of critical importance. The ITPs must share real time state information through this link and some SS7 traffic handled by the pair may traverse this link.

The only certified and supported configuration is a configuration with Ethernet cross cables.

Both ITPs must run the identical version of IOS.

Information about ITP Group Operation

Group Roles

An ITP that is a member of an ITP Group operates in one of two redundancy roles, Active or Standby. The ITP operating in the Active role is referred to as the group Manager and is responsible for maintaining all MTP3 and SCCP state information for the ITP Group. The ITP operating in the Standby role is referred to as the group Alternate and relies on the Manager for the state information it needs for handling traffic for its links. Any MTP3 and SCCP management messages received by the Alternate are forwarded to the Manager, which runs the SS7 management procedures for both ITPs. The Alternate takes over the role of Manager in the event of a failure of the Manager.

The Manager has a redundancy state of ACTIVE. The Alternate, under steady state conditions, has a redundancy state of STANDBY HOT, meaning that it is prepared to take over the Manager (Active) role if the current Manager fails. Other Standby states are STANDBY COLD, which indicates that Alternate just assumed the Standby role and STANDBY COLD-BULK, which indicates that the Alternate is in the process of being updated by the Manager with the state information it needs to become STANDBY HOT.

The group role information is displayed in the output of the **show cs7 group state** command:

```
ITP Group state information:
  Redundancy Facility state:
    RF State:                ACTIVE
    RF Peer State:           STANDBY HOT

  Group role information:
    Current State:          Manager
```

The SNMP notification ciscoRFProgressionNotif is generated by an ITP Group member whenever its redundancy state, or that of its peer, transitions to STANDBY COLD, STANDBY HOT or ACTIVE.

Group Member Isolation

An ITP Group member detects the presence of its group peer by monitoring the state of the group control transport (configured under the **cs7 group** command) and the redundancy state transport (configured under the **ipc zone default** and **association** commands). When both of these transports fail a group member must assume that the group peer has failed and that it is working in isolation as a group Manager.

In order to improve system availability and prevent the loss of both of these transports due a single component failure, it is recommended that the group control and redundancy state transports be configured as dual-homed SCTP associations running over two interfaces on each group member. This can be achieved by specifying two **local-ip** addresses and two **remote-ip** addresses when configuring the group control and redundancy state transports.

If a network failure causes both transports to come down, both group members assume the role of Manager. If communication between the two group members is re-established, then one of the ITPs is forced to assume an Alternate role and be reloaded in order for it to achieve the proper Standby state. The following messages is issued in this situation:

```
%CS7GROUP-5-ACTIVETOSTANDBY: Redundancy state transition from Active to Standby -
reload required
%RF_INTERDEV-4-RELOAD: % RF induced self-reload
```

Group Transport Configuration Changes

Changes in the group control and redundancy state transports are disruptive events when there are two ITP Group members present and handling traffic. It is suggested that transport configuration changes be made at times of minimal impact.

Configuration changes to the group control transport require the user to shutdown the transport when making the changes. When this transport is shutdown the Manager and Alternate are unable to exchange ITP control information or forward SS7 traffic between them. For this reason traffic forwarding on the Alternate is stopped and its links placed in a system-shutdown state until the transport is re-established:

```
ITP1#show cs7 linkset
lsn=to_STP1          apc=3.4.5          state=avail    avail/links=2/4
  SLC  Interface      Service  PeerState      Inhib
  00   10.0.0.1 6666 5555   avail    -----      ----
  01   11.0.0.1 6666 5555   avail    InService  -----
  *02   (on ITP2)      sys-shut -----      ----
  *03   (on ITP2)      sys-shut -----      ----
```

Configuration changes to the redundancy state transport also require the user to shutdown the transport when making the changes. When this transport is shutdown the Manager is unable to update the SS7 management state on the Alternate. For this reason traffic forwarding on the Alternate is stopped and its links placed in a system-shutdown state while the transport is shutdown. When the transport is re-established (with the **no shutdown** command) the redundancy infrastructure in the Alternate has no way of knowing whether it has missed any state updates, so it issues an *%RF_INTERDEV-4-RELOAD: % RF induced self-reload* message and reload. On reload, the Alternate receives a complete set of redundancy and SS7 state information from the Manager.

How to Configure the ITP Group Feature

Configuring the ITP Group feature consists of the following tasks:

- [Configuring the Inter-Device Redundancy Parameters, page 82](#)
- [Enabling the ITP Group Feature, page 83](#)
- [Configuring the Group SCTP Parameters, page 85](#)
- [Defining Linksets that Span Group Peers, page 86](#)

Configuring the Inter-Device Redundancy Parameters

SUMMARY STEPS

Perform these steps on both ITP group members.

1. **enable**
2. **configure terminal**
3. **redundancy [inter-device]**
4. **exit**
5. **ipc zone default**
6. **association** *association-id*
7. **protocol sctp**
8. **local-port** *port-number*
9. **local-ip** *ip-address*
10. **exit**
11. **remote-port** *port-number*
12. **remote-ip** *ip-address*

DETAILED STEP

S

	Command or Action	Purpose
Step 1	enable Example: ITP> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: ITP# configure terminal	Enables global configuration mode.
Step 3	redundancy inter-device Example: ITP(config)# redundancy inter-device	Enables interdevice redundancy submode.
Step 4	exit Example: ITP(config-red-interdevice)# exit	Returns to global configuration mode.
Step 5	ipc zone default Example: ITP(config)# ipc zone default	Configures the Inter-device Peer Communication protocol (IPC). Enables the IPC zone mode, in which you configure the communication link between the two devices.

	Command or Action	Purpose
Step 6	association <i>association-id</i> Example: ITP(config-ipczone)# association 1	Configures an association between the two devices. Enable IPC association mode.
Step 7	protocol <i>sctp</i> Example: ITP(config-ipczone-assoc)# protocol sctp	Configures SCTP protocol to be used as the transport protocol for this association. Enables the SCTP protocol mode.
Step 8	local-port <i>port-number</i> Example: ITP(config-ipc-protocol-sctp)# local-port 1111	Specifies the local SCTP port. Enables IPC Transport SCTP local mode. Note The port number for the local IPC SCTP association can not be the same as the port number for the CS7 group association. When you define a local IPC SCTP port number (for example port number 1024) the next available port number (in this example port number 1025) is automatically created for the IPC SCTP association used for checkpointing. Neither of these port numbers (in this example, neither 1024 nor 1025) may be used for the CS7 group port number.
Step 9	local-ip <i>ip-address</i> Example: ITP(config-ipc-local-sctp)# local-ip 1.1.1.1	Specifies the local IP address that will be used in the SCTP association.
Step 10	remote-port <i>port-number</i> Example: ITP(config-ipc-local-sctp)# remote-port 2222	Specifies the remote SCTP port. Enables IPC Transport SCTP remote mode.
Step 11	remote-ip <i>ip-address</i> Example: ITP(config-ipc-remote-sctp)# remote-ip 1.1.1.2	Specifies the remote IP address that will be used in the SCTP association.

What to Do Next

Enable the ITP Group feature

Enabling the ITP Group Feature

The ITP Group feature allows two ITPs to share an SS7 point code and appear as a single entity. This section describes the steps to configure two ITPs as members of a group.

Prerequisites

Proper group operation requires that both ITP group members have a consistent ITP configuration. Each member must have the same understanding of the group point code(s) and linkset membership. Both peers must be the same physical Cisco platform.

SUMMARY STEPS

Perform these steps on both ITP group members.

1. **enable**
2. **configure terminal**
3. **cs7 group name port-number**
4. **local-ip ip-address**
5. **peer peer-name port-number**
6. **remote-ip ip-address**
7. *DETAILED STEPS*

	Command or Action	Purpose
Step 1	enable Example: ITP> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: ITP# configure terminal	Enters global configuration mode.
Step 3	cs7 group name port-number Example: ITP(config)# cs7 group ITP1 33333	Configures the ITP group name and port number and enables the group configuration mode. Valid port numbers range from 1024 to 49151. Note The port number for the local IPC SCTP association can not be the same as the port number for the CS7 group association. When you define a local IPC SCTP port number (for example port number 1024) the next available port number (in this example port number 1025) is automatically created for the IPC SCTP association used for checkpointing. Neither of these port numbers (in this example, neither 1024 nor 1025) may be used for the CS7 group port number.
Step 4	local-ip ip-address Example: ITP(config-group)# local-ip 1.1.1.1	Specifies up to four local IP addresses for the association.

	Command or Action	Purpose
Step 5	peer <i>port-number</i> Example: ITP(config-group)# peer ITP2 4444	Enables the ITP to initiate the SCTP association with its peer and enables group peer mode.
Step 6	remote-ip <i>ip-address</i> Example: ITP(config-group-peer)# remote-ip 2.2.2.2	Specifies up to four remote IP addresses for the association.

What to Do Next

Configure the group SCTP Parameters.

Configuring the Group SCTP Parameters

There are several commands for managing the association and tuning the SCTP parameters. To configure group SCTP parameters, use the following commands, as appropriate:

Commands for Configuring SCTP Parameters

Command	Mode	Purpose
assoc-retransmit <i>retries</i>	Group Peer	Configures the number of consecutive retransmissions SCTP will perform before failing an association. Using the no form of the command sets the association retransmission threshold to its default value.
bundling <i>msec</i>	Group Peer	Configures the amount of time that SCTP will wait for messages from RF for purposes of bundling multiple RF messages into a single SCTP message. Bundling is enabled by default with a 20 milliseconds delay. Using the no form of the command disables SCTP bundling.
cumulative-sack <i>msec</i>	Group Peer	Configures the amount of time SCTP will wait before sending a selective acknowledgement (SACK) to the peer in the absence of other conditions that would generate a SACK. Using the no form of the command sets the SACK timeout back to its default value.
init-retransmit <i>max-retries</i>	Group	Configures the number of consecutive retransmissions SCTP will perform when attempting to establish an association with a peer before the peer is considered unreachable. Using the no form of the command sets the initialization retransmission threshold to its default value.

Command	Mode	Purpose
<code>init-timeout msec</code>	Group	Configures the timeout value for association setup messages. Using the no form of the command sets the initialization timeout value to its default value.
<code>keepalive msec</code>	Group Peer	Configures the amount of time SCTP will wait before retransmitting a keepalive message in the absence of data traffic. Using the no form of the command sets the keepalive interval back to its default value.
<code>max-streams inbound-number outbound-number</code>	Group	Configures the maximum number of streams SCTP will allow in the inbound and outbound direction. Using the no form of the command sets the maximum inbound stream limit back to its default value.
<code>path-retransmit max-retries</code>	Group Peer	Configures the number of consecutive retransmissions SCTP will perform before failing a path within an association. Using the no form of the command sets the path retransmission threshold to its default value.
<code>receive-window bytes</code>	Group	Configures the initial advertised received window size in bytes for the association. Using the no form of the command sets the receive window size to its default value.
<code>retransmit-timeout msec</code>	Group Peer	Configures the maximum amount of time SCTP will wait before retransmitting data. Using the no form of the command sets the maximum retransmission timeout to its default value.
<code>tx-queue-depth depth</code>	Group Peer	Configures the maximum transmit queue depth for new SCTP associations established with the local port.

What to Do Next

Define Linksets that span group peers.

Defining Linksets that Span Group Peers

To configure a linkset you must name the linkset and specify the point code of the adjacent signaling point.

Prerequisites

You must specify the SS7 variant and the point code before you can configure linksets.

SUMMARY STEPS

Perform these steps on both ITP group members.

1. **enable**
2. **configure terminal**
3. **cs7 linkset** *ls-name adjacent-point-code*
4. **link** *slc peer-name*

DETAILED STEPS

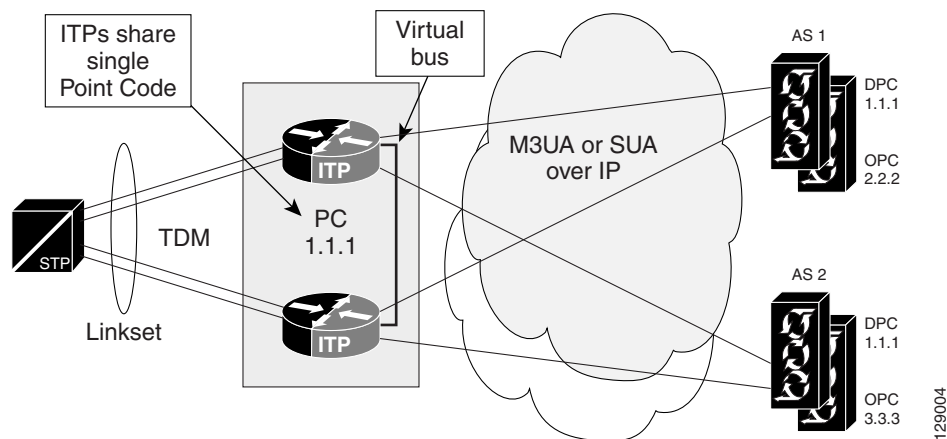
	Command or Action	Purpose
Step 1	enable Example: ITP> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: ITP# configure terminal	Enters global configuration mode.
Step 3	cs7 linkset Example: ITP(config)# cs7 linkset to-STP 5.5.5	Specifies a linkset to an adjacent node and enables linkset configuration mode. Linkset names are case-specific.
Step 4	link Example: ITP(config-ls)# link 0 ITP1 s1/0 ITP(config-ls)# link 1 ITP2 s1/0	Specifies a link and enables link configuration mode. The <i>peer-name</i> specifies the group peer on which the physical link exists.

Configuration Example for ITP Group

This configuration example shows the operation of two ITPs sharing point code 1.1.1. The STP has four links connected to 1.1.1, two to each of the ITPs. The ITPs maintain a communication path that is used for exchanging redundancy information, checkpointing information and a separate path for distributed link traffic. Each ITP has path to AS1 and AS2, in this case these are attached via M3UA or SUA.

The configuration is illustrated in [Figure 9](#). The configuration follows the illustration.

Figure 9 ITP Group



Configuration for ITP1

Configuration for ITP1 in the example above is as follows:

```
redundancy inter-device
!
ipc zone default
  association 1
  no shutdown
  protocol sctp
  local-port 11111
  local-ip 1.1.1.1
  remote-port 22222
  remote-ip 1.1.1.2
!
cs7 variant ITU
cs7 point-code 1.1.1

cs7 group ITP1 33333
  local-ip 1.1.1.1
  peer ITP2 44444
  remote-ip 1.1.1.2

cs7 linkset to_STP 5.5.5
  link 0 ITP1 s1/0
  link 1 ITP1 s1/1
  link 2 ITP2 s1/0
  link 3 ITP2 s1/1
```

Configuration for ITP2

Configuration for ITP2 in the example above is as follows:

```
redundancy inter-device
!
ipc zone default
  association 1
  no shutdown
  protocol sctp
  local-port 22222
  local-ip 1.1.1.2
  remote-port 11111
  remote-ip 1.1.1.1
!
cs7 variant ITU
cs7 point-code 1.1.1

cs7 group ITP2 44444
  local-ip 1.1.1.2
  peer ITP1 33333
  remote-ip 1.1.1.1

cs7 linkset to_STP 5.5.5
  link 0 ITP1 s1/0
  link 1 ITP1 s1/1
  link 2 ITP2 s1/0
  link 3 ITP2 s1/1
```

Performing ITP Group Software Upgrade

This procedure describes the steps to upgrade the ITP IOS software if you have implemented ITP Group.

1. Determine the ITP Group state of the two ITPs in the group being upgraded. This can be accomplished by issuing the **show cs7 group state** command. The ITP with a group state of *Manager* will be referred to as the Manager throughout this procedure. The ITP with a group state of *Alternate* will be referred to as the Alternate throughout this procedure.
2. If the ITPs are to be loaded from flash or disk, transfer the new ITP images to the flash/disk on both the Manager and Alternate.

Steps 3 - 5 are performed on the Manager.

3. On the Manager issue a **shutdown** command for all MTP2 links that physically reside on the Manager. This will redirect all traffic handled by the ITP Group through the Alternate.
4. On the Manager issue a **shutdown** command for all Ethernet interfaces that are configured with IP addresses used by the group control transport and the redundancy state transport. These IP addresses appear on the **local-ip** statements under the **cs7 group** command and the **ipc zone default/association** commands. Both the Manager and Alternate will transition to a group state of *ManagerIsolated*. This can be verified by issuing the **show cs7 group state** command.
5. Immediately save the Manager configuration and reload the Manager with the new ITP image.
6. When the Manager reloads and achieves a group state of *ManagerIsolated*, reactivate (**no shutdown**) all MTP2 links that physically reside on the Manager and verify that the traffic is being forwarded by the Manager.

Steps 7 - 10 are performed on the Alternate.

7. On the Alternate save any configuration changes to the startup-config that are required for the upgraded image (such as the name and location of the new image to be loaded). Then shutdown all MTP2 links that physically reside on the Alternate. This will redirect all traffic handled by the ITP Group through the Manager.
8. Immediately reload the Alternate with the new ITP image. The updated running-config that contains the **shutdown** commands for the MTP2 links does not have to be saved.
9. While the Alternate is reloading reactivate (**no shutdown**) the Ethernet interfaces on the Manager that were shutdown in Step 4). Ensure that this step is performed before the Alternate is fully initialized.
10. The Alternate will resume its role as the Alternate when it initializes and begin forwarding traffic on its MTP2 links when it has received its state information from the Manager.



Global Title Translation

A global title is an application address, such as an 800 number, calling card number, or mobile subscriber identification number. Global Title Translation (GTT) is the process by which the SCCP translates a global title into the point code and subsystem number of the destination SSP where the higher-layer protocol processing occurs.

Feature History for Global Title Translation

Release	Modification
12.2(33)IRA	Added support for this feature.
12.2(33)IRE	Added support for the GTT next table feature.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



Note

Configuration Mode Restrictions: Simultaneous changes to the configuration from multiple CLI sessions are not supported. Only one configuration session is allowed to enter in configuration mode at a time; other sessions should not enter in configuration mode. The **show line** or **show users EXEC** command may be used to determine the active user sessions on an ITP, and the **clear line EXEC** command may be used to ensure that only a single active session exists.

Contents

- [Overview of GTT Components, page 92](#)
This section describes the functional components of GTT and provides the basic commands to enable them.
- [Storing and Loading GTT Configuration Data, page 96](#)
GTT configuration data is stored and loaded differently than traditional router configuration data. This section describes how storing and loading works for GTT data files.
- [Modifying and Verifying the GTT Selector, page 104](#)

This section describes the commands for modifying the basic attributes of a GTT selector and displaying the GTT configuration.

- [Configuring GTT: 6 Scenarios, page 105](#)

This section describes the specific tasks and commands for configuring GTT, using 6 real-world scenarios.

- [Configuring the GTT Application Group, page 119](#)

This section describes the tasks and commands for specifying GTT application groups.

- [Configuring Global Title Address Conversion, page 121](#)

This section describes the tasks and commands for specifying Global Title Address (GTA) conversion mapping.

For information about specifying changes to Global Title fields when configuring the Instance Translation feature, see the “[Configuring Global Title Conversion](#)” section on page 70 of the “[Multiple Instances and Instance Translation](#)” chapter.

- [Verifying Global Title Translations, page 123](#)

This section describes the methods and commands for determining if GTT is performing properly.

- [Logging GTT Errors with the ITP Logging Facility, page 124](#)

This section describes the commands for logging GTT errors to a specified local or remote destination.

- [GTT Configuration Examples, page 126](#)

This section includes a full ITP configuration, including GTT.



Note

The GTT provisioning syntax and structure is based on GR-82 STP Generic Requirements - Telcordia Technologies, Issue 3 December 1999.

Overview of GTT Components

A global title is an application address, such as an 800 number, calling card number, or mobile subscriber identification number. Global Title Translation (GTT) is the process by which the SCCP translates a global title into the point code and subsystem number of the destination SSP where the higher-layer protocol processing occurs.

The two forms of GTT are described in detail in the [Configuring GTT: 6 Scenarios, page 105](#):

- Intermediate GTT -- A subsequent global title is required by another node, thus the routing indicator is set to zero, indicating *route by global title (gt)*.
- Final GTT -- No subsequent global title is required by another node, thus the routing indicator is set to 1, indicating *route by point code and ssn (pcssn)*.

The main components of GTT are described in the following sections:

- [GTT Selectors, page 93](#)
- [GTT Global Title Address Entries, page 93](#)
- [GTT Application Groups, page 94](#)
- [GTT Mated Application Entries, page 95](#)

GTT Selectors

A GTT Selector defines the parameters that select the translation table used to perform the translation of an SCCP message to its next or final destination. A GTT selector comprises a mandatory name, Translation Type (TT), and Global Title Indicator (GTI - only mandatory for ITU). In addition, an optional Numbering Plan (NP), Nature of Address Indicator (NAI), and Quality of Service (QOS) may be specified in certain cases.

GTT Selectors have 2 configuration modes:

- The global configuration mode allows configuration of new selectors or is used to enter the submode for modifying/updating an existing selector.
- The gtt selector configuration submode is used to modify certain attributes of the selector or used to update GTAs in the referenced selector.

Rules for Creating GTT Selectors

The following rules apply when configuring a GTT Selector:

- NP and NAI can not be specified if the variant is ANSI.
- GTI can be specified only if the variant is ITU.
- NP and NAI must be specified if GTI=4.
- The selector name must be unique and from 1 to 12 characters long.

To create a GTT selector, use the following command in global configuration mode:

Command	Purpose
Router(config)# cs7 gtt selector <i>selector-name</i> tt <i>tt</i> gti <i>gti</i> np <i>np</i>	Names and configures the GTT selector and enables CS7 GTT selector submode.

Rules for Modifying GTT Selectors

- A selector's TT, GTI, NP and NAI cannot be modified once they have been added. A selector must be completely deleted to change these values.
- If a QoS class is entered for a selector, it must have been defined prior to being used by the selector.
- If a new name is given for the selector, it must be unique and not longer than 12 characters.

Rules for Deleting GTT Selectors

- The selector name must exist.
- A selector cannot be deleted if it contains Global Title Address (GTA) entries.

GTT Global Title Address Entries

A Global Title Address (GTA) entry defines the result of a translation for a particular address mask. GTA entries are configured from the CS7 GTT selector submode. The result of a translation consists of:

- A new MTP3 Destination Point Code
- A new SCCP CDPA Routing Indicator (RI)
- A new SCCP CDPA Subsystem Number (SSN)

- A new SCCP CDPA Translation Type (TT) (mutually exclusive with SSN)
- A GTT Application Group (mutually exclusive of all of the above)
- A QoS Class
- An M3UA or SUA AS name

Rules for Adding GTA Entries

- A solitary GTT Mated Application (MAP) entry is automatically created when the routing indicator keyword is **pcssn** and a subsystem number (*ssn*) is specified.
- There must be room to add the MAP entry if required, since there is a maximum of 10 subsystems per point code in the GTT Mated Application table including one default entry for ssn 1. (See [GTT Mated Application Entries](#), page 95.)
- The routing indicator keyword must be **gt** if a new translation type (**ntt**) is specified.
- A TT and SSN cannot both be specified.
- The PC should not be equal to the node's self PC, capability point code, or secondary PC.
- 1 to 15 digits may be specified for the GTA. (Valid range is 0 through F hexadecimal.)
- The GTA digits must be unique for the GTA Table.
- If a GTT Application group name is specified, it must already exist in the GTT Application Group table.
- If the routing indicator is **pcssn**, indicating final GTT, but no SSN is specified, then at least one GTT MAP entry must exist for the specified PC.

To specify a GTA, use the following commands as appropriate to your needs, in CS7 GTT selector submode:

Command	Purpose
Router(config-cs7-gtt-selector)# gta gta app-grp app-grp	Defines a GTA that translates to a GTT application group.
Router(config-cs7-gtt-selector)# gta gta asname as-name {gt pcssn} [ssn ssn ntt newtt sccp-allow-pak-conv number pam pam-name]	Defines a GTA that translates to an M3UA or SUA Application Server name.
Router(config-cs7-gtt-selector)# gta gta pcssn pc {gt pcssn} [ssn ssn ntt newtt sccp-allow-pak-conv number pam pam-name]	Defines a GTA entry that translates to a point code and optional subsystem number.

GTT Application Groups

A GTT Application group is an alternative result for the explicit PC and SSN in a GTA entry. A GTT application group should be used instead of the PC/SSN result in the following cases:

- When more than 1 backup is required for a destination
- When load sharing across more than 2 destinations is required
- When load sharing for intermediate GTT destinations is required
- When a different backup is required for the same primary destination dependent on the GTA
- When a different RI value is desired dependent on the destination selected from the application group

- When a point code backup is required for an M3UA or SUA AS, or vice versa
- When performing a weighted load sharing with traffic received with the same calling party address routed to the same destination

GTT Application groups have 2 configuration modes:

- The top-mode allows configuration of new group names or is used to enter the submode for modifying/updating an group or group item.
- The submode is used to modify certain attributes of the group or used to update entries in the group.

GTT Mated Application Entries

A GTT Mated Application (MAP) entry has two main purposes. It is used internally by the SCCP application to track point code and SSN states such as congestion and availability. In addition it is used to define backups or alternates for a particular PC/SSN combination. An entry in the GTA table that contains a PC and SSN will have a corresponding entry in the MAP table. The entry in the MAP table may be modified to work in 1 of 3 modes:

- Solitary—No alternate if PC and/or SSN is not available
- Shared—Load shared equally across the primary PC/SSN and backup PC/SSN
- Dominant—Always translate to primary PC/SSN if available, and only translate to backup if primary is unavailable

Rules for Configuring GTT MAP Entries

The following rules apply:

- A backup point-code and subsystem must be specified if mode (multiplicity) is shared or dominant.
- A backup point-code and subsystem cannot be specified if mode (multiplicity) is solitary.
- A PC/SSN entry cannot be deleted if it is being used as a backup by another PC/SSN entry. (See [Rules For Removing GTT Configurations](#):, page 105)
- A PC/SSN entry cannot be deleted if it is referenced by an entry in the GTA table. (See [Rules For Removing GTT Configurations](#):, page 105)
- The primary and backup point-code should not be identical.
- There is a maximum of 10 subsystems per point-code allowed, including 1 default entry for SSN 1.
- The PC should not be equal to the node's self PC, capability PC, or secondary PC.

To configure a GTT MAP entry, use the following command in global configuration mode:

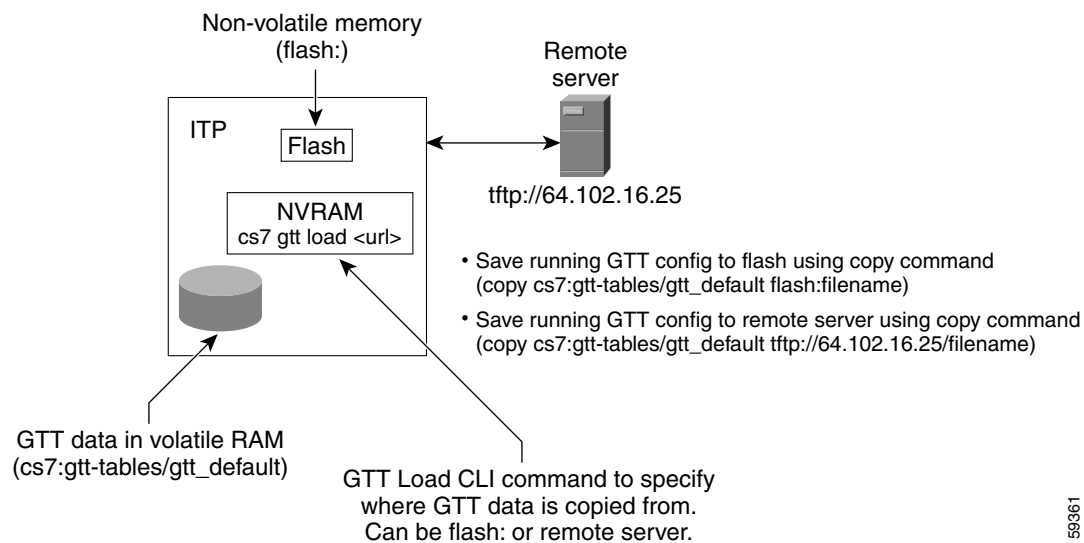
Command	Purpose
Router(config)# cs7 gtt map <i>ppc pssn [flags] mult [bpc] [bssn]</i>	Specify a GTT MAP entry.

Storing and Loading GTT Configuration Data

GTT configuration data is stored and loaded differently than traditional router configuration data. GTT configuration commands are not stored in non-volatile RAM (NVRAM), so commands such as **write memory** and **show running config** have no effect. Figure 10 shows the GTT data relationships on an ITP. This section describes:

- Loading a GTT Table from a Remote File Server or Flash (No existing GTT Data), page 96
- Loading a GTT Table from a Remote File Server or Flash (Existing GTT Data), page 97
- Bulk Loading/Replacing GTT Database, page 98
- Syntax and Format Rules for Creating a GTT Database Download File, page 98

Figure 10 GTT Table Loading



In order to preserve a GTT configuration across ITP reloads, you must use the GTT Table Loading feature.



Warning

All GTT data will be lost during a router reboot if you do not use the GTT Table Loading procedure.

Loading a GTT Table from a Remote File Server or Flash (No existing GTT Data)

The steps for loading a GTT table when the ITP has no existing GTT data are as follows:

- Step 1** Determine the desired default location for the GTT file to be loaded during ITP reloads. The default location can be either Flash or a remote server. For example, if the GTT file is to be loaded from Flash, the URL would be similar to the following:

```
flash:gttdata.txt
```

If the GTT file is to be loaded from a remote server, the URL would be similar to the following:

```
tftp://64.102.16.25/gttdata.txt
```

Step 2 Specify that the GTT file is to be loaded into RAM during subsequent ITP reloads.

Command	Purpose
Router(config)# cs7 gtt load <i>URL</i>	Specify the URL location from which the GTT database will be loaded upon ITP reload.

For example, using the default location and filename flash:gttdata.txt, the command would be:

```
cs7 gtt load flash:gttdata.txt
```

Step 3 Save the **cs7 gtt load** definition to NVRAM with a **write memory** command.

Step 4 Configure all desired GTT data using the CLI.

Step 5 Save the GTT data to the file specified in step 2 using the **copy** command or the **cs7 save gtt-table** privileged EXEC command as in the following example:

```
cs7 save gtt-table flash:gttdata.txt
```



Note

The file “cs7:gtt-tables/gtt_default” is a machine generated file. Its format is not meant for hand editing. It is recommended the CLI or an externally provided GUI product be used to configure GTT data, rather than editing the gtt_default file.

Steps 4 and 5 can be repeated for subsequent updates of GTT data.



Note

Whenever a GTT configuration is performed for an instance, you have to perform a specific save and load of the GTT configuration for this instance.

Loading a GTT Table from a Remote File Server or Flash (Existing GTT Data)

For an existing system with GTT data, to execute the load command immediately use the following command in global configuration mode:

Command	Purpose
Router(config)# cs7 gtt load <i>URL</i> [execute]	Specify the URL location of the GTT database and, optionally, load it now.

Bulk Loading/Replacing GTT Database

It may be desirable to replace the entire contents of a GTT database with a new database without rebooting the ITP. The **cs7 gtt load** command discussed above does not support this capability. To perform a bulk load of the entire GTT database without the need to reboot an ITP, use the following command in privileged EXEC mode:

Command	Purpose
Router# cs7 gtt replace-db <i>URL</i> Are you sure? [confirm] GTT table: <i>URL</i> , loaded successfully.	Replace the entire contents of a GTT database with a new database without rebooting the ITP.

Syntax and Format Rules for Creating a GTT Database Download File

This section describes the syntax and format of the text file used to store and load GTT information on the ITP. This information may be useful for advanced users who require the ability to generate GTT tables offline and then load the GTT Database file onto the ITP.

Since GTT data is not preserved in NVRAM, and the maximum size of GTT data can be up to 500,000 entries, a separate compressed format (comma separated) is provided to represent GTT data configured on the ITP. The text file is generated by the ITP when GTT data is saved to a file.

Command Identifiers in a GTT Database Download File

Table 4 shows the command identifiers supported by the GTT table download format. Each line in the text file is identified with a one-character string. All command identifiers except **v** may be prefixed with a “**d**” to indicate a delete action. Otherwise the action is assumed to be an add action. A modify action occurs only when the item already exists and one or more attributes have changed. The table shows the command identifier and the action it specifies.

Table 4 GTT Database Download File Command Identifiers

Command Identifier	Action
v	Add or modify the format version of the GTT configuration file. Must be the first command in the GTT configuration file because it identifies which parameters are valid within the various commands.
s	Add or modify GTT Selector.
ds	Delete Selector.
g	Add or modify GTT GTA.
dg	Delete GTT GTA.
a	Add or modify GTT Application Groups or items in the group.
da	Delete GTT Application Groups or items in the group.
m	Add or modify GTT MAP.
dm	Delete a GTT MAP.
c	Add or modify a Concerned Point Code List.
dc	Delete a Concerned Point Code List or item in the list.

Table 4 *GTT Database Download File Command Identifiers (continued)*

p	Add or modify a GTT address conversion entry.
dp	Delete a GTT address conversion entry

Syntax Rules:

- All lines must be terminated with a '\n' (unix eol).
- All tokens are comma separated.
- Each line is parsed for syntax checks and then checked for semantics.
- If a line is parsed and fails either syntax or semantic checks the download process is aborted at the point of failure.

Parameter Values in GTT Database Download Files

This section describes the values of the parameters that you use with the command identifiers when you create a GTT database download file.

The first line in any GTT file must indicate the version and variant of the GTT file. [Table 5](#) lists the current GTT table versions by ITP software version.

Table 5 *GTT File Version*

ITP Software Rel	GTT Table Version
MB4	1.0
MB5	2.0
MB6	2.0
MB7	3.0
MB8	3.0
MB9	3.1
MB9A	3.1
MB10	4.0
MB11	4.0
MB12	4.0
MB13	4.0
12.2(20)SW	4.1
12.2(21)SW1	4.2
12.2(23)SW	4.2
12.2(23)SW1	4.3
12.2(25)SW	4.3

[Table 6](#) lists the values for each parameter of the GTT commands that can be specified in a GTT database download file.

Table 6 GTT Command Parameter Values

Parameter	Valid Values
<i>version</i>	GTT Table Version - 1.0, 2.0, 3.0, 3.1, 4.0, 4.1, 4.2, 4.3(See Table 5)
<i>variant</i>	Variant - {ANSI, ITU, CHINA}
<i>selector name</i>	Name of Selector - alphanumeric string maximum of 12 chars
<i>tt</i>	Translation Type - integer {0-255}
<i>gti</i>	Global Title Indicator- integer {2,4}
<i>np</i>	Numbering Plan - integer {0-15}
<i>nai</i>	Nature of Address Indicator - integer {0-127}
<i>es</i>	Encoding scheme for the address conversion result {0-2}
<i>qos</i>	Quality of service Class identifier {1-7}
<i>gta</i>	Global Title Address Digits - numeric/hex sting 1 to 15 digits
<i>pc</i>	Destination point code in hex
<i>ri</i>	Routing indicator { gt , pcssn }
<i>ssn</i>	Subsystem Number - integer {2-255}
<i>ntt</i>	New Translation Type - integer {0-255}
<i>app-grp</i>	Application Group name - alphanumeric string maximum of 12 chars
<i>group-name</i>	Application Group name - alphanumeric string maximum of 12 chars
<i>mult</i>	Multiplicity { sol , dom , sha , cos }
<i>mult.1</i>	Multiplicity { sha , cos }
<i>mult.2</i>	Multiplicity { sha , cos , cgp }
<i>cost</i>	Cost or priority of destination {1-8}
<i>ppc</i>	Primary point code in hex
<i>pssn</i>	Primary Subsystem Number - integer {2-255}
<i>bpc</i>	Backup point code in hex
<i>bssn</i>	Backup Subsystem Number - integer {2-255}
<i>concern pc list name</i>	Concerned Point Code List Name - alphanumeric string maximum of 12 chars.
<i>rrc</i>	Boolean Re-Route if Congested - integer {0,1}
<i>adj</i>	Boolean Adjacency indicator {0,1}
<i>pre-addrconv</i>	Name of address conversion table - alphanumeric string maximum of 12 chars.
<i>post-addrconv</i>	Name of address conversion table - alphanumeric string maximum of 12 chars.
<i>network-name</i>	Network name of instance - alphanumeric string maximum of 12 chars.

Examples of Entries in a GTT Database Download File

This section provides the syntax and examples of entries in a GTT database:

Version and Variant

To specify the version of the GTT configuration file and the variant, use the syntax appropriate to your version:

- Syntax for version 1.0 to 3.0:

v,*version*,*variant*

Examples:

```
v1.0,ITU
v2.0,ANSI
v3.0,CHINA
```

- Syntax for version 4.0: In version 4.0 the ITP software supports multiple variants via the use of multiple instances. Each instance is assigned a variant.

v,*version*,*variant*,*instance*

Example:

```
v4.0,ANSI,0
```

- Syntax for version 4.1 and 4.2

v,*version*,*variant*,*instance*,*network-name*

Example:

```
v4.1,ITU,0,itu-national
```

GTT Selector

To add, modify, or delete a GTT Selector:

- Syntax:

[d]*sselectorname*,*tt*,*gti*,*[np]*,*[nai]*,*[qos]*,*[pre-addrconv]*,*[post-addrconv]*

Examples:

```
stest,0,4,7,4,1
stestsel,0,2, , ,
sa12345672,100,4,15,127,
```

GTT GTA

To add, modify, or delete a GTT GTA:

- Syntax for version 1.0:

[d]*gselectorname*,*gta*,*[pc]*,*[ri]*,*[ssn]*,*[ntt]*,*[app-grp]*,*[qos]*

Examples:

```
gtest,349,1012,gt,100, , ,
gtest,828,1012,gt, ,100, ,
gtest,828258,1012,pcssn,129, , ,
gtest,8282588595,1012,pcssn,100, ,1,
gtest,919, , , , ,test,
gtest,920, , , , ,test,
gtest,980,859,pcssn,10, , ,
```

- Syntax for version 2.0 to 4.1:

[d]*gselectorname*,*gta*,*[pc]*,*[ri]*,*[ssn]*,*[ntt]*,*[app-grp]*,*[qos]*, *[asname]*

Examples:

```

gtest,349,1012,gt,100, , ,
gtest,828,1012,gt, ,100, ,
gtest,828258,1012,pcssn,129, , ,
gtest,8282588595,1012,pcssn,100, ,1,
gtest,919, , , , ,test,
gtest,920, , , , ,test,
gtest,980,859,pcssn,10, , ,
gtest,999, , , , , ,sua_as1

```

- Syntax for version 4.2:
Same as previous except *ssn* may be **0** when *ri* is **gt**.

GTT Application Groups

To add, modify, or delete a GTT Application Group:

- Syntax for version 1.0:
`[d]agroup-name,[mult.I],cost,pc,ri,[ssn]`
Example:
`aapp0,cost,1,1012,gt,`
- Syntax for version 2.0:
`[d]agroup-name,[mult.I],cost,pc,ri,[ssn],[asname]`
Example:
`aapp0,cost,1, , , ,as0`
- Syntax for version 3.0:
`[d]agroup-name,[mult.I],cost,pc,ri,[ssn],[asname]`
No syntax change, but can enter local-pc in table.
Example:
`aapp1,sha,1,10203,pcssn, ,`
- Syntax for version 3.1:
`[d]agroup-name,[mult.I],cost,pc,ri,[ssn],[asname]`
No syntax change, but allows 8 items with same cost
Example:
`aapp1,sha,1,10203,pcssn, ,`
- Syntax for version 4.0:
`[d]agroup-name,[mult.2],cost,pc,ri,[ssn],[asname]`
CGPA load sharing introduced
Example:
`aapp1,cgp,1,20203,pcssn, ,`
- Syntax for version 4.1:
The item in the application group can be in a different instance than the application group. The *network-name* parameter is added to indicate the instance to which the item belongs.
`[d]agroup-name,[mult.2],cost,pc,ri,[ssn],[asname],[network-name]`

Example:

```
aapp1,cgp,1,20203,pcssn,5, ,instance1
```

- Syntax for version 4.2:

Unchanged, except *ssn* may be 0 for intermediate GTT.

Example:

```
aapp1,cos,1,10203,pcssn,5, ,instance1
```

GTT MAP

To add, modify or delete a GTT MAP:

- Syntax for version 1.0 and 2.0

```
[d]mppc,pcssn,mult,[bpc],[bssn],[concern pc list name],[rrc],[adj]
```

- Syntax for version 3.0 to 4.2 adds support for local-pc in the MAP table.

Examples:

```
m809,10,sol,,,0,0
m859,10,sol,,,0,0
m861,10,sol,,,0,0
m1012,10,sol,,,0,0
m859,20,sha,861,20,,0,1
m859,25,dom,861,25,,1,0
```

Concerned PC Lists

To add, modify, or delete a Concerned PC List:

- Syntax for version 1.0 to 3.0

```
[d]cconcern pc list name,pc
```

Examples:

```
clist1,809
clist1,859
clist3,1012
```

- Syntax for version 4.0

```
[d]cconcern pc list name,pc,instance
```

Example:

```
clist1,1024,1
```

Address Conversion Tables

To add, modify, or delete an address conversion table:

- Syntax for version 1.0 to 4.2

```
[d]paddress conversion table name,[np],[nai],gta,[gta],[np],[nai]
```

- Syntax for version 4.3

```
[d]paddress conversion table name,[np],[nai],gta,[gta],[np],[nai],[es]
```

Modifying and Verifying the GTT Selector

You can modify certain attributes of a selector in addition to using the selector for its primary purpose of updating GTAs. To modify attributes of the selector, use the following commands in the `cs7 gtt` selector submode.

To configure the default GTT entry in a GTT table to point to another GTT table (next table) in the same instance, use the following command:

Command	Purpose
Router(config-cs7-gtt-selector)# next-table <i>selector-name</i>	Configures the default GTT selector to point to a next table.

To change the name of the selector, use the following command:

Command	Purpose
Router(config-cs7-gtt-selector)# new-name <i>selector-name</i>	Renames the GTT selector.

After you have defined a GTA address conversion table, you can apply the table on a GTT selector basis. To specify the global title address conversion table to apply either prior to or after performing local global title translation, use either of the following commands:

Command	Purpose
Router(config-cs7-gtt-selector)# pre-gtt-address-conversion <i>tablename</i>	Specifies the global title address conversion table to apply prior to performing local global title translation.
Router(config-cs7-gtt-selector)# post-gtt-address-conversion <i>tablename</i>	Specifies the global title address conversion table to apply after performing local global title translation.

Since the GTT data is not stored in NVRAM, commands such as **show running config** will not display the GTT data. To display the current running configuration regarding GTT use the **show cs7 gtt config** command in privileged EXEC mode:

```
ITP# show cs7 gtt config
cs7 instance 0 gtt selector cs7test0 tt 0 gti 4 np 1 nai 3
  gta 33333 pcssn 1.5.4 gt
  gta 333  asname gg pcssn
next-table name cs7test1
cs7 instance 0 gtt selector cs7test1 tt 1 gti 4 np 1 nai 2
  gta 22222 pcssn 2.5.4 gt
  gta 222  asname mm pcssn
```

To display the CS7 GTT selectors, use the **show cs7 gtt selector** command in privileged EXEC mode:

```
ITP# show cs7 gtt selector
Selector Name   TT   GTI   NP   NAI   DFLTQOS   #GTAs
-----
c7gsp           0     4     1     3           3
itp_gtt         0     4     0     4           1
```

Configuring GTT: 6 Scenarios

The following sections describe how to configure GTT data on the ITP for different scenarios applicable to real customer networks. The scenarios include:

- [Configuring Intermediate GTT To Route MSUs to a Single Point Code, page 105](#)
- [Configuring Intermediate GTT To Load Balance MSUs Across Two Or More Point Codes, page 107](#)
- [Configuring Final GTT To Route MSUs to a Solitary Point Code, page 110](#)
- [Configuring Final GTT To Route MSUs to a Primary and Backup Point Code and SSN \(Dominant Mode\), page 113](#)
- [Configuring Final GTT To Load Balance MSUs Across a Group of Point Codes and Subsystems, page 116](#)
- [Configuring Final GTT to an SUA AS with a Backup Point Code \(Dominant Mode\), page 118](#)

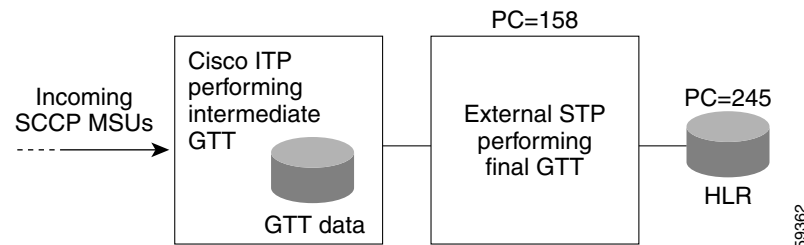
Rules For Removing GTT Configurations:

- To delete a selector you must first delete any GTAs that reference it, using the **no gta** command. After deleting the GTAs, you can remove the selector, using the **no selector** command.
- To delete a mated application (GTT MAP), you must first delete any application groups and GTAs that reference it (using the **no cs7 gtt application-group** command and **no gta** command). You can then delete the mated application configuration using the **no cs7 gtt map** command.
- To delete a map entry that references another map entry as a backup, change all entries that reference it to “solitary” then delete the map entry with the **no cs7 gtt map** command. You cannot directly delete the map entry with backup pc/ssn using the **no cs7 gtt map** command.
- To delete an application group that is referenced by a GTA, you must first delete the GTA using the **no gta** command. After deleting the GTA, you can remove the application group with the **no cs7 gtt app-grp** command.

Configuring Intermediate GTT To Route MSUs to a Single Point Code

This configuration describes the scenario shown in [Figure 11](#).

Figure 11 *Intermediate GTT With One Destination*



The ITP on the left side of [Figure 11](#) is required to perform intermediate GTT for a set of digits (GTAs). There is only 1 choice for the next destination regardless of its availability. All SCCP traffic that requires GTT and that matches the configured digits is to be GTT routed to the destination PC=158.

Provisioning the ITP

To provision the ITP, perform the following steps:

- Step 1** Determine the criteria needed to select the appropriate translation table. For ITU the most common Global Title Indicator is 4. This means a TT, NP and NAI identify the translation table. For ANSI, only the TT is required. For this example we will use TT=0, NP=1, NAI=3.



Note The choices of TT, NP, and NAI are application specific. Refer to the SS7 network administrator to determine the appropriate combination of TT, NP, and NAI. ITU-T Q.714 Specifications of Signaling System No. 7- Signaling Connection Control Part defines many of the well-known applications.

- Step 2** Determine if a GTT Selector matching the criteria stated above already exists:

Command	Purpose
Router# show cs7 gtt selector	Display GTT selector information.

If a matching GTT selector exists, it can be referenced by its text name. If not, a new selector must be created. For this example assume it does not exist and the name **c7gsp** will be used.

- Step 3** Determine the range of digits from the called party address (CDPA) that need to be routed to PC=158. In this example assume that any digits matching the prefix 3330810 need to be GTT routed to PC=158. All GTA digits entered on the ITP are prefix matched against the actual digits arriving in the MSU requiring GTT. When 3330810 is provisioned on the ITP it really means 3330810xxxxx... where x is any digit. The ITP currently supports prefix matching from 1 to 15 digits (1 - 9 and hex characters A - F).

Configuring the ITP GTT Database

Once the above criteria are determined, follow these steps to configure the ITP GTT database:

- Step 1** Configure the selector:

Command	Purpose
Router(config)# cs7 gtt selector selector tt tt gti gti np np nai nai	Names and configures the GTT selector and enters CS7 GTT selector submenu.

Using the details of the example, the command would be:

```
cs7 gtt selector c7gsp tt 0 gti 4 np 1 nai 3
```

In this simple case only one translation needs to be added within the selector.

- Step 2** Configure the GTA within the selector:

Command	Purpose
Router(config-cs7-gtt-selector)# gta gta result-type pc routing-indicator	Names and configures the GTA.

The result type is used to specify whether the GTA will be routed to a specific point code and optional SSN (pcssn) or to an application group (app-grp). In this case the result type is pcssn which allows the operator to specify a specific point code (pc=158). An SSN is not used in this example:

```
gta 3330810 pcssn 158 gt
```

The above command can be referred to as a GTA rule. The rule states that the CDPA digits matching 3330810 will be routed to a point-code and optional subsystem number (pcssn). The point-code is 158, the subsystem number in this example is not defined and the routing indicator is set to 'gt' indicating intermediate GTT. Omitting a new SSN in the rule causes the original SSN to be preserved during the translation.

Step 3 Exit the submode and verify the data entered:

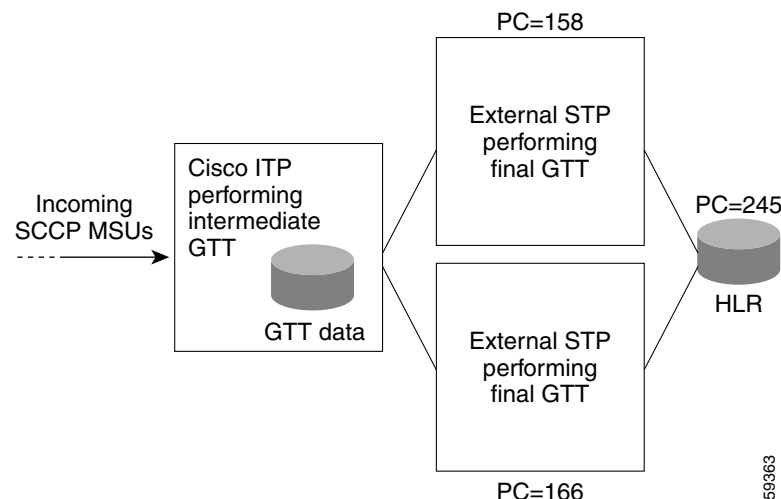
Command	Purpose
Router(config-cs7-gtt-selector)# exit	Exits CS7 GTT selector submode.
Router(config)# exit	Exits global configuration mode.
Router# show cs7 gtt gta selector [digits]	Displays details about the given GTA.

To delete a GTT configuration, follow the rules in the [“Rules For Removing GTT Configurations:”](#) section on page 105.

Configuring Intermediate GTT To Load Balance MSUs Across Two Or More Point Codes

This configuration describes the scenario shown in [Figure 12](#).

Figure 12 Intermediate GTT Shared Across 2 Destinations



This example is similar to the previous example except that instead of only 1 destination point-code a group of point-codes shall be used. For this example the mode (multiplicity) used to pick which point-code to choose from the group is **shared**. This means that all SCCP messages that matched the translation will be equally shared across the available destinations in the group in a round-robin fashion.

The MTP3 destination status is used to determine if the point code is available.

In [Figure 12](#) the ITP on the left side of the illustration is required to act as an intermediate translation point to the mated pair of STPs, which handle all final translations to a HLR. In this case the ITP is required to share all GTT routed traffic for a range of digits between a mated pair of STPs (PC=158 and PC=166).

Provisioning the ITP

To provision the ITP, perform the following steps:

-
- Step 1** Determine the criteria needed to select the appropriate translation table. For this example assume GTT selector criteria GTI=4, TT=0, NP=1, NAI=3. Also assume the appropriate selector already exists in the ITP GTT database.
 - Step 2** Define a GTT application group representing the mated pair of STPs (PC=158, PC=166) in the intermediate/shared mode.
 - Step 3** Determine the range of digits from the called party address (CDPA) that need to be routed to the application group containing PC=158 and PC=166. In this example assume that any digits matching the prefix 328 needs to be GTT routed to the application group.
-

Configuring the ITP GTT Database

Once the above criteria are determined the following steps may be followed to configure the ITP GTT database:

-
- Step 1** Define a GTT application group representing the mated pair of STPs in the intermediate/shared mode:

Command	Purpose
Router(config)# cs7 gtt application-group <i>group-name</i>	Assigns an application group name and enables the CS7 GTT application-group submode for adding items to the group.

Using the details of the example, the command would be:

```
Router(config)# cs7 gtt application-group intergroup1
```

- Step 2** Add the point-codes into the application group then exit application group submode:

Command	Purpose
Router(config-cs7-gtt-app-grp)# pc <i>point-code</i> <i>cost</i> <i>routing-indicator</i>	Adds a point code, cost, and routing indicator to the application group.
Router(config-cs7-gtt-app-grp)# exit	Exits CS7 GTT application-group submode.

Using the details of the example, the commands would be:

```
Router(config-cs7-gtt-app-grp)# pc 158 1 gt
Router(config-cs7-gtt-app-grp)# pc 166 2 gt
Router(config-cs7-gtt-app-grp)# exit
```

The default mode for the group is share, which does not have to be changed for this example. In shared mode, all items in an application group must be given a unique cost (1-8) as cost is a mandatory parameter. However, in the shared mode, the cost parameter is ignored and all provisioned items in the application group are shared equally. The cost can be thought of as an item number.

In the shared mode the cost can be thought of as an item number. Should the mode be changed to a “cost” mode, the method for choosing the next destination would switch from a round-robin scheme to a least cost available algorithm. (The cost is ignored when the group is share, and share is the default.) An example of using the cost mode is not shown, but can be thought of as follows:

Instead of sharing all traffic between the items in the group, pick the least cost item (1 being the least) and choose it always if available. If the least cost item is not available, choose the next least cost available item and route to it. If no items are available, drop message and initiate error and measurement procedures.

Step 3 Enter the submode configuration for the existing selector:

Command	Purpose
Router(config)# cs7 gtt selector selector	Enables the CS7 GTT selector submode for the given selector.

Using the details of the example, the commands would be:

```
Router(config)# cs7 gtt selector c7gsp
```

After performing the above step, the CLI enters selector submode for configuring translations options within the selector. In this simple case only one translation needs to be added within the selector.

Step 4 Configure the GTA within the selector:

Command	Purpose
Router(config-cs7-gtt-selector)# gta gta result-type app-grp	Names and configures the GTA for the given selector.

Using the details of the example, the command would be:

```
Router(config-cs7-gtt-selector)# gta 328 app-grp intergroup1
```



Note The application group intergroup1 may be used by as many GTT rules as needed. Avoid creating application groups with the same items in them.

The above command can be referred to as a GTA rule. The rule states that the CDPA digits matching 328 will be routed to the application group “intergroup1.” Using an application group allows destinations to be modified, added, or deleted without impacting the GTA table.

Step 5 Exit the submode and verify the data entered:

Command	Purpose
Router(config-cs7-gtt-selector)# exit	Exits CS7 GTT selector submode.

Command	Purpose
Router(config)# exit	Exits global configuration mode.
Router# show cs7 gtt gta selector [sgta sgta] [egta egta]	Displays details about the specified GTA.

Using the details of the example, the command and output would be:

```
Router# show cs7 gtt gta c7gsp

Selector Name      TT   GTI   NP   NAI   DFLTQOS   #GTAs
-----
c7gsp              0     4     1     3           2

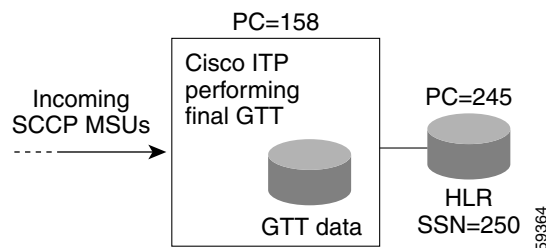
GTA
-----
3330810            158           gt
328                                intergroup1
```

To delete a GTT configuration, follow the rules in the [“Rules For Removing GTT Configurations:”](#) section on page 105.

Configuring Final GTT To Route MSUs to a Solitary Point Code

This configuration describes the scenario shown in [Figure 13](#).

Figure 13 ITP performing Final GTT to a Solitary Point Code



This example is similar to the previous example in that a solitary point-code is used. However, this example involves final GTT rather than intermediate GTT from the previous 2 examples. The main difference in intermediate vs. final GTT is the resultant routing indicator of the outgoing/translated message. The ITP also makes use of the Subsystem status when choosing the destination.

In [Figure 13](#) the ITP (PC=158) is required to perform final GTT to a HLR (PC=245/ SSN=250) for a specific range of digits from the CDPA. In this case the ITP is required to route all GTT traffic for the range of digits to an end node such as the HLR in this example.

Provisioning the ITP

To provision the ITP, perform the following steps:

-
- Step 1** Determine the criteria needed to select the appropriate translation table. For this example assume GTT selector criteria GTI=4, TT=0, NP=1, NAI=3. Also assume the appropriate selector already exists in the ITP GTT database.
- Step 2** Determine the range of digits from the called party address (CDPA) that need to be routed to the HLR. In this example assume that any digits matching the prefix 3335114 needs to be GTT routed to the HLR.
- Step 3** Determine if the ITP should replace the SSN in the called party with SSN=250 or the ITP should rely on the proper SSN already being set in the CDPA. In this example the ITP will implicitly replace SSN=250 in the called party regardless of any existing SSN.
-

Configuring the ITP GTT Database

Once the above criteria are determined the following steps may be followed to configure the ITP GTT database.

- Step 1** Enter the submode configuration for the existing selector:

Command	Purpose
Router(config)# cs7 gtt selector <i>selector</i>	Specifies the selector name and enables CS7 GTT selector submode for configuring translations options within the selector.

Using the details of the example, the command would be:

```
Router(config)# cs7 gtt selector c7gsp
```

After performing the above step, the CLI enters selector submode for configuring translations options within the selector. In this simple case only one translation needs to be added within the selector.

- Step 2** Configure the GTA within the selector:

Command	Purpose
Router(config-cs7-gtt-selector)# gta <i>gta result-type pc routing-indicator</i> ssn <i>ssn</i>	Names and configures the GTA for the given selector.

Using the details of the example, the command would be:

```
Router(config-cs7-gtt-selector)# gta 3335114 pcssn 245 pcssn ssn 250
```

The above command can be referred to as a GTA rule. The rule states that the CDPA digits matching 3335114 will be routed to a point-code and subsystem. The point-code is 245 and the SSN=250. The resultant routing indicator shall be set to **pcssn**, indicating final GTT (route on point code and subsystem). Since the SSN was specified as 250, it will override any SSN that previously existed in the called party. Conversely if the SSN was not specified in this rule, the ITP would try to route to whatever subsystem existed in the CDPA.

- Step 3** Exit the submode and use the **show cs7 gtt** commands to verify the data entered:

Command	Purpose
Router(config-cs7-gtt-selector)# exit	Exits CS7 GTT selector submode.
Router(config)# exit	Exits global configuration mode.
Router# show cs7 gtt gta gta	Displays details about the specified GTA.
Router# show cs7 gtt map	Displays details about the GTT MAP entries.

Using the details of the example, the show command and output would be:

```
Router# show cs7 gtt gta c7gsp
```

```

Selector Name   TT   GTI   NP   NAI   DFLTQOS   #GTAs
-----
c7gsp           0     4     1     3           3

GTA             PC             RI     SSN   TT   App-Grp   QOS   ASname
-----
3330810         158             gt
3335114         245             pcssn  250
328                                     intergroup1

```

```
Router# show cs7 gtt map
```

```

PPC      PSSN   MULT   BPC           BSSN   ConPCLst       RRC ADJ   Ref
245      250    sol   -----    ---
off no    1

```

Table 7 describes the fields in the **show cs7 gtt map** display.

Table 7 *show cs7 gtt map Field Descriptions*

Field	Description
PCC	Primary Point Code
PSSN	Primary Subsystem Number
Mult	Multiplicity (load share mode)
BPC	Backup Point Code for Primary Point Code
BSSN	Backup Subsystem Number for Primary Subsystem Number
ConPCLst	Concerned point-code list name. Concerned point-code lists are created using the cs7 gtt concern-pclist command. All destinations in the list are notified when a subsystem status change occurs. Concerned point-code lists are optional for all GTT MAP entries.
RRC	Reroute to backup if primary is congested Used to tell SCCP routing if the backup should be used when the primary is congested. Default is OFF.
ADJ	Adjacency flag. Used to signify if a PC/SSN should be considered adjacent to local node in regards to SCCP management. Default is NO.
Ref	Reference Count. Indicates how many times a MAP entry is referenced by GTA or application group entries. A referenced MAP can not be removed.

**Note**

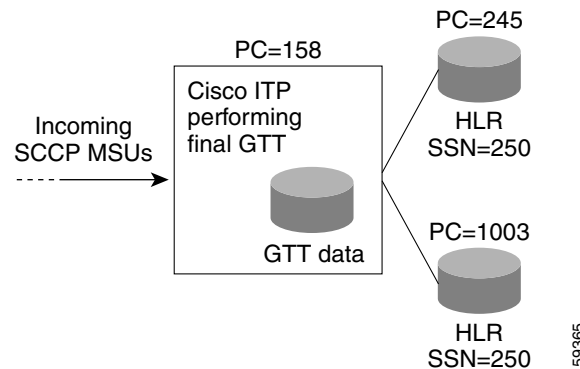
Whenever final GTT is provisioned with an explicit subsystem from a GTA entry such as the one for GTA=3335114, a GTT MAP (Mated Application) entry is required. The ITP will automatically create a solitary MAP as needed when the GTA entry is created. The GTT MAP entry is used internally by the ITP to manage the status of a subsystem. The operator could have pre-provisioned this MAP entry prior to configuring the GTT using the **cs7 gtt map** command. For an example where the MAP is provisioned prior to the GTA see the [“Configuring Final GTT To Route MSUs to a Primary and Backup Point Code and SSN \(Dominant Mode\)” section on page 113](#). The MAP can also be used to define a mate point-code for the primary point-code. This is an alternative to using application-groups, which take up more memory.

To delete a GTT configuration, follow the rules in the [“Rules For Removing GTT Configurations:” section on page 105](#).

Configuring Final GTT To Route MSUs to a Primary and Backup Point Code and SSN (Dominant Mode)

This configuration describes the scenario shown in [Figure 14](#)

Figure 14 Final GTT routed to a primary and backup PC/SSN



This example is similar to the previous example in that final GTT is being performed. However, this example involves final GTT using a customized GTT MAP entry where a backup PC and SSN are also utilized.

In [Figure 14](#) the ITP (PC=158) is required to perform final GTT to a HLR (PC=245/ SSN=250) for a specific range of digits from the CDPA. Also suppose the HLR (PC=245) has a backup (PC=1003) in case of a failure. In this case the ITP is required to route all GTT traffic for a range of digits to the primary HLR if it is available. If the primary HLR becomes unavailable, the ITP is required to use the backup instead. This method of choosing the primary and backup subsystems is typically referred to as operating in the dominant mode. Backup point code support is provided only with GTT selector.

Provisioning the ITP

To provision the ITP, perform the following steps:

-
- Step 1** Determine the criteria needed to select the appropriate translation table. For this example assume GTT selector criteria GTI=4, TT=0, NP=1, NAI=3. Also assume the appropriate selector already exists in the ITP GTT database.
- Step 2** Determine the range of digits from the called party address (CDPA) that need to be routed to the HLR. In this example assume that any digits matching the prefix 339 needs to be GTT routed to the primary HLR (PC=245) if available or the backup HLR (PC=1003) if the primary is not available.
- Step 3** Determine if the ITP should replace the SSN in the called party with SSN=250 or the ITP should rely on the proper SSN already being set in the CDPA. In this example the ITP will implicitly replace SSN=250 in the called party regardless of any existing SSN.
- Step 4** Determine if a GTT MAP entry having the appropriate mode and backup criteria exists. For this example assume the GTT MAP entry does not exist and create it.
-

Configuring the ITP GTT Database

Once the above criteria are determined, follow these steps to configure the ITP GTT database:

- Step 1** Enter the GTT MAP entry:

Command	Purpose
Router(config)# cs7 gtt map <i>ppc pssn [flags] mode [bpc] [bssn]</i>	Specifies the GTT MAP definition.

Using the details of the example, the command would be:

```
Router(config)# cs7 gtt map 245 250 rrc dom 1003 250
```

The above command can be referred to as a GTT MAP definition. The definition dictates that PC=245 and SSN=250 is a primary application backed up in the dominant mode by PC=1003 and SSN=250. The rrc flag specifies that if the primary PC/SSN becomes congested we will re-route to the standby PC/SSN.

- Step 2** Enter the submode configuration for the existing selector:

Command	Purpose
Router(config)# cs7 gtt selector <i>selector</i>	Enables CS7 GTT selector submode for configuring translations options within the selector.

Using the details of the example, the command would be:

```
Router(config)# cs7 gtt selector c7gsp
```

In this simple case only one translation needs to be added within the selector.

- Step 3** Configure the GTA within the selector:

Command	Purpose
Router(config-cs7-gtt-selector)# gta <i>gta result-type point-code routing-indicator ssn ssn</i>	Configure the GTA for the given selector.

Using the details of the example, the command would be:

```
Router(config-cs7-gtt-selector)# gta 339 pcssn 245 pcssn ssn 250
```

The above command can be referred to as a GTA rule. The rule states that the CDPA digits matching 339 will be routed to a point-code and subsystem. The point-code is 245 and the SSN=250. The resultant routing indicator shall be set to 'pcssn' indicating final GTT (route on point code and subsystem). Since the SSN was specifically specified as 250, it will override any SSN that previously existed in the called party. Conversely if the SSN was not specified in this rule, the ITP would try to route to whatever subsystem existed in the CDPA. Since a GTT MAP entry was pre-defined and the PC=245 / SSN=250 exists in the GTT Mated Application entity set, a backup PC/SSN shall be used in the dominant mode with the rrc flag indicating re-route to backup if primary is congested.

Step 4 Exit the submode and verify the data entered:

Command	Purpose
Router(config-cs7-gtt-selector)# exit	Exits CS7 GTT selector submode.
Router(config)# exit	Exits global configuration mode.
Router# show cs7 gtt gta gta	Displays details about the given GTA.
Router# show cs7 gtt map	Displays details about the GTT MAP entries.

Using the details of the example, the show command and output would be:

```
Router# show cs7 gtt map
      PPC      PSSN  MULT  BPC      BSSN  ConPCLst      RRC ADJ  Ref
      245      250   dom   1003      250      on no    2
```



Note

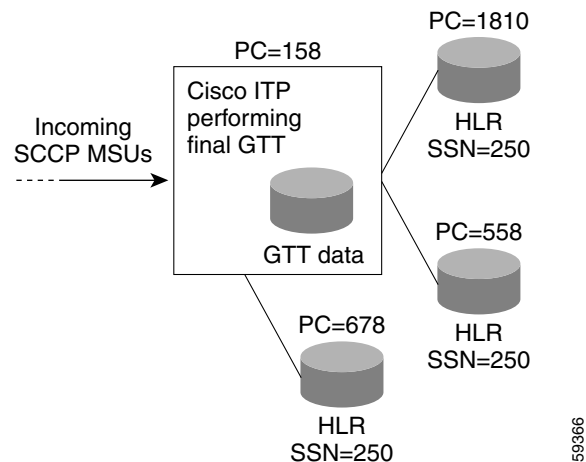
You can not delete any map entry that references another MAP entry. You must first change all entries that reference it to **sol** before you can delete the entry with the **no cs7 gtt map** command. To modify a MAP entry you must replace the entire command, including all keywords and arguments.

To delete a GTT configuration, follow the rules in the [“Rules For Removing GTT Configurations:”](#) section on page 105.

Configuring Final GTT To Load Balance MSUs Across a Group of Point Codes and Subsystems

This configuration describes the scenario shown in [Figure 15](#).

Figure 15 *Final GTT Load Balanced Across Multiple PC/SSN Nodes*



This example is similar to the example shown in [Figure 12](#) in that an application group name is being used rather than an explicit point-code or PC/SSN. However, this example involves final GTT instead of intermediate GTT.

In [Figure 15](#) the ITP (PC=158) is required to perform final GTT to an application existing on multiple end nodes to reduce the CPU load at any given single node. In this case the ITP is required to share all GTT traffic for a range of digits between multiple end nodes (in this case 3 shall be used - maximum of 8 destinations possible).

Provisioning the ITP

To provision the ITP, perform the following steps:

- Step 1** Define a GTT application group representing the 3 HLRs.
- Step 2** Determine the criteria needed to select the appropriate translation table. For this example assume GTT selector criteria GTI=4, TT=0, NP=1, NAI=3. Also assume the appropriate selector already exists in the ITP GTT database.
- Step 3** Determine the range of digits from the called party address (CDPA) that need to be routed to the HLR. In this example assume that any digits matching the prefix 900 needs to be GTT routed to the application group containing the 3 HLRs.
- Step 4** Determine if the ITP should replace the SSN in the called party with SSN=250 or the ITP should rely on the proper SSN already being set in the CDPA. In this example the ITP will implicitly replace SSN=250 in the called party regardless of any existing SSN.

- Step 5** Determine if GTT MAP entries for the 3 end nodes exist. For this example assume the 3 MAP entries already exist. Note: When final GTT is being performed with the use of application groups, the MAP entry is required for each PC/SSN, but the fields in the MAP entry such as the load share mode, bpc, bssn, and optional flags are ignored.

Configuring the ITP GTT

Once the above criteria are determined, follow these steps to configure the ITP GTT database:

- Step 1** Define a GTT application group representing the 3 HLRs in the final/shared mode.

Command	Purpose
Router(config)# cs7 gtt application-group <i>group-name</i>	Defines the GTT application group and enables CS7 GTT application-group submode.

Using the details of the example, the command would be:

```
Router(config)# cs7 gtt application-group finalgroup1
```

- Step 2** Add the point codes into the application group then exit the configuration submode for the application group:

Command	Purpose
Router(config-cs7-gtt-app-grp)# pc <i>point-code</i> ssn <i>ssn</i> <i>cost</i> <i>routing-indicator</i>	Adds the point codes to the application group.
Router(config-cs7-gtt-app-grp)# exit	Exits CS7 GTT application-group submode.

Using the details of the example, the commands would be:

```
Router(config-cs7-gtt-app-grp)# pc 1810 ssn 250 1 pcssn
Router(config-cs7-gtt-app-grp)# pc 558 ssn 250 2 pcssn
Router(config-cs7-gtt-app-grp)# pc 678 ssn 250 3 pcssn
Router(config-cs7-gtt-app-grp)# pc 1234 ssn 2 1 gt sccp-allow-pak-conv 1
Router(config-cs7-gtt-app-grp)# exit
```

- Step 3** Enter the submode configuration for the existing selector:

Command	Purpose
Router(config)# cs7 gtt selector <i>selector</i>	Enables CS7 GTT selector submode.

Using the details of the example, the commands would be:

```
Router(config)# cs7 gtt selector c7gsp
```

In this simple case only one translation needs to be added within the selector.

- Step 4** Configure the GTA within the selector:

Command	Purpose
Router(config-cs7-gtt-selector)# gta <i>gta result-type</i> <i>group-name</i>	Configures the GTA for the given selector.

Using the details of the example, the commands would be:

```
Router(config-cs7-gtt-selector)# gta 900 app-grp finalgroup1
```

The above command can be referred to as a GTA rule. The rule states that the CDPA digits matching 900 will be routed to the application group “finalgroup1.”

Step 5 Exit the submode and verify the data entered:

Command	Purpose
Router(config-cs7-gtt-selector)# exit	Exits CS7 GTT selector submode.
Router(config)# exit	Exits global configuration mode.
Router# show cs7 gtt application-group	Displays details about the GTT application groups.
Router# show cs7 gtt gta gta	Displays details about the given GTA.

Using the details of the example, the show commands and their output would be:

```
Router# show cs7 gtt application-group
Application Group Name: finalgroup1
Multiplicity           : share
Ref Count              : 1

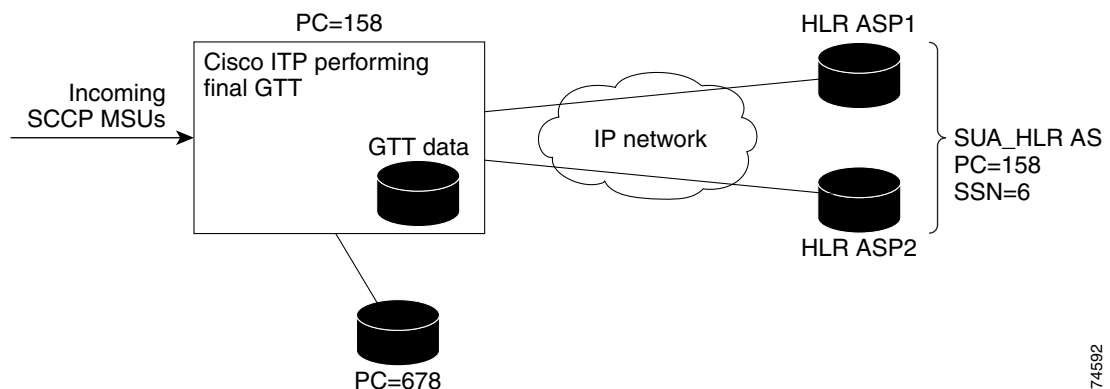
Application Identifier  RI      Cost
-----
PC=1810 SSN=250        pcssn  1
PC=558  SSN=250        pcssn  2
PC=678  SSN=250        pcssn  3
```

To delete a GTT configuration, follow the rules in the [“Rules For Removing GTT Configurations:” section on page 105](#).

Configuring Final GTT to an SUA AS with a Backup Point Code (Dominant Mode)

This configuration describes the scenario shown in [Figure 16](#).

Figure 16 Final GTT to an SUA AS with a Backup PC/SSN in SS7 Network



74592

This example is similar to the previous example in that final GTT is being performed. However, this example involves final GTT directly to an SUA AS name with a backup PC and SSN located via an SS7 linkset.

In [Figure 16](#) the ITP (PC=158) is required to perform final GTT to a primary HLR (PC=158/ SSN=6) for a specific range of digits from the CDPA. The primary HLR is composed of two SUA ASPs within an SUA AS in loadsharing mode. The routing key for the AS is sharing the ITP PC (PC=158) with an SCCP subsystem of 6.

The primary HLR (PC=158) has a backup (PC=678) in case of a failure. In this case, the ITP is required to route all GTT traffic for a range of digits to the primary HLR if it is available. If the primary HLR becomes unavailable, the ITP is required to use the backup HLR. This method of choosing the primary and backup subsystems is typically referred to as operating in the dominant mode, and is handled by using an application group.

Provisioning the ITP

To provision the ITP, perform the following steps:

-
- Step 1** Define a GTT application group representing the two HLRs. Note that two ASPs implement the SUA HLR, but the GTT database sees only a single SUA AS.
 - Step 2** Determine the criteria needed to select the appropriate translation table. For this example assume GTT selector criteria GTI=4, TT=0, NP=1, NAI=3. Also assume the appropriate selector already exists in the ITP GTT database.
 - Step 3** Determine the range of digits from the called party address (CDPA) that need to be routed to the HLR. In this example assume that any digits matching the prefix 900 need to be GTT routed to the application group containing the 2 HLRs.
 - Step 4** Determine if the ITP should replace the SSN in the called party with SSN=6, or if the ITP should rely on the proper SSN already being set in the CDPA. In this example, the ITP will explicitly write SSN=6 in the called party regardless of any existing SSN.
 - Step 5** Determine if a GTT MAP entry exists for the SCP HLR. For this example, assume the MAP entry already exists. Note: When final GTT is being performed with the use of application groups, the MAP entry is required for each PC/SSN, but the fields in the MAP entry such as the load share mode, bpc, bssn, and optional flags are ignored.
-

Configuring the GTT Application Group

Once the above criteria are determined, follow these steps to configure the ITP GTT database:

-
- Step 1** Define a GTT application group representing the 2 HLRs in the final/shared mode.

Command	Purpose
Router(config)# cs7 gtt application-group <i>group-name</i>	Defines the GTT application group and enables CS7 GTT application-group submenu.

Using the details of the example, the command would be:

```
Router(config)# cs7 gtt application-group finalgroup1
```

- Step 2** Add the SUA AS name, and the backup HLR point code into the application group, and then exit the configuration submode for the application group:

Command	Purpose
Router(config-cs7-gtt-app-grp)# asname <i>as-name</i> { <i>cost</i> [<i>ssn ssn</i>] { <i>gt</i> [<i>ntt ntt</i>] <i>pcssn</i> } [<i>rate-limit rate</i>] <i>wf</i> [<i>ssn ssn</i>] { <i>gt</i> [<i>ntt ntt</i>] <i>pcssn</i> }} [<i>sccp-allow-pak-conv number</i>]	Adds an SUA or M3UA AS name to the application group.
Router(config-cs7-gtt-app-grp)# pc <i>pc</i> [<i>ssn ssn</i>] { <i>cost</i> { <i>gt</i> [<i>ntt ntt</i>] <i>pcssn</i> } [<i>rate-limit rate</i>] <i>wf</i> { <i>gt</i> [<i>ntt ntt</i>] <i>pcssn</i> }} [<i>sccp-allow-pak-conv number</i>]	Adds a point code to the application group.
Router(config-cs7-gtt-app-grp)# exit	Exits CS7 GTT application-group submode.

Using the details of the example, the commands would be:

```
Router(config-cs7-gtt-app-grp)# asname SUA_HLR 1 ssn 6 pcssn
Router(config-cs7-gtt-app-grp)# pc 678 ssn 6 2 pcssn
Router(config-cs7-gtt-app-grp)# pc 1234 ssn 2 1 gt sccp-allow-pak-conv 1
Router(config-cs7-gtt-app-grp)# exit
```

- Step 3** Enter the submode configuration for the existing selector:

Command	Purpose
Router(config)# cs7 gtt selector <i>selector</i>	Enables CS7 GTT selector submode.

Using the details of the example, the commands would be:

```
Router(config)# cs7 gtt selector c7gsp
```

In this simple case only one translation needs to be added within the selector.

- Step 4** Configure the GTA within the selector:

Command	Purpose
Router(config-cs7-gtt-selector)# gta <i>gta result-type group-name</i>	Configures the GTA for the given selector.

Using the details of the example, the commands would be:

```
Router(config-cs7-gtt-selector)# gta 900 app-grp finalgroup1
```

The above command can be referred to as a GTA rule. The rule states that the CDPA digits matching 900 will be routed to the application group “finalgroup1.”

- Step 5** Exit the submode and verify the data entered:

Command	Purpose
Router(config-cs7-gtt-selector)# exit	Exits CS7 GTT selector submode.
Router(config)# exit	Exits global configuration mode.
Router# show cs7 gtt application-group	Displays details about the GTT application groups.
Router# show cs7 gtt gta <i>gta</i>	Displays details about the given GTA.

Using the details of the example, the show commands and their output would be:

```
Router# show cs7 gtt application-group
Application Group Name: finalgroup1
Multiplicity           : cost
Ref Count              : 1
```

Application Identifier	RI	Cost	PCST	SST	CONGESTED	AS ST	AVAIL
AS=SUA_HLR	pcssn	1					avail
PC=678 SSN=6	pcssn	2					avail

To delete a GTT configuration, follow the rules in the [“Rules For Removing GTT Configurations:”](#) section on page 105.

Configuring Global Title Address Conversion



Note

This section describes the tasks and commands for specifying Global Title Address (GTA) conversion mapping. For information about specifying changes to Global Title fields when configuring the Instance Translation feature, see the [“Configuring Global Title Conversion”](#) section on page 70 of the [“Multiple Instances and Instance Translation”](#) chapter.

Global Title Address conversion tables are used to specify mappings such as E.212 to E.214 address conversion and E.212 to E.164 address conversion in ITU networks. Global Title Address conversion includes the following capabilities and functions:

- The address conversion process is applied to digits in the Called Party address, and is invoked when RI=GT.
- The address conversion process is separately configurable, allowing for variable length address and resultant digit string (up to a maximum of 15 digits).
- For ITU networks, the numbering plan and nature of address indicator values in the GTA may be changed.
- Global Title Address conversion tables can be stored on local or network hard media, just as the GTT entries are.
- Global Title Address conversion table updates are allowed during router operation.
- Global Title Address conversion can occur before and/or after GTT.
- Initially, conversion rules perform a best match on the defined input addresses. Upon a successful match, the input address is replaced with the resultant, or output, address. The addresses are stored in a radix tree with the input address as the key.



Note

Since the GTT data is not stored in NVRAM, commands such as **show running config** will not display the GTT data. To display the current running configuration regarding GTT use the **show cs7 gtt config** command.

To define a address conversion table and enter GTT address conversion submode, use the following command in global configuration mode:

Command	Purpose
Router(config)# cs7 gtt address-conversion <i>tablename</i>	Specifies a GTT address conversion table name (1-12 characters) and enables CS7 GTT address conversion table submode.

To define an input address and an output address, use the following commands in CS7 GTT address conversion table submode:

Command	Purpose
Router(config-cs7-gtt-conv-tbl)# update [in-address <i>in-address</i>] [nai <i>nai</i>] [np <i>np</i>] [out-address <i>out-address</i>] [np <i>np</i>] [nai <i>nai</i>] [es <i>es-val</i>]	Defines input and (optionally) output address entries.

To define a new numbering plan for the entire table, use the following command in CS7 GTT address conversion submode:

Command	Purpose
Router(config-cs7-gtt-conv-tbl)# np <i>newnp</i>	Defines the new numbering plan value for the entire table. Only valid for ITU networks.

To define a new nature of address for the entire table (in ITU networks only), use the following command in CS7 GTT address conversion submode:

Command	Purpose
Router (config-cs7-gtt-conv-tbl)# nai <i>newnai</i>	Defines the new nature of address value for the entire table. Only valid for ITU networks.

After you have defined a GTA address conversion table, you can apply the table on a GTT selector basis. To specify the global title address conversion table to apply either prior to or after performing local global title translation, use either of the following commands in CS7 GTT selector submode:

Command	Purpose
Router(config-cs7-gtt-selector)# pre-gtt-address-conversion <i>tablename</i>	Specifies the global title address conversion table to apply prior to performing local global title translation.
Router(config-cs7-gtt-selector)# post-gtt-address-conversion <i>tablename</i>	Specifies the global title address conversion table to apply after performing local global title translation.

Verifying Global Title Translations

After the ITP is configured with GTT data and the links come into service, you can determine if the GTT and routing are working properly. This section describes three methods for verifying GTT:

- [GTT Measurements, page 123](#)
- [SCCP Accounting, page 123](#)
- [Subsystem Status, page 124](#)

GTT Measurements

You can display CS7 GTT measurements based on system, map, counters, selector, application-group, or line card.

To display a report for each PC/SSN combination, including the number of times it was used by a successful translation, use the following command in privileged EXEC mode:

Command	Purpose
Router# show cs7 gtt measurements map	Displays a report for each PC/SSN combination.

To display measurements kept on a Selector basis, use the following command in privileged EXEC mode:

Command	Purpose
Router# show cs7 gtt measurements selector <i>[selector]</i>	Displays a report for each selector.

To display measurements for the system, use the following command in privileged EXEC mode:

Command	Purpose
Router# show cs7 gtt measurements systot	Displays a system report.

To display measurements for the application group, use the following command in privileged EXEC mode:

Command	Purpose
Router# show cs7 gtt measurements application-group <i>name</i>	Displays GTT measurements kept on a application group basis.

SCCP Accounting

In addition to the GTT measurements that are kept on a system wide scale, Cisco ITP provides optionally configurable per linkset GTT accounting. In it's current implementation, GTT accounting provides a mapping between the linkset that packets come in on, the selector that they match, the GTA within that selector, and final translated point codes. This accounting is performed for successful GTT.

To display GTT accounting, use the following command in privileged EXEC mode:

Command	Purpose
Router# show cs7 accounting gtt-active	Displays the real time status of each entry in the GTT MAP table.

Subsystem Status

The ITP SCCP application must process SCCP management messages to track the status of remote subsystems. A GTT MAP entry should be created for all remote subsystems the ITP will be routing to via GTT. The ITP provides a method for displaying the real time status for any remote subsystem entered in its database. To display the status of a remote subsystem use the keyword **stat** in conjunction with the **show cs7 gtt map** privileged EXEC command:

Command	Purpose
Router# show cs7 accounting gtt-active	Displays the real time status of each entry in the GTT MAP table.

The following sample output of the **show cs7 accounting gtt-active** command shows the real-time status of each entry in the GTT MAP table:

```
Router# show cs7 gtt map stat
PC          SSN    PCST   SST    CONGESTED
668         250    UNAVL  avail  -----
1003        250    avail  avail  -----
1008        250    avail  UNAVL  -----
2020        250    avail  avail  level 2
```

Logging GTT Errors with the ITP Logging Facility

The ITP Logging Facility enables you to log GTT errors to a local or remote destination for post processing. The logging facility enables you to set an interval at which the log will be archived automatically or save the archive manually as you require. You can also display the current log as you require. These capabilities are shown in the following tasks. [Table 8 on page 125](#) lists and describes GTT errors.

To enable the ITP to log GTT errors, use the **cs7 log** command in global configuration mode:

Command	Purpose
ITP(config)# cs7 log type size size	Enables logging, specifies the logging type, and defines the maximum number of entries in the log. The valid range is 0 to 100000. When the 100000 limit is reached, new entries will overwrite existing entries, starting from the first entry.
Example: ITP(config)# cs7 cs7 log gtt size 1000005	

To enable automatic archiving of a log to a remote or local destination, use the **cs7 log checkpoint** command in global configuration mode:

Command	Purpose
ITP(config)# cs7 log type checkpoint secs destination	Enables archiving to a specified path and sets the archiving interval in seconds.
Example: ITP(config)# cs7 log gtt checkpoint 3600 tftp://10.1.1.2/logs/	

To save a log to a file, use the **cs7 save log** command in privileged EXEC mode:

Command	Purpose
ITP(config)# cs7 save log type destination	Detaches the current log from the active log process and saves it to a destination. New log entries that occur while the save is in progress are written to a new log file and are not lost. The logs are written in readable text format.
Example: ITP(config)# cs7 save log gtt tftp://10.1.1.3/logs/gttlog1.txt	

To display a log, use the **show cs7 log** command in Privileged EXEC mode:

Command	Purpose
ITP# show cs7 log type	Displays the current log.
Example: ITP# show cs7 log gtt	

GTT Error Log

Table 8 lists and describes GTT Errors:

Table 8 **GTT Error Log**

Error Text	Description
CdPA SSN does not exist in GTT MAP Table.	The ITP received an MSU requiring GTT routing for which the SSN in the called party was not configured in the ITP's GTT MAP table.
Translated DPC unavailable.	The ITP received an MSU requiring GTT routing for which the translated DPC in the ITP's GTT MAP table was marked as unavailable.
Translated DPC congested.	The ITP received an MSU requiring GTT routing for which the translated DPC in the ITP's GTT MAP table was marked as congested.
Translated SSN unavailable.	The ITP received an MSU requiring GTT routing for which the translated DPC/SSN in the ITP's GTT MAP table was marked as SSN unavailable.

Table 8 **GTT Error Log (continued)**

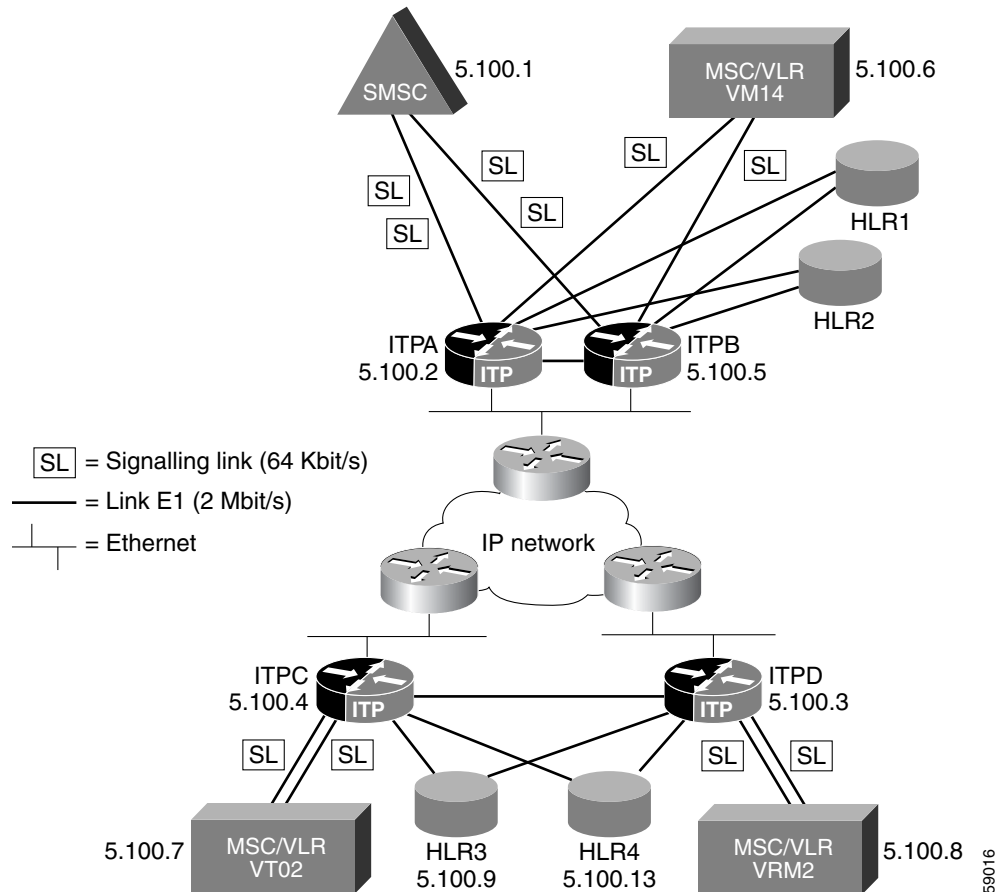
Error Text	Description
Translated SSN congested.	The ITP received an MSU requiring GTT routing for which the translated DPC/SSN in the ITP's GTT MAP table was marked as SSN congested.
CalledP GTI not valid.	The ITP received an MSU requiring GTT routing for which GTI in the SCCP called party was a value other than 2 or 4. These are the only supported values for GTI on the ITP.
CalledP missing SSN.	The ITP received an MSU requiring GTT routing for which the SSN in the called party was expected, but not present.
Invalid GT Type.	The ITP received a MSU destined to a local SSN of the wrong type.
No translation configured.	The ITP received an MSU requiring GTT routing for which no translation was configured in the GTT database.
Invalid or unsupported message type.	The ITP received an SCCP message with an unsupported or invalid msg type.
Hop Counter expired.	The ITP received an MSU requiring GTT routing for which the hop counter was expired.
Unqualified error.	The ITP received an MSU requiring GTT routing which resulted in error that could not be matched to any specific error message.
Unexpected MTP3 routing failure.	SCCP tried to route traffic to MTP3 which resulted in an unexpected routing failure.
Could not find corresponding GTT MAP entry.	The ITP received an MSU requiring GTT routing, but could not find a corresponding GTT MAP entry to verify PC/SSN status.
SCCP unavailable at translated DPC.	The ITP received an MSU requiring GTT routing, but SCCP was marked as unavailable at remote node.
No member available in GTT Application Group.	The ITP received an MSU requiring GTT routing, but no member was found available in the resultant GTT application group.
No matching GTT selector found.	The ITP received an MSU requiring GTT routing, but no matching GTT selector was found in the GTT database.
Network indicator mismatch.	SCCP received an MSU, but the network indicator field did not match the variant configured.
Instance conversion failed.	SCCP tried to route across instances, but instance conversion failed.

GTT Configuration Examples

This section includes examples for the following aspects of GTT configuration:

- [ITP GTT Configuration for ITPA Example, page 128](#)
- [ITP GTT Configuration for ITPB Example, page 130](#)
- [ITP GTT Configuration for ITPC Example, page 133](#)
- [ITP GTT Configuration for ITPD Example, page 135](#)

Figure 17 *ITPs as STPs in an SS7oIP Topology*



This configuration example includes the Global Title Translation (GTT). Four Cisco ITPs are configured. The network configuration is illustrated in [Figure 17](#).

In this example, Intermediate GTT is performed on ITPB. All GTAs matching 339 are sent to the capability point code shared by ITPC and ITPD, where Final GTT is performed.

➔ The arrow symbol indicates the configuration statements most relevant to the GTT configuration on each ITP.

Assumptions:

All routers have redundant ethernet connectivity and therefore all SCTP associations use two IP addresses (multi-homing).

Point codes and IP addresses for ITP routers:

ITPA 5.100.2 172.18.44.242 117.117.117.2

ITPB 5.100.5 172.18.44.243 117.117.117.3

```
ITPC 5.100.4 172.18.45.1 117.117.119.4
ITPD 5.100.3 172.18.46.1 117.117.118.4
```

Point codes for SS7 SSPs:

```
SMSC 5.100.1
VMI4 5.100.6
VT02 5.100.7
VRM2 5.100.8
HLR3 5.100.9
HLR4 5.100.13
```

ITP GTT Configuration for ITPA Example

```
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ITPA
!
enable secret 5 $1$iBmo$AF1H6u2CVGDRM5BMeuGmx/
enable password lab
!
!
no ip cef
no ip finger
no ip domain-lookup
!
cs7 variant itu
cs7 point-code 5.100.2
→ cs7 capability-pc 5.100.12
!
controller E1 1/0/0
channel-group 0 timeslots 1
!
controller E1 1/0/1
channel-group 0 timeslots 1
!
controller E1 2/0/0
channel-group 0 timeslots 1
!
!
interface FastEthernet0/0/0
ip address 172.18.44.242 255.255.255.128
no ip route-cache distributed
no ip route-cache
no ip mroute-cache
!
interface FastEthernet0/0/1
ip address 117.117.117.2 255.255.255.0
no ip route-cache distributed
no ip route-cache
no ip mroute-cache
!
interface Serial1/0/0:0
no ip address
```

```
encapsulation mtp2
no ip route-cache distributed
no ip route-cache
load-interval 30
!
interface Serial11/0/1:0
no ip address
encapsulation mtp2
no ip route-cache distributed
no ip route-cache
load-interval 30
!
interface Serial12/0/0:0
no ip address
encapsulation mtp2
no ip route-cache distributed
no ip route-cache
load-interval 30
!
cs7 local-peer 7000
local-ip 172.18.44.242
local-ip 117.117.117.2
!
!
! Routes using linksets to ITPC and ITPD have a default
! priority of 5. Routes to adjacent node SMS-C and VMI4
! are inserted by the systems with priority 5 and when
! the linkset is configured. They don't have to be defined
! here. Backup-routes to SMS-C and VMI4 are inserted with
! priority 9 using the "C-Link".
!
cs7 route-table system
update route 5.100.7 7.255.7 linkset ITPc
update route 5.100.8 7.255.7 linkset ITPd
update route 5.100.1 7.255.7 linkset ITPb priority 9
update route 5.100.6 7.255.7 linkset ITPb priority 9
!
cs7 linkset ITPc 5.100.4
accounting
link 0 sctp 172.18.45.1 117.117.119.4 7000 7000
route all table system
!
cs7 linkset ITPd 5.100.3
accounting
link 0 sctp 172.18.46.1 117.117.118.4 7000 7000
route all table system
!
cs7 linkset smsc 5.100.1
accounting
link 0 Serial11/0/0:0
link 1 Serial12/0/0:0
route all table system
!
cs7 linkset vmi4 5.100.6
accounting
link 0 Serial11/0/1:0
route all table system
!
cs7 linkset ITPb 5.100.5
accounting
link 0 sctp 172.18.44.243 117.117.117.3 7000 7000
route all table system
!
ip classless
```

```

no ip http server
!
!
!
line con 0
  transport input none
line aux 0
line vty 0 4
  password lab
  login
!
end

```

ITP GTT Configuration for ITPB Example

In the following configuration example, ITPB is configured to perform ITP QoS SCCP packet classification. QoS class 1 is assigned to the GTT selector table named **c7gsp**. QoS class 2 is assigned to GTA 339. According to QoS rules of precedence, if a QoS class is assigned to a selector table and to a GTA within that selector table, the QoS class assigned to the GTA entry has precedence over the QoS class assigned to the selector table.

```

version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ITPB
!
enable secret 5 $1$iBmo$AF1H6u2CVGDRM5BMeuGmx/
enable password lab
!
!
!
!
!
no ip cef
no ip finger
no ip domain-lookup
!
cs7 variant itu
cs7 point-code 5.100.3
→ cs7 capability-pc 5.100.12
!
controller E1 1/0/0
  channel-group 0 timeslots 1
!
controller E1 1/0/1
  channel-group 0 timeslots 1
!
controller E1 2/0/0
  channel-group 0 timeslots 1
!
!
interface FastEthernet0/0/0

```



```

ip address 172.18.44.243 255.255.255.128
no ip route-cache distributed
no ip route-cache
no ip mroute-cache
!
interface FastEthernet0/0/1
ip address 117.117.117.3 255.255.255.0
no ip route-cache distributed
no ip route-cache
no ip mroute-cache
!
interface Serial1/0/0:0
no ip address
encapsulation mtp2
no ip route-cache distributed
no ip route-cache
load-interval 30
!
interface Serial1/0/1:0
no ip address
encapsulation mtp2
no ip route-cache distributed
no ip route-cache
load-interval 30
!
interface Serial2/0/0:0
no ip address
encapsulation mtp2
no ip route-cache distributed
no ip route-cache
load-interval 30
!
cs7 local-peer 7000
local-ip 172.18.44.243
local-ip 117.117.117.3
!
cs7 local-peer 8000
local-ip 172.18.44.243
local-ip 117.117.117.3
!
cs7 local-peer 9000
local-ip 172.18.44.243
local-ip 117.117.117.3
!
cs7 qos class 1
qos-ip-precedence 4
!
cs7 qos class 2
qos-ip-precedence 3

! Routes using linksets to ITPC and ITPD have a default
! priority of 5. Routes to adjacent node SMS-C and VMI4
! are inserted by the systems with priority 5 and when
! the linkset is configured. They don't have to be defined
! here. Backup-routes to SMS-C and VMI4 are inserted with
! priority 9 using the "C-Link".
!
cs7 route-table system
update route 5.100.7 7.255.7 linkset ITPc
update route 5.100.8 7.255.7 linkset ITPd
update route 5.100.1 7.255.7 linkset ITPa priority 9
update route 5.100.6 7.255.7 linkset ITPa priority 9
!
→ cs7 gtt selector c7gsp tt 0 gti 4 np 3 nai 4

```

```

    qos-class 1
→ gta 339 qos-class 2 pcssn 5.100.14 gt

cs7 linkset ITPc 5.100.4
  accounting
  link 0 sctp 172.18.45.1 117.117.119.4 7000 7000
    qos-class 1
  link 1 sctp 172.18.45.1 117.117.119.4 8000 8000
    qos-class 2
  link 2 sctp 172.18.45.1 117.117.119.4 9000 9000
  route all table system
!
cs7 linkset ITPd 5.100.3
  accounting
  link 0 sctp 172.18.46.1 117.117.118.4 7000 7000
  route all table system
!
cs7 linkset smsc 5.100.1
  accounting
  link 0 Serial1/0/0:0
  link 1 Serial2/0/0:0
  route all table system
!
cs7 linkset vmi4 5.100.6
  accounting
  link 0 Serial1/0/1:0
  route all table system
!
cs7 linkset ITPa 5.100.2
  accounting
  link 0 sctp 172.18.44.242 117.117.117.2 7000 7000
  route all table system
!
ip classless
no ip http server
!
!
!
line con 0
  transport input none
line aux 0
line vty 0 4
  password lab
  login
!
end
!
```

ITP GTT Configuration for ITPC Example

```

version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ITPC
!
enable secret 5 $1$iBmo$AF1H6u2CVGDRM5BMeuGmx/
enable password lab
!
!
!
!
no ip cef
no ip finger
no ip domain-lookup
!
cs7 variant itu
cs7 point-code 5.100.4
→ cs7 capability-pc 5.100.14
!
controller E1 1/0/0
channel-group 0 timeslots 1
!
controller E1 2/0/0
channel-group 0 timeslots 1
!
!
interface FastEthernet0/0/0
ip address 172.18.45.1 255.255.255.128
no ip route-cache distributed
no ip route-cache
no ip mroute-cache
!
interface FastEthernet0/0/1
ip address 117.117.119.4 255.255.255.0
no ip route-cache distributed
no ip route-cache
no ip mroute-cache
!
interface Serial1/0/0:0
no ip address
encapsulation mtp2
no ip route-cache distributed
no ip route-cache
load-interval 30
!
interface Serial2/0/0:0
no ip address
encapsulation mtp2
no ip route-cache distributed
no ip route-cache
load-interval 30
!
cs7 local-peer 7000
local-ip 172.18.45.1
local-ip 117.117.119.4
!
!

```

```

! Routes to SMS-C and VMI4 use a combined linkset.
! This is defined by inserting two routes with
! identical priority (5 is default).
!
cs7 route-table system
  update route 5.100.1 7.255.7 linkset ITPa
  update route 5.100.1 7.255.7 linkset ITPb
  update route 5.100.6 7.255.7 linkset ITPa
  update route 5.100.6 7.255.7 linkset ITPb
  update route 5.100.8 7.255.7 linkset ITPd
!
cs7 linkset ITPa 5.100.2
  accounting
  link 0 sctp 172.18.44.242 117.117.117.2 7000 7000
  route all table system
!
cs7 linkset ITPb 5.100.5
  accounting
  link 0 sctp 172.18.44.243 117.117.117.3 7000 7000
  route all table system
!
cs7 linkset ITPd 5.100.3
  accounting
  link 0 sctp 172.18.46.1 117.117.118.4 7000 7000
  route all table system
!
cs7 linkset vt02 5.100.7
  accounting
  link 0 Serial1/0/0:0
  link 1 Serial2/0/0:0
  route all table system
!
ip classless
no ip http server
!
!
!
line con 0
  transport input none
line aux 0
line vty 0 4
  password lab
  login
!
end

```

ITP GTT Configuration for ITPD Example

```

version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ITPD
!
enable secret 5 $1$iBmo$AF1H6u2CVGDRM5BMeuGmx/
enable password lab
!
!
!
!
no ip cef
no ip finger
no ip domain-lookup
!
cs7 variant itu
cs7 point-code 5.100.3
→ cs7 capability-pc 5.100.14
!
controller E1 1/0/0
channel-group 0 timeslots 1
!
controller E1 2/0/0
channel-group 0 timeslots 1
!
!
interface FastEthernet0/0/0
ip address 172.18.46.1 255.255.255.128
no ip route-cache distributed
no ip route-cache
no ip mroute-cache
!
interface FastEthernet0/0/1
ip address 117.117.118.4 255.255.255.0
no ip route-cache distributed
no ip route-cache
no ip mroute-cache
!
interface Serial1/0/0:0
no ip address
encapsulation mtp2
no ip route-cache distributed
no ip route-cache
load-interval 30
!
interface Serial2/0/0:0
no ip address
encapsulation mtp2
no ip route-cache distributed
no ip route-cache
load-interval 30
!
cs7 local-peer 7000
local-ip 172.18.46.1
local-ip 117.117.118.4
!
!

```

```

! Routes to SMS-C and VMI4 use a combined linkset.
! This is defined by inserting two routes with
! identical priority (5 is default).
!
cs7 route-table system
  update route 5.100.1 7.255.7 linkset ITPa
  update route 5.100.1 7.255.7 linkset ITPb
  update route 5.100.6 7.255.7 linkset ITPa
  update route 5.100.6 7.255.7 linkset ITPb
  update route 5.100.7 7.255.7 linkset ITPc
!
cs7 linkset ITPa 5.100.2
  accounting
  link 0 sctp 172.18.44.242 117.117.117.2 7000 7000
  route all table system
!
cs7 linkset ITPb 5.100.5
  accounting
  link 0 sctp 172.18.44.243 117.117.117.3 7000 7000
  route all table system
!
→ cs7 gtt map 5.100.9 100 share 5.100.13 100
→ cs7 gtt selector cnam tt 0 gti 4 np 3 nai 4
→ gta 339 pcssn 5.100.9 pcssn ssn 100
!
cs7 linkset ITPd 5.100.4
  accounting
  link 0 sctp 172.18.45.1 117.117.119.4 7000 7000
  route all table system
!
cs7 linkset vrm2 5.100.8
  accounting
  link 0 Serial1/0/0:0
  link 1 Serial2/0/0:0
  route all table system
!
ip classless
no ip http server
!
!
!
line con 0
  transport input none
line aux 0
line vty 0 4
  password lab
  login
!
end

```



M3UA and SUA SS7 Over IP Signaling Gateways

The Cisco ITP Signaling Gateway (ITP SG) feature provides open-standards-based SS7 over IP solutions through the implementation of SIGTRAN MTP3-User Adaptation (M3UA) and SCCP User Adaptation (SUA) protocols.

Feature History for M3UA and SUA SS7 over IP Signaling Gateways

Release	Modification
12.2(33)IRA	Added support for this feature.
12.2(33)IRD	Added offload support for SGMP.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



Note

Configuration Mode Restrictions: Simultaneous changes to the configuration from multiple CLI sessions are not supported. Only one configuration session is allowed to enter in configuration mode at a time; other sessions should not enter in configuration mode. The **show line** or **show users EXEC** command may be used to determine the active user sessions on an ITP, and the **clear line EXEC** command may be used to ensure that only a single active session exists.

Contents

- [Information About M3UA and SUA ITP Signaling Gateways, page 138](#)
- [How to Configure Signaling Gateways, page 145](#)
- [ITP Signaling Gateway Configuration Examples, page 153](#)



Note

Most of the commands that are shown in the configuration task sections of this chapter are described in detail in the “[ITP Command Set](#)” chapter. Some general IOS configuration commands are not included in the ITP Command Set chapter. For those commands, a footnote indicates the IOS document where more information can be found.

Information About M3UA and SUA ITP Signaling Gateways

The Cisco ITP SG feature enables you to develop or deploy IP-based application servers without having to develop MTP layers and SCCP on the application server platform. The application server platform needs only to implement the MTP3 User Part or SCCP User Part appropriate for the application. The MTP layers and SCCP layer reside on the ITP SG.

The ITP SG is responsible for terminating and/or translating MTP/SCCP events on the SG. The translated event or the user part protocol data is sent to the application over the IP network.

SS7 network management messages are translated to M3UA, or SUA messages before being transferred to the application server. User part messages are encapsulated and transferred transparently to the application server.

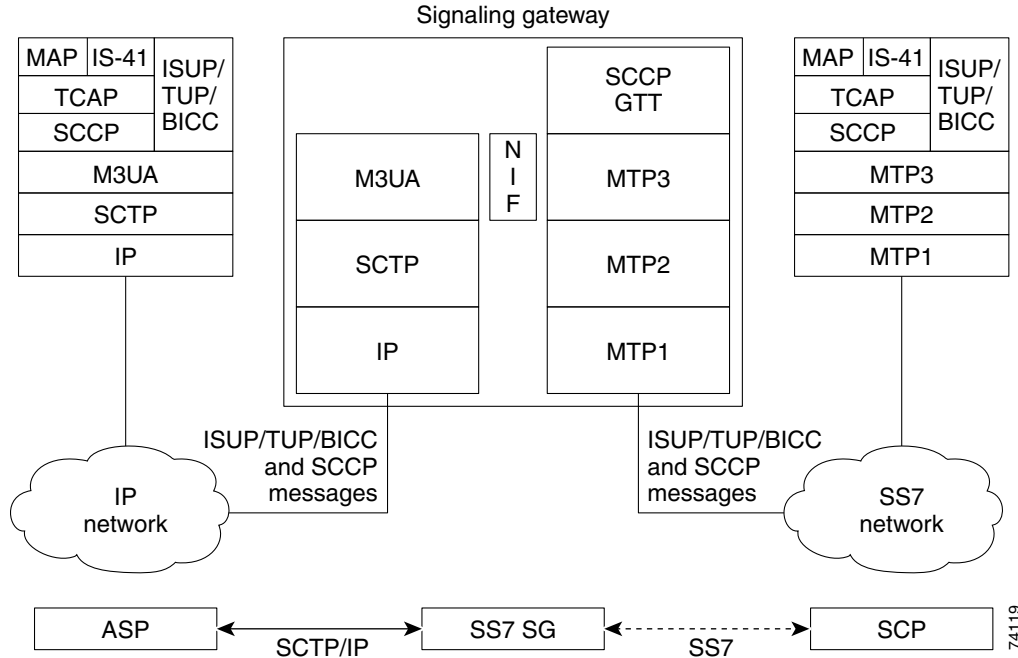
The following sections provide an overview of the main components and features of the Cisco ITP SG:

M3UA

M3UA is a client/server protocol that provides a gateway to the legacy SS7 network for IP-based applications that interface at the MTP3 layer, such as ISDN User Part (ISUP) and Signaling Connection Control Part (SCCP). For M3UA, the user part can be ISUP for call setup applications or SCCP for TCAP/MAP and RANAP applications.

M3UA describes a transport mechanism for delivering SS7 MTP3-User Part messages as well as certain MTP network management events over SCTP transport to IP-based application processors or databases. The M3UA SG terminates the SS7 MTP2 and MTP3 protocol layers and delivers ISUP, SCCP and/or any other MTP3-User protocol messages. Protocol termination and translation and user part protocol encapsulations are done by the M3UA nodal inter-working function (NIF) on the SG. The NIF is the interface between MTP3 and M3UA.

[Figure 18](#) depicts the relationship between the legacy SS7 Service Control Point (SCP), the M3UA SG, the IP-based Application Server Process (ASP), and the protocol stacks.

Figure 18 M3UA Signaling Gateway Protocol Stacks

In [Figure 18](#) the legacy SS7 SCP on the far right uses MTP1, MTP2, and MTP3 for transporting SCCP and ISUP messages into the network. The SG terminates the SS7 links, translates the MTP3 messages into M3UA messages, and transports them to the ASP over SCTP/IP. M3UA at the ASP delivers SCCP and ISUP messages.

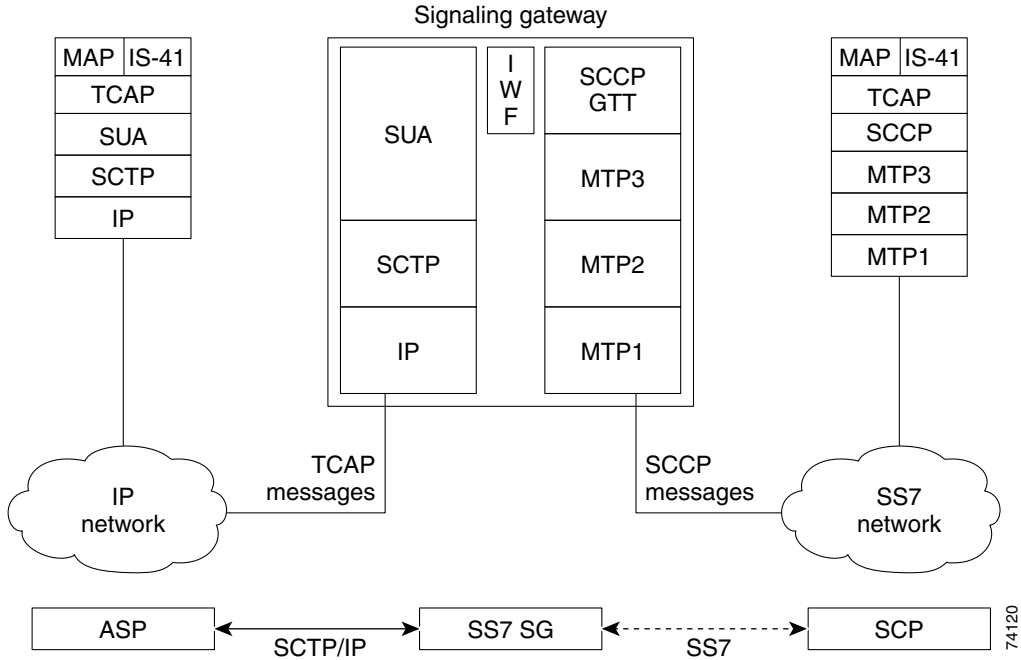
SUA

SUA is a client/server protocol that provides a gateway to the legacy SS7 network for IP-based applications that interface at the SCCP layer, such as TCAP, RANAP, etc. For SUA, the SCCP user part can be TCAP/MAP, RANAP, etc. The MTP layers and the SCCP layer reside on the SG.

SUA describes a transport mechanism for delivering SS7 SCCP-User Part messages as well as certain SCCP network management events over SCTP transport to IP-based application processors or databases. The SUA SG terminates the SS7 MTP2, MTP3, and SCCP protocol layers and delivers TCAP, RANAP and/or any other SCCP-User protocol messages. For SUA, the protocol termination and translation and user part protocol encapsulations are done by the SUA inter-working function (IWF) on the SG. The IWF is the interface between SCCP and SUA.

[Figure 19](#) depicts the relationship between the legacy SS7 SCP, the SUA SG, the IP-based ASP, and the protocol stacks.

Figure 19 *SUA Signaling Gateway Protocol Stacks*



In Figure 19 the legacy SS7 SCP on the far right uses MTP1, MTP2, and MTP3 for transporting SCCP messages into the network. The SG terminates the SS7 links, translates the SCCP messages into SUA messages, and transports them to the ASP over SCTP/IP. SUA at the ASP delivers TCAP messages.

SGMP

Two signaling gateways can function as a mated pair and exchange necessary state information using the Signaling Gateway Mate Protocol (SGMP). SGMP is used to establish an association to the mated signaling gateway with an equivalent SG configuration.

The mated-pair SGs are used to loadshare and/or back up each other in failover scenarios. The mated SG can be used as a backup point code for cases when there is a failure of an association between this SG and the ASP.

When the SG mate association is active, the SG is informed of AS state changes on the mate in real time. When an AS becomes inactive, subsequent messages are rerouted to the mate if the corresponding AS on the mate is active.

When the AS on the original SG returns to active state, new messages are temporarily queued to allow in-transit messages from the mated SG to arrive at the ASP. Queued messages are released to the ASP upon expiration of an AS recovery timer.

The mated-pair SGs also exchange ASP binding information. This allows rerouted traffic that is bound to a specific ASP to continue uninterrupted even when the AS on the original SG returns to active state. The bound traffic continues to be rerouted through the SG mate to the bound ASP. The only exception is when the bound ASP becomes active on the original SG. In this case, the bound traffic begins flowing through the original SG to the same ASP, following a queueing period to allow in-transit messages to arrive at the ASP.

Mated-pair SGs must have equivalent SG configuration, including the same AS definitions. However, the local point code of each SG must be unique and must not match the local point code, the capability point code, the secondary point code, or any AS point code (DPC).

**Note**

C-Link routing takes priority over routing.

**Note**

We recommend you manage the traffic rate in order to avoid congestion and packet drop in case of ASP association failure when the AS is in the Active state.

C-Link Backup Routing of M3UA/SUA Traffic

The C-link backup routing provides backup routing to M3UA and SUA ASs using an MTP3/M2PA linkset to a remote SG serving the same ASs over SCTP/IP. The routing is available to any ITP running a sigtran protocol (M3UA and/or SUA) and offloaded MTP3. The remote SG that is reachable through the C-link may be another ITP, or any SG serving the same ASs.

Traffic destined for an unavailable M3UA/SUA AS on the ITP is routed to the remote SG through the C-link (with some restrictions described below), provided a route to the M3UA/SUA point code was configured using the C-link. If is configured on the ITP, C-link routing takes priority.

We recommend that the M3UA/SUA AS configuration on C-link connected SGs is identical, so that traffic received through the C-link is routed to the correct ASPs.

The C-link is configured on the ITP as an MTP3/M2PA linkset and the routes to AS point codes are configured as standard mtp3 routes (with no SLS rotation). ITP configuration currently disallows configuring a route to an AS point code, or configuring an AS point code to which an MTP3 route already exists. This release supports MTP3 routes to AS point codes, with the following limitations:

- A route to an AS point code matching a local, capability, or secondary ITP point code is not allowed.
- A route to an AS point code shared by multiple AS's is not allowed.

This release also supports AS routing keys with a point code to which an MTP3 route already exists, with the following limitation:

- A routing key containing a point code to which an MTP3 route already exists is not allowed if the point code is already configured in another AS routing key.
- A routing key containing a point code already configured as a linkset adjacent point code is not allowed.

Restrictions

The following list identifies restrictions to the basic functionality of the C-link Backup Routing feature:

- Any AS serving an ITP local, capability, or secondary point code is not supported by the C-link.
- Any AS sharing a point code with another AS is similarly unsupported. In such a configuration, a message received through the C-link may not match an active routing key even though the AS point code is available.
- ITP configurations that map GTT directly to an AS name are not supported by the C-link because the AS has no point code.
- C-link routing using cluster or summary routes is not supported.

C-link Route Availability

Per standard MTP3 practice, route availability to the remote AS point code is controlled by TFA/TFP/TFR messages received over the C-link. In the absence of any such messages, the route is assumed to be available. The configured route using the C-link must be fully qualified.

AS Point Code Availability

Similar to , when an AS goes locally inactive and a route to the AS point code is available, the ITP broadcasts TFR if supported by the variant, and TFA otherwise.

ASP Bindings

No proprietary messages are exchanged through the C-link. This means that, without enabled, the ITP is unaware of ASP bindings on the remote SG and always routes messages to a locally active AS, even if a locally inactive ASP has a binding active on the remote SG.

Application Server (AS)

An Application Server (AS) is a logical entity serving a specific Routing Key. An example of an Application Server is a virtual switch element handling all call processing for a unique range of PSTN trunks, identified by an SS7 DPC/OPC/CIC_range. Another example is a virtual database element, handling all HLR transactions for a particular SS7 DPC/OPC/SCCP_SSN combination. The AS implements a set of one or more unique Application Server Processes, of which one or more is normally actively processing traffic.

Application Server Process (ASP)

An Application Server Process (ASP) is an IP-based instance of an application server, such as Call Agents, HLRs, SMSCs, etc.

An ASP may implement more than one AS.

Point Code Assignment and Management

Special care must be taken when planning the assignment of point codes to ASes. The ITP SG feature allows point code assignment to ASes and ASPs as follows:

- An AS may be assigned the primary local point code or the secondary local point code owned by the ITP SG. The AS is sharing the point code with the ITP SG.
- An AS may be assigned a capability code or alias point code of the ITP SG. The AS is sharing the point code with the ITP SG's mated-pair.
- An AS may be assigned a unique point code not previously assigned to any of the SGs in the mated-pair.
- An ASP can be assigned a unique point code by being the only ASP in an AS that has been assigned a unique point code.

- All ASes or groups of ASes serviced by the ITP SG may share a given point code. Any group of ASes that shares the same point code is referred to as a Signaling Point Management Cluster (SPMC). Note that a M3UA AS and a SUA AS may share only one of the router's point codes (primary local, secondary local, or capability).

Assigning more than one AS the same point code can have significant affect on the ability of the ITP SG to report ASP, AS, user part, or subsystem outages or unavailability to the SS7 network.

AS Load-sharing Support

The ITP M3UA and SUA SG features support the load-share redundancy model.

By default, the traffic-mode of the AS will be set to load-share if the first valid ASP Active message received from an ASP in the AS has the traffic mode type set to load-share. Any subsequent ASP Active message received from an ASP in the AS that does not have the traffic mode type set to load-share will be rejected.

The desire to enforce AS load-sharing is indicated by setting the traffic-mode type parameter under the AS configuration to load-share round-robin or load-share bindings. If the traffic mode type has been configured as load-share, then any ASP Active message received for an ASP in that AS containing a traffic mode parameter with the traffic mode type not set to load-share will be rejected.

The SG will perform either basic round-robin load sharing among the active ASPs in the AS or round-robin load sharing based on a load-share seed.

When basic round-robin load sharing is done, the first received MSU will be processed by the first active ASP in the list, the next MSU by the next active ASP in the list, and so on. When each ASP in the list has been sent an MSU, the distribution of subsequent MSUs will begin again with the first active ASP in the list.

A load-share seed is a parameter or a group of parameters in an MSU and is traffic-type dependent. For example, the seed could be the DPC/OPC/CIC combination, the SLS, etc. When load-sharing is based on a load-share seed all MSUs for an AS with the same seed value must be processed by the same ASP until that ASP becomes inactive. The association of a load-share seed with a specific ASP is referred to as a binding or having traffic bound to an ASP.

Binding is necessary to maintain the proper sequencing of MSUs or to ensure that all MSUs that are a part of the same transaction, procedure, or connection are processed by the same ASP. When an MSU is received the SG will first check to see if the load-share seed of the MSU has been bound to a specific ASP. If it has been bound to an ASP, the MSU will be directed to that ASP. If no binding was found, the SG will select and bind the load-share seed to an ASP from the list of active ASPs for the AS.

Default bindings are assigned sequentially to the ASP list in the AS, up to a maximum value equal to the sum of the ASP weights in the AS. The number of default bindings owned by a single ASP is equal to its weight. ASPs of weight 0 get no default bindings. When a message is received with an unbound load-share seed, it is assigned to the ASP that owns the default binding equal to $(received\_load\_share\_seed) \bmod (total\_asp\_weight)$. This loadshares all bound traffic according to the relative ASP weights within the AS. If the assigned ASP is inactive or congested, the binding is round-robin loadshared to another active ASP. If the owning ASP subsequently becomes active, the binding is reassigned to it, with an 800 msec queueing period to allow in-transit messages to arrive at the old ASP. If the new ASP becomes inactive during the queueing period, queued messages are processed as new bindings. When an ASP becomes inactive all bindings for that ASP are cleared.

Load sharing per traffic type is performed as follows:

- ISUP traffic: round-robin load sharing will be done with the DPC/OPC/CIC of the MSU as the load-share seed.
- SCCP class 0 traffic: basic round-robin load sharing will be done without regard to any parameters in the MSU.
- SCCP class 1 traffic: round-robin load sharing will be done with the SLS of the MSU as the load-share seed.

When an AS requires traffic to be bound to a specific ASP, ASPs in the AS may need to exchange state information to avoid transaction, procedure, or connection disruption in the event of ASP failure and subsequent traffic redistribution.

AS Fail-over support

The ITP M3UA and SUA SG features support the over-ride or primary/back up redundancy model. By default, the traffic-mode type of an AS is specified dynamically as follows. If the traffic mode parameter under the AS was not configured, the traffic mode of the AS will be set to over-ride if the first valid ASP Active message received for an ASP in the AS indicates a traffic mode type of over-ride. Any subsequent ASP Active message received from an ASP in the AS that does not have the traffic mode type set to over-ride will be rejected.

The desire to enforce the operation of an AS in over-ride mode is indicated by configuring the traffic-mode type parameter under the AS to over-ride. If the traffic mode type has been configured as over-ride, any ASP Active received for an ASP in that AS that contains a traffic mode parameter with traffic mode type not set to over-ride will be rejected.

In the over-ride mode AS model, traffic for the AS is not load-shared. AS traffic is only sent to the active ASP in the AS. Only one ASP is active at a time. If ASP1 and ASP2 are in the same AS, and ASP1 is active when an ASP Active(over-ride) from ASP2 is received, ASP1 will be sent a NOTIFY(alternate-asp-active) message and be placed in the inactive state. ASP2 will be placed in active state and AS traffic will now be redirected to ASP2.

SCCP Traffic Processing for M3UA

SCCP traffic to an M3UA AS PC can be sent to only one AS. If SCCP traffic must be split (for example, by SSN), then use SUA for the affected PC.

A Signaling Connection Control Part (SCCP) Management (SCMG) message for an M3UA AS PC will be routed according to normal routing key search and AS traffic mode rules. For a broadcast traffic mode AS, the SCMG message will be sent to all active ASPs in the AS. For an override traffic mode AS, the SCMG message will be sent to the active ASP. For a loadshare AS, the SCMG message will be sent to only one of the active ASPs in the AS. Broadcast or override mode is recommended if the ASPs in a loadshare AS do not share management information.

When an SCMG message is sent to one of the router's point codes (primary local, secondary local, or capability point code), the SCMG message is distributed to a M3UA AS if the AS PC is in the router's concerned point code list. In addition, the SCMG message is sent to M3UA ASes that share a point code with the router and all M3UA ASes with GTT routing keys.

ITP SG Quality Of Service (QoS)



Note

ITP Quality of Service (QoS) is described fully in the “[ITP QoS](#)” chapter. If you are unfamiliar with QoS, you are advised to refer to that chapter for more detail.

How to Configure Signaling Gateways



Note

IP routing is enabled on the ITP by default, and must not be disabled. Disabling IP routing can result in connection errors.

This section describes the following ITP SG configuration tasks:

- [Performing Basic ITP Configuration, page 145](#)
- [Enabling and Disabling M3UA and SUA, page 146](#)
- [Enabling SGMP, page 147](#)
- [Enabling SGMP Offloading, page 149](#)
- [Defining an Application Server Process \(ASP\), page 150](#)
- [Defining Application Servers \(AS\) and Routing Keys, page 152](#)
- [Enabling M3UA Extended User Part Unavailable \(UPU\) Operation, page 153](#)



Note

ITP is designed to send error messages on a per second basis. If multiple error messages are received simultaneously for which ITP has to send error messages back, ITP sends the error message for only the first packet. The rest of the messages are throttled back.

Performing Basic ITP Configuration



Note

Basic ITP configuration is described fully in the “[Configuring ITP Basic Functionality](#)” chapter. If you are unfamiliar with ITP basic configuration, you are advised to refer to that chapter for more details.

This section summarizes the basic ITP configuration tasks. To accomplish the basic ITP configuration, use the following commands in global configuration mode:

	Command	Purpose
Step 1	Router(config)# cs7 variant {ansi itu china}	Specifies which SS7 variant the router is running.
Step 2	Router(config)# cs7 national-options {TFR multiple-congestion}	Specifies ITU national options.
Step 3	Router(config)# cs7 network-indicator {international national reserved spare}	Specifies this network indicator.
Step 4	Router(config)# cs7 point-code format 1-24 [1-23 [1-22]] description string	Specifies the point code representation.

	Command	Purpose
Step 5	Router(config)# cs7 point-code delimiter [default dash]	Specifies the delimiter between bits as either dots or dashes.
Step 6	Router(config)# cs7 capability-pc point-code	Specifies the capability point code for the ITP.

Enabling and Disabling M3UA and SUA

Configuring M3UA or SUA on the ITP SG provides the definitions necessary for the ITP SG to accept connections from an ASP.

You may configure either M3UA, SUA, or both, as needed.

Enabling M3UA

To use M3UA as a connectivity solution, you must configure the M3UA subsystem on the ITP SG.

First you must configure an M3UA local SCTP port on the ITP for inbound connections to use as their destination port. You may configure a local port number in the range 1024 to 65535. This port may not currently be configured for M2PA, SUA, or SGMP. (2905 is the well-known port for M3UA.)

After you configure an M3UA local port, you must configure at least one local IP address known to the ITP for use by M3UA.

To configure an M3UA local port number and configure a local IP address for use by M3UA, use the following commands, beginning in global configuration mode:

Command	Purpose
Router(config)# cs7 m3ua local-port-number [offload linecard-slot-number bay-number]	Specifies a local port for inbound connections and enters CS7 M3UA submode.
Router(config-cs7-m3ua)# local-ip ip-address	Configures a local IP address for use by M3UA. The local-ip ip-address must be an IP address that was already configured on the linecard to which you are offloading this M3UA instance.

Disabling M3UA

To disable the local M3UA port, use the following command in CS7 M3UA submode:

Command	Purpose
Router(config-cs7-m3ua)# shutdown	Disables this local port on the ITP SG and kills all associations with this port.

There are several SCTP parameters that you can modify under the M3UA local instance. The tasks and commands to tune timers and SCTP parameters are described in the [“Tuning ITP” section on page 394](#) of the “Verifying, Monitor, and Tuning ITP” chapter.

Enabling SUA

To use SUA as a connectivity solution, you must configure the SUA subsystem on the ITP SG.

First you must configure an SUA local SCTP port on the ITP for inbound connections to use as their destination port. You may configure a local port number in the range 1024 to 65535. This port may not currently be configured for M2PA, M3UA, or SGMP. (14001 is the well-known port for SUA.)

After you configure an SUA local SCTP port, you must configure at least one local IP address known to the ITP for use by SUA via the SCTP communications protocol.

To configure an SUA local port number and configure a local IP address for use by SUA, use the following commands, beginning in global configuration mode:

Command	Purpose
<code>Router(config)# cs7 sua local-port-number [offload linecard-slot-number bay-number]</code>	Specifies a local port for inbound connections and enters CS7 SUA submode.
<code>Router(config-cs7-sua)# local-ip ip-address</code>	Configures a local IP address for use by SUA. local-ip ip-address must be an IP address that was already configured on the linecard to which you are offloading this SUA instance.

Disabling SUA

To disable the local SUA port, use the following command in CS7 SUA submode:

Command	Purpose
<code>Router(config-cs7-sua)# shutdown</code>	Disables this local port on the ITP SG and kills all associations with this port.

There are several SCTP parameters that you can modify under the SUA local instance. The tasks and commands to tune timers and SCTP parameters are described in the [“Tuning ITP” section on page 394](#) of the “Verifying, Monitor, and Tuning ITP” chapter.

Enabling SGMP

Two SGs can function as a mated pair and exchange necessary state information using the Signaling Gateway Mate Protocol. SGMP is used to establish an association to the mated signaling gateway with an equivalent SG configuration.

The mated-pair SGs are used to loadshare and/or back up each other in failover scenarios. The mated SG can be used as a backup point code for cases when there is a failure of an association between this SG and the ASP.

When the SG mate association is active, the SG is informed of AS state changes on the mate in real time. When an AS becomes inactive, subsequent messages are rerouted to the mate if the corresponding AS on the mate is active.

When the AS on the original SG returns to active state, new messages are temporarily queued to allow in-transit messages from the mated SG to arrive at the ASP. Queued messages are released to the ASP upon expiration of an AS recovery timer.

Mated-pair SGs must have equivalent SG configuration. However, the local point code of each SG must be unique and must not match the local point code, the capability point code, the secondary point code, or any AS point code (dpc) configured on its mate.

Configuring a QoS classification for the SG mated pair is optional.

To enable and define the link to the SG mate, use the following commands, beginning in global configuration mode:

Command	Purpose
Router(config)# cs7 sgmp <i>local-port</i>	Enables SGMP and specifies the SGMP local port.
Router(config-cs7-sgmp)# local-ip <i>ip-address</i>	Configures a local IP address for use by SGMP.
Router(config-cs7-sgmp)# exit	Return to global configuration mode.
Router(config)# cs7 mated-sg <i>mate-name remote-port</i>	Define the mated SG name and remote port number and enable CS7 mated-sg submode.
Router(config-cs7-mated-sg) remote-ip <i>remote-ip</i>	Specify the remote IP address of the mated SG.
Router(config-cs7-mated-sg) qos-class <i>class</i>	(Optional) Defines the QoS class for the SG mated pair.



Note

If you deploy ITPs in a mated-pair redundant configuration, you may optionally define a special IP-based cross link between the two ITPs. Although significant mated pair redundancy is achieved without a cross-link definition (node failures and single IP path failures do not require this definition), such a cross link increases overall availability by offering a routing path around the specific case where all IP connectivity between an ITP and ASP fails, but the mated-pair ITP has an available IP path to the ASP.

Enabling SGMP Offloading

Cisco 7600 platforms with Cisco Service and Application Modules for IP (SAMIs) installed can offload SGMP onto any number of linecards by supporting multiple SGMP associations. Data messages are rerouted via SGMP from the ingress linecard to an egress linecard hosting an SGMP association. Even with offloading configured, SGMP control messages are still generated by the supervisor module and are sent to the supervisor module when received on an offloaded SGMP association.

SGMP offload improves reliability by removing the linecard to supervisor module path for rerouted data packets and replacing it with the same card-to-card path used for other ITP payload traffic on the Cisco 7600 platform with SAMIs installed.



Caution

You cannot configure SGMP offload when non-offloaded SGMP is configured. If non-offload SGMP is configured, you must delete it before configuring the SGMP offload.

To enable and define the link to the SG mate and enable linecard offloading, use the following commands, beginning in global configuration mode:

	Command or Action	Purpose
Step 1	enable Example: ITP> enable	Enables privileged EXEC mode.
Step 2	configure terminal Example: ITP# configure terminal	Enters global configuration mode.
Step 3	ITP(config)# cs7 sgmp [<i>local-port</i>] offload [<i>slot</i>] [<i>bay</i>] Example: ITP(config)# cs7 sgmp 9999 offload 2 1	Enables SGMP, specifies the local port number for SGMP, enables SGMP offloading, and enters cs7 sgmp configuration submenu.
Step 4	ITP(config-cs7-sgmp)# local-ip <i>ip-address</i> Example: ITP(config-cs7-sgmp)# local-ip 172.18.48.79	Configures a local IP address for use by the first of the two mated SGs.
Step 5	ITP(config-cs7-sgmp)# exit Example: ITP(config-cs7-sgmp)# exit	Returns to global configuration.
Step 6	ITP(config)# cs7 mated-sg <i>name</i> <i>remote-port</i> [<i>local-port</i>] [passive] Example: ITP(config)# cs7 mated-sg mated1 8888 9999	Defines the connection to the second of the two mated SGs.

	Command or Action	Purpose
Step 7	<pre>ITP(config-cs7-mated-sg) remote-ip remote-ip</pre> Example: <pre>Router(config-cs7-mated-sg) remote-ip 172.18.48.80</pre>	Specifies the remote IP address of the second of the two mated SGs.
Step 8	<pre>ITP(config-cs7-sgmp) # exit</pre> Example: <pre>ITP(config-cs7-sgmp) # exit</pre>	Returns to global configuration.
Step 9	<pre>ITP(config) # cs7 as as-name sgmp</pre> Example: <pre>ITP(config) # cs7 as sgmp_as sgmp</pre>	Defines an AS and enters cs7 AS submode.
Step 10	<pre>ITP(config-cs7-as) # mated-sg name remote-port [local-port] [passive]</pre> Example: <pre>ITP(config-cs7-as) # cs7 mated-sg mated1 8888 9999</pre>	Defines the connection from the AS to the mated SG.
Step 11	<pre>ITP(config-cs7-as) # routing-key rcontext</pre> Example: <pre>ITP(config-cs7-as) # routing key 200</pre>	Configures the routing key for the AS.

Examples

The following example shows an SGMP configured for offloading:

```
cs7 sgmp 9999 offload 2 1
  local-ip 172.18.48.79
cs7 mated-sg mated1 8888 9999
  remote-ip 172.18.48.80
cs7 as sgmp_as sgmp
  mated-sg mated1
  routing-key 200
```

Defining an Application Server Process (ASP)

Each ASP connecting to the ITP SG must be represented by an ASP definition. The ASP definition allows the ITP SG to validate the ASP IP address list and port number upon establishment of the SCTP association.

The ASP definition requires an ASP name that is used for configuration and monitoring only. The ASP name may be up to 12 characters long. The first character must be alphabetic. The name must not match any reserved keyword (such as m3ua, sua, all, operational, active, statistics, bindings, or detail).

The ASP definition also requires at least one of the remote IP addresses of the ASP, the remote SCTP port number, and the local port number that indicates the M3UA or SUA subsystem.

The combination of the remote port, remote IP, and local port must be unique for each configured ASP. If a remote port of 0 is configured, the ASP will match on any remote port (provided the remote IP and local port match).

Configuring a QoS classification is optional, as is specification of SCTP association parameter values. When a QoS classification is configured for an ASP or an AS, it takes effect only on the subsequent ASP connection. The QoS can only be changed when ASP is NOT active. Use the **shutdown** and **no shutdown** commands in CS7 ASP configuration mode to shut down and then activate the ASP with the QoS change.

To define an ASP, use the following commands, beginning in global configuration mode:

Command	Purpose
Router(config)# cs7 asp <i>asp-name remote-port local-port</i> [m3ua sua]	Configures a CS7 ASP definition and enters CS7 ASP submode.
Router(config-cs7-asp) # remote-ip <i>remote-ip</i>	Specifies the remote IP address of the ASP.
Router(config-cs7-asp) # qos-class <i>class</i>	Defines the QoS class for the ASP
Router(config-cs7-asp) # match any qos-class <i>class</i>	Sets the match criteria.
Router(config-cs7-asp) # match si si qos-class <i>class</i>	Sets the serviced indicator match criteria.

To block or to terminate the SCTP association with the ASP, use one of the following commands in CS7 ASP submode:

Command	Purpose
Router(config-cs7-asp) # block	Allows a new SCTP association with this ASP, but doesn't let it become active. In other words, always rejects ASP-ACTIVE messages from the ASP. If block is set while the ASP is active, it is forced inactive (but the association remains up).
Router(config-cs7-asp) # shutdown	Terminates the SCTP association with this ASP. New SCTP associations will be rejected if the ASP is in shutdown mode.

You can optionally allow the SUA ASP additional control in determining whether an SCCP UDT or XUDT message will be generated upon receiving a CLDT message. To enable the SUA to request that the SCCP layer generate an XUDT message if the ASP has provided either the IMPORTANCE or HOP_COUNTER parameters within the CLDT message, use the following command in global configuration mode:

Command	Purpose
Router(config)# cs7 [instance <i>instance-number</i>] sua-allow-xudt-request	Enables the SUA to request that the SCCP layer generate an XUDT message if the ASP has provided either the IMPORTANCE or HOP_COUNTER parameters within the CLDT message.

There are several SCTP parameters that you can modify under the ASP definition. The tasks and commands to tune timers and SCTP parameters are described in the of the “Verifying, Monitor, and Tuning ITP” chapter.

Defining Application Servers (AS) and Routing Keys

Each ASP connecting to an ITP SG must be represented in an AS definition. The AS definition is used to properly route messages to the appropriate set of ASPs handling a particular routing key.

The AS definition requires a unique AS name that will identify the AS for configuration or monitoring. The AS name may be up to 12 characters long. The first character must be alphabetic. The AS name may not match a reserved keyword (such as m3ua, sua, all, operational, active, statistics, bindings, or detail).

The AS definition must indicate whether the AS is M3UA or SUA.

The number of ASPs associated with an AS should not exceed 16.

Configuring a QoS classification for the AS is optional.

To configure an AS definition, use the following command in global configuration mode:

Command	Purpose
Router(config)# cs7 as <i>as-name</i> [m3ua sua]	Configures a CS7 AS definition and enters CS7 AS submode.

Each ASP connecting to an ITP must have a routing key configured for each AS definition. The routing key defines the routing parameters used to send traffic to the ASP. Within the routing key, a routing context must be defined to identify traffic sent to and from a particular ASP. The routing context must be unique for each AS defined, but there is no other significance of the value chosen when pertaining to an ASP configuration. In the routing key, the DPC should be a valid point code.

To configure the AS routing key, use the following command in CS7 AS submode:

Command	Purpose
Router(config-cs7-as)# routing-key <i>rcontext</i> { gtt <i>dpc</i> [opc <i>pc</i> <i>pc-mask</i>] [si { aal2 bicc b-isup h248 isup sat-isup sccp tup }] [cic <i>cic-min</i> [<i>cic-max</i>] [ssn <i>ssn</i>]}}	Defines the AS routing key.

To associate the ITP AS and ASP definitions and, optionally specify weighted round-robin ASP distribution within an AS, use the following command in CS7 AS submode:

Command	Purpose
Router(config-cs7-as)# asp <i>asp-name</i> [weight <i>weight</i>]	Specifies the ASPs contained in the AS.

You can optionally specify the traffic mode, QoS class, recovery timeout interval and burst recovery timeout interval. To configure these options, use the following commands, in CS7 AS submode:

Command	Purpose
Router(config-cs7-as)# traffic-mode {broadcast loadshare [bindings [sls [opc-sls [opc-shift {opc-shift-number}]] cgpa-sls][redistribute-active]] cic [redistribute-active] [opc-sls [opc-shift {opc-shift-number}]] cgpa-sls][redistribute-active]] roundrobin] override}	Specifies the traffic mode of operation of the ASP within this AS. The default is loadshare bindings.
Router(config-cs7-as)# recovery-timeout msec	Specifies the recovery timeout value, in milliseconds. The valid range is 1 to 2000 msec. The default is 2000 msec.
Router(config-cs7-as)# burst-recovery-timeout msec	Specifies the amount of time allowed for an association to recover from a burst of traffic caused by failover.
Router(config-cs7-as)# qos-class class	Defines the QoS class for the ASP.

Enabling M3UA Extended User Part Unavailable (UPU) Operation

By default, the ITP sends a response-mode UPU when a received message has a DPC equal to an active AS point code and meets either of the following conditions:

- The SI value in the message is not ISUP, TUP, or SCCP
- The SI defined in the active AS routing key does not match the SI value in the message.

ITP extended UPU operation allows the ITP to send UPU in the following additional cases:

- Routing key parameters defined in the active AS don't match the message.
- An AS with OPC configured and SI configured for ISUP or TUP becomes inactive.

To enable M3UA extended UPU operation for these cases, use the following command in global configuration mode:

Command	Purpose
ITP(config)# cs7 m3ua extended-upu	Extends M3UA UPU Operation. In all cases, UPU is rate-limited to no more than 1 per second per SI value.

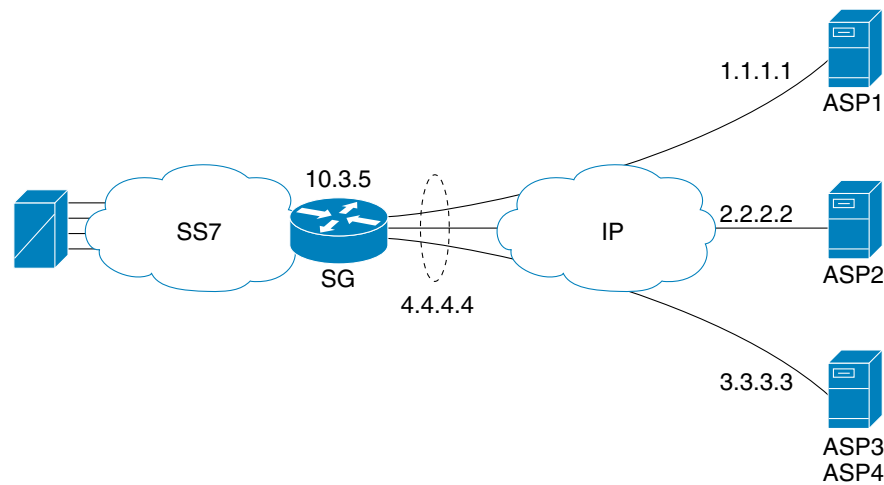
ITP Signaling Gateway Configuration Examples

This section includes examples for the following aspects of ITP SG configuration:

- [M3UA Configuration Example, page 154](#)
- [SUA Configuration Example, page 155](#)
- [ITP Signaling Gateway: ASPs with Unique Point Codes Configuration Example, page 155](#)
- [ITP SG Mated-SG Configuration Example, page 156](#)
- [ITP SG GTT Configuration Example, page 158](#)
- [ITP SG QoS Configuration Examples, page 159](#)

Figure 20 illustrates the M3UA and SUA configuration examples that follow.

Figure 20 ITP Signaling Gateway



74459

M3UA Configuration Example

This configuration is illustrated in Figure 20.

```

cs7 variant ansi
cs7 point-code 10.3.5

interface ethernet 0/0
 ip address 4.4.4.4 255.255.255.128

cs7 m3ua 2905
 local-IP 4.4.4.4

cs7 asp ASP1 2905 2905 m3ua
 remote-ip 1.1.1.1
cs7 asp ASP2 2905 2905 m3ua
 remote-ip 2.2.2.2
cs7 asp ASP3 10001 2905 m3ua
 remote-ip 3.3.3.3
cs7 asp ASP4 10002 2905 m3ua
 remote-ip 3.3.3.3

cs7 as BLUE m3ua
 routing-key 100 10.3.8
 asp ASP1
 asp ASP2
 traffic-mode loadshare

cs7 as GREEN m3ua
 routing-key 200 10.3.7
 asp ASP2
 asp ASP3
 asp ASP4
 traffic-mode loadshare

```


SUA Configuration Example

This example is illustrated in [Figure 20](#).

```

cs7 variant ansi
cs7 point-code 10.3.5

interface ethernet 0/0
 ip address 4.4.4.4 255.255.255.128

cs7 sua 15000
 local-ip 4.4.4.4

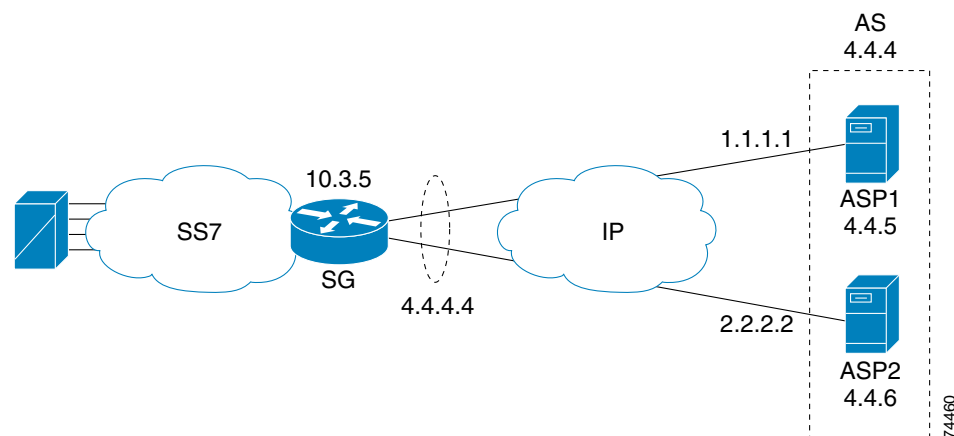
cs7 asp ASP1 14001 15000 sua
 remote-ip 1.1.1.1
cs7 asp ASP2 14001 15000 sua
 remote-ip 2.2.2.2
cs7 asp ASP3 10001 15000 sua
 remote-ip 3.3.3.3
cs7 asp ASP4 10002 15000 sua
 remote-ip 3.3.3.3

cs7 as BLUE sua
 routing-key 100 10.3.8 ssn 8
 asp ASP1
 asp ASP2
 traffic-mode override

cs7 as GREEN sua
 routing-key 200 10.3.8 ssn 7
 asp ASP2
 asp ASP3
 asp ASP4
  
```

ITP Signaling Gateway: ASPs with Unique Point Codes Configuration Example

Figure 21 ITP Signaling Gateway: ASPs with Unique Point Codes



The following configuration example is illustrated in [Figure 21](#).

```

cs7 variant ansi
cs7 point-code 10.3.5

interface ethernet 0/0
 ip address 4.4.4.4 255.255.255.128

cs7 m3ua 2905
 local-ip 4.4.4.4

cs7 asp ASP1 2905 2905 m3ua
 remote-ip 1.1.1.1
cs7 asp ASP2 2905 2905 m3ua
 remote-ip 2.2.2.2

cs7 as ISUPAS m3ua
 routing-key 100 4.4.4
 asp ASP1
 asp ASP2

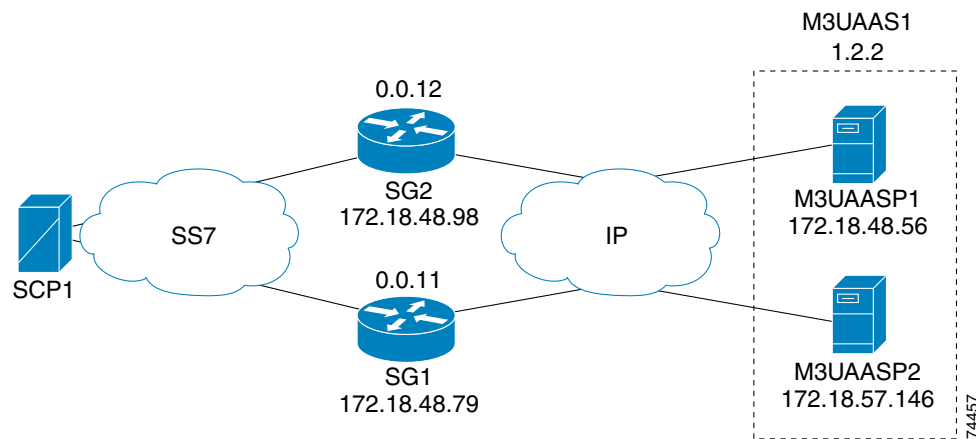
cs7 as ISUPASP1 m3ua
 routing-key 200 4.4.5
 asp ASP1

cs7 as ISUPASP2 m3ua
 routing-key 300 4.4.6
 asp ASP2

```

ITP SG Mated-SG Configuration Example

Figure 22 ITP Signaling Gateway: Mated-SG



The following configuration example is illustrated in [Figure 22](#).

SG1:

```

cs7 variant ANSI
cs7 point-code 0.0.11
!
interface FastEthernet0/0
 ip address 172.18.48.79 255.255.255.128
!

```

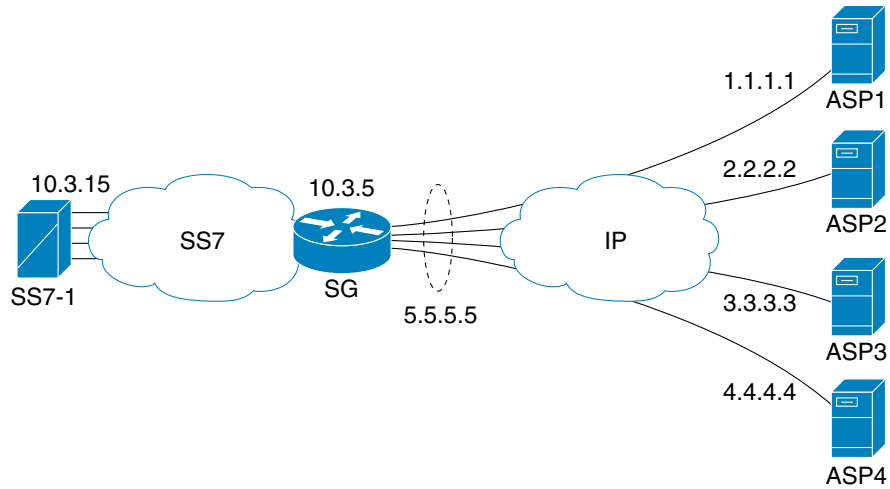
```
cs7 m3ua 2905
  local-ip 172.18.48.79
!
cs7 9999
  local-ip 172.18.48.79
!
cs7 mated-sg sg2 9999
  remote-ip 172.18.48.98
!
cs7 asp m3uaasp1 2905 2905 m3ua
  remote-ip 172.18.48.56
!
cs7 asp m3uaasp2 2905 2905 m3ua
  remote-ip 172.18.57.146
!
cs7 as M3UAAS1 m3ua
  routing-key 200 1.2.2
  asp m3uaasp1
  asp m3uaasp2
  traffic-mode override
!
```

SG2:

```
cs7 variant ANSI
cs7 point-code 0.0.12
!
interface FastEthernet0/0
  ip address 172.18.48.98 255.255.255.128
!
cs7 m3ua 2905
  local-ip 172.18.48.98
!
cs7 9999
  local-ip 172.18.48.98
!
cs7 mated-sg sg1 9999
  remote-ip 172.18.48.79
!
cs7 asp m3uaasp1 2905 2905 m3ua
  remote-ip 172.18.48.56
!
cs7 asp m3uaasp2 2905 2905 m3ua
  remote-ip 172.18.57.146
!
cs7 as M3UAAS1 m3ua
  routing-key 200 1.2.2
  asp m3uaasp1
  asp m3uaasp2
  traffic-mode override
!
```

ITP SG GTT Configuration Example

Figure 23 ITP Signaling Gateway: GTT



74461

The following configuration example is illustrated in [Figure 23](#).

```
cs7 variant ansi
cs7 point-code 10.3.5

interface ethernet 0/0
 ip address 5.5.5.5 255.255.255.128
interface serial 0/0
 encapsulation mtp2

cs7 sua 14001
 local-ip 5.5.5.5

cs7 m3ua 15000
 local-IP 5.5.5.5

cs7 route-table system

cs7 asp ASP1 10001 15000 m3ua
 remote-ip 1.1.1.1
cs7 asp ASP2 10001 15000 m3ua
 remote-ip 2.2.2.2
cs7 asp ASP3 14001 14001 sua
 remote-ip 3.3.3.3
cs7 asp ASP4 14001 14001 sua
 remote-ip 4.4.4.4

cs7 as BLUE m3ua
 routing-key 1 gtt
 asp ASP1
 asp ASP2
 traffic-mode override

cs7 as GREEN sua
 routing-key 2 gtt
 asp ASP3
 asp ASP4
 traffic-mode loadshare
```

```

cs7 as GREENASP3 sua
  routing-key 3 gtt
  asp ASP3

cs7 as GREENASP4 sua
  routing-key 4 gtt
  asp ASP4

cs7 linkset SS71 10.3.15
  link 0 serial 0/0
  route all table system

cs7 gtt selector 800NUM tt 255
  gta 800456 app-grp BLUE800
  gta 800457 app-grp GREEN800

cs7 gtt selector E164SEL tt 14
  gta 1123456789001 asname GREENASP3 pcssn
  gta 1123456789002 asname GREENASP4 pcssn

cs7 gtt application-group BLUE800
  multiplicity cost
  asname BLUE 1 pcssn
  pc 10.3.15 2 gt

cs7 gtt application-group GREEN800
  multiplicity cost
  asname GREEN 1 pcssn
  pc 10.3.15 2 pcssn

```

ITP SG QoS Configuration Examples

Example 1

In Example 1 all the traffic flowing to asp1 will be classified based on the QoS class 3 since asp1 belongs to AS as1.

```

cs7 qos class 3
  qos-ip-precedence 3
!
cs7 m3ua 2905
  local-ip 7.7.7.7
!
cs7 asp asp1 2905 2905 m3ua
  remote-ip 5.5.5.5
!
cs7 as as1 m3ua
  routing 05050505 4.4.4
  asp asp1
  qos-class 3
!

```

Example 2

In Example 2, since asp2 has been provisioned with qos-class 4, all the traffic flowing to asp2 will be classified with QoS class 4.

```
cs7 qos class 4
    qos-ip-dscp 40
!
cs7 m3ua 2905
    local-ip 7.7.7.7
!
cs7 asp asp2 2905 2905 m3ua
    remote-ip 5.5.5.6
    qos-class 4
!
cs7 as as2 m3ua
    routing 05050506 4.4.4
    asp asp1
!
```

Example 3

In Example 3 the ISUP and SCCP ASPs are located on the same host (same IP address, but different SCTP ports). They are defined as two different ASPs. Since isup-asp belongs to isup-as and isup-as-bk ASes, the QoS with highest IP Type Of Service (TOS), i.e. qos-class 5, will be used for the traffic flowing to isup-asp. Also the traffic flowing to sccp-asp will be classified based on QoS class 3 since this ASP belongs to AS sccp-as.

```
cs7 qos class 3
    qos-ip-precedence 3
cs7 qos class 5
    qos-ip-precedence 5
!
cs7 m3ua 2905
    local-ip 7.7.7.7
!
cs7 asp isup-asp 5500 2905 m3ua
    remote-ip 6.6.6.6
cs7 asp sccp-asp 6000 2905 m3ua
    remote-ip 6.6.6.6
!
cs7 as isup-as m3ua
    routing-key 06060606 5.5.5
    asp isup-asp
    qos-class 5
!
cs7 as isup-as-bk m3ua
    routing-key 07070707 6.6.6
    asp isup-asp
    qos-class 3
!
cs7 as sccp-as m3ua
    routing-key 08080808 7.7.7
    asp sccp-asp
    qos-class 3
!
```

Example 4

In Example 4 any traffic coming in from asp3 will be classified as having QoS class 3. Also any ISUP (si=5) traffic coming in from asp4 will be classified as having QoS class 5. The packet is classified this way so that, if needed, it would properly get routed over M2PA links, as explained in the [“Specifying QoS Routing Over M2PA Links”](#) section on page 297.

```
cs7 qos class 3
    qos-ip-precedence 3
cs7 qos class 5
    qos-ip-dscp 40
!
cs7 m3ua 2905
    local-ip 7.7.7.7
!
cs7 asp asp3 2905 2905 m3ua
    remote-ip 6.6.6.10
    match any qos-class 3
cs7 asp asp4 2905 2905 m3ua
    remote-ip 6.6.6.11
    match si 5 qos-class 5
!
```




Gateway Screening (GWS)

The Cisco ITP Gateway Screening (GWS) feature prevents unauthorized use of the STP and controls the flow of messages into or through the STP. GWS examines the contents of the incoming or outgoing Message Signaling Unit (MSU) and either allows or rejects the MSU based on the provisioned screening. GWS can be implemented in conjunction with access lists, Global Translation Table (GTT), and Multi-Layer Routing (MLR).

GWS allows you to configure GWS tables to drop an SCCP packet based on matching a set of conditions. When you drop an SCCP packet, an SCCP error return function sends a UDTs back to the source of the SCCP packet.

Feature History for GWS

Release	Modification
12.4(15)SW7	Egress traffic rate limit introduced.
12.2(33)IRA	Feature introduced.
12.2(33)IRF	Ingress traffic rate limit introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



Note

Configuration Mode Restrictions—Simultaneous changes to the configuration from multiple CLI sessions are not supported. At a time, only one configuration session is allowed to enter in configuration mode; other sessions should not enter in configuration mode. The **show line** or **show users EXEC** command may be used to determine the active user sessions on an ITP, and the **clear line EXEC** command may be used to ensure that only a single active session exists.

Contents

- [Information About GWS, page 164](#)
- [How to Configure GWS, page 178](#)
- [Monitoring GWS, page 195](#)

- [Configuration Examples for GWS, page 198](#)
- [Additional References, page 202](#)

Information About GWS

Screening rules are specified in tables and are applied to an inbound or outbound linkset or an application server (AS). If the incoming message is allowed, it is sent to MTP/SCCP/ISUP/M3UA/SUA for further processing. If the outgoing message is allowed, it is routed to the specified destination.

The following sections provide more detail about GWS:

- [GWS Tables, page 164](#)
- [GWS Table Matching Order for Incoming Packets, page 175](#)

GWS Tables

GWS tables are identified by the type of screening to be applied.

Each GWS table consists of two types of information:

- Screening information: screening parameters
- Structural information: next screening steps

Screening rules are chained to indicate the next screening steps. The final result is either to allow the message for further routing or to discard the message.

For a given chain, only one occurrence of a screening table type is allowed. For example, if the incoming message is to be screened against an allowed OPC table and the next step is to screen against an allowed DPC table, the third step cannot be to screen against an allowed OPC table.

The next screening step in any screening table must indicate either:

- An action set defined in the configuration
- A next step table.

[Table 9](#) shows an example of an allowed screening table, in this case an allowed opc table:

Table 9 *Sample Allowed OPC Table*

PC Start	PC End	Next Screening Step Allowed
x.x.x	y.y.y	table allowed-dpc1
x1.x1.x1	y1.y1.y1	table allowed-dpc1
default		action-set reject-ver

Figure 24 shows chained screening tables that screen incoming messages based on Linkset, OPC, and SI. Figure 25 shows chained screening tables that screen incoming messages based on AS, OPC, and SI.

Figure 24 Chained Screening Tables - MTP

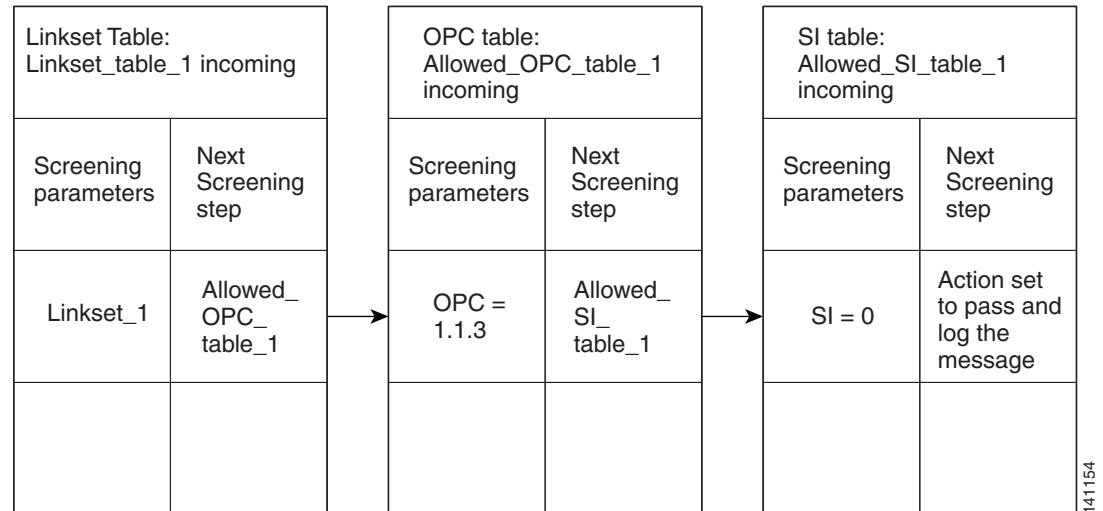


Figure 25 Chained Screening Tables - xUA

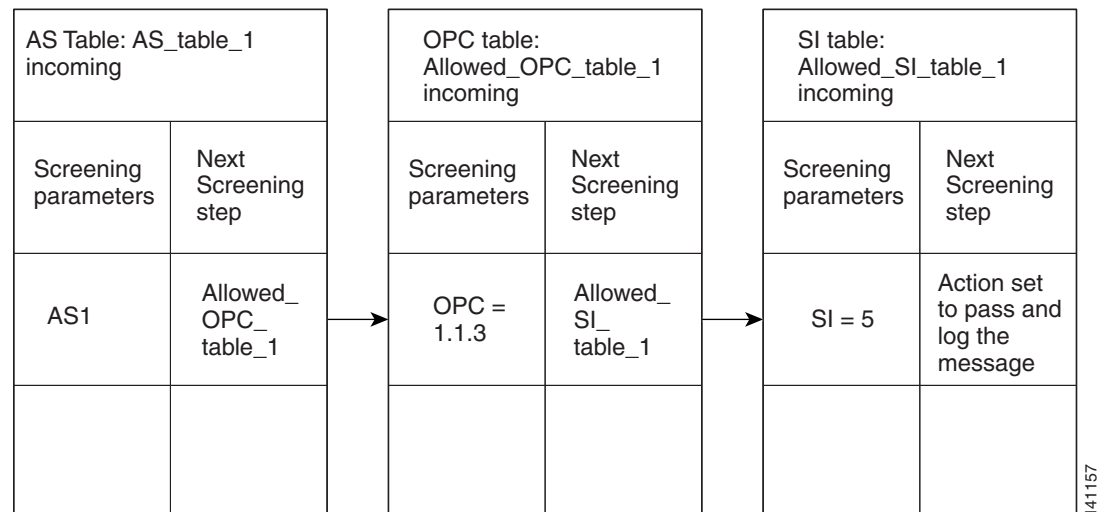


Table 10, Table 11, and Table 12 list valid GWS screening table types and the valid configuration commands for each type:

Table 10 *MTP Parameters*

Table Type	Description	Screening Commands
aff-dest	Affected destination in MTP management messages.	• pc-range • default
dpc	Destination Point Code	• pc-range • default
mtp-msg-type	MTP message type	• si mtp-msg-h0 mtp-msg-h1-range • si mtp-msg-type • default
opc	Originating Point Code	• pc-range • default
sio	SIO Table	• si • default

Table 11 *SCCP Parameters*

Table Type	Description	Screening Commands
aff-pc-ssn	Affected PC-SSN in SCCP management messages • Affected PC • Affected SSN	• pc-range ssn • default
cdpa-gta-prefix	CdPA GTA Prefix Table • Minimum Digits • Maximum Digits • GTA prefix	• gta-prefix • default
cdpa-gta-range	CdPA GTA Range Table • GTA range	• gta-start • default
cdpa-pc-ssn	Called Party Address PC-SSN • CdPA-SSN • CdPA-PC • CdPA SCMG format ID	• pc-range ssn • default

Table 11 **SCCP Parameters (continued)**

Table Type	Description	Screening Commands
cdpa-selector	Called Party Selector • TT (Translation Type) • GTI (Global Title Indicator) • NP (Numbering Plan) • NAI (Nature of Address Indicator)	• tt-range • default
cgpa-gta-prefix	CgPA GTA Prefix Table • Minimum Digits • Maximum Digits • GTA prefix	• gta-prefix • default
cgpa-gta-range	CgPA GTA Range Table • GTA range	• gta-start • default
cgpa-pc-ssn	Calling Party Address PC-SSN • CgPA-SSN • CgPA-PC	• pc-range ssn • default
cgpa-selector	Calling Party Selector • TT (Translation Type) • GTI (Global Title Indicator) • NP (Numbering Plan) • NAI (Nature of Address Indicator)	• tt-range • default
sccp-msg-hdr	SCCP Header Message Type	• sccp-msg • default

Table 12 **ISUP Parameters**

Table Type	Description	Screening Commands
isup-msg-type	ISUP message type (IAM, ACM, etc.)	• isup-msg-type • default

Table 13 shows possible next step chained table types given the current table.

Table 13 **Next Step Tables**

Current Table	Possible Next Step Tables
Gateway linkset or AS	• Allowed opc • Blocked opc • Allowed sio • Blocked sio • Allowed dpc • Blocked dpc • Action-set to allow block the message
Allowed opc	• Blocked opc • Allowed sio • Blocked sio • Allowed dpc • Blocked dpc • Allowed cgpa-pc-ssn • Blocked cgpa-pc-ssn • Action-set to allow block the message
Blocked opc	For default: • Allowed sio • Blocked sio • Allowed dpc • Blocked dpc • Allowed cgpa-pc-ssn • Blocked cgpa-pc-ssn For each entry: • Action-set to block the message

Table 13 **Next Step Tables (continued)**

Current Table	Possible Next Step Tables
Allowed sio	- Blocked sio - Allowed dpc - Blocked dpc If si = 0 - Allowed aff-dest - Blocked aff-dest - Allowed mtp-msg-type - Blocked mtp-msg-type If si = 1 or 2 - Allowed mtp-msg-type - Blocked mtp-msg-type If si = 3 - Allowed cgpa-pc-ssn - Blocked cgpa-pc-ssn - Allowed cdpa-pc-ssn - Blocked cdpa-pc-ssn - Allowed sccp-msg-hdr - Blocked sccp-msg-hdr If si = 5 - Allowed isup-msg-type - Blocked isup-msg-type Action-set to allow block message

Table 13 **Next Step Tables (continued)**

Current Table	Possible Next Step Tables
Blocked sio	For default • Allowed dpc • Blocked dpc If si = 0 • Allowed aff-dest • Blocked aff-dest • Allowed mtp-msg-type • Blocked mtp-msg-type If si = 1 or 2 • Allowed mtp-msg-type • Blocked mtp-msg-type If si = 3 • Allowed cgpa-pc-ssn • Blocked cgpa-pc-ssn • Allowed cdpa-pc-ssn • Blocked cdpa-pc-ssn • Allowed sccp-msg-hdr • Blocked sccp-msg-hdr If si = 5 • Allowed isup-msg-type • Blocked isup-msg-type For each entry • Action-set to block message
Allowed dpc	• Blocked dpc • Allowed aff-dest • Blocked aff-dest • Allowed cgpa-pc-ssn • Blocked cgpa-pc-ssn • Allowed isup-msg-type • Blocked isup-msg-type • Action-set to allow block message

Table 13 *Next Step Tables (continued)*

Current Table	Possible Next Step Tables
Blocked dpc	For default - Allowed aff-dest - Blocked aff-dest - Allowed cgpa-pc-ssn - Blocked cgpa-pc-ssn - Allowed isup-msg-type - Blocked isup-msg-type For each entry - Action-set to block message
Allowed mtp-msg-type	- Blocked mtp-msg-type - Allowed dpc - Blocked dpc - Allowed aff-dest - Blocked aff-dest - Action-set to allow block message
Blocked mtp-msg-type	For default - Allowed dpc - Blocked dpc - Allowed aff-dest - Blocked aff-dest For each entry - Action-set to block message
Allowed aff-dest	- Blocked aff-dest - Action-set to allow block message
Blocked aff-dest	For default - No table allowed For each entry - Action-set to block message

Table 13 **Next Step Tables (continued)**

Current Table	Possible Next Step Tables
Allowed cgpa-pc-ssn	- Blocked cgpa-pc-ssn - Allowed sccp-msg-hdr - Blocked sccp-msg-hdr - Allowed cgpa-selector - Blocked cgpa-selector - Allowed cdpa-pc-ssn - Blocked cdpa-pc-ssn - Action-set to allow block message
Blocked cgpa-pc-ssn	For default - Allowed sccp-msg-hdr - Blocked sccp-msg-hdr - Allowed cgpa-selector - Blocked cgpa-selector - Allowed cdpa-pc-ssn - Blocked cdpa-pc-ssn For each entry - Action-set to block message
Allowed sccp-msg-hdr	- Blocked sccp-msg-hdr - Allowed cgpa-selector - Blocked cgpa-selector - Allowed cdpa-pc-ssn - Blocked cdpa-pc-ssn - Action-set to allow block message
Blocked sccp-msg-hdr	For default - Allowed cgpa-selector - Blocked cgpa-selector - Allowed cdpa-pc-ssn - Blocked cdpa-pc-ssn For each entry - Action-set to block message

Table 13 **Next Step Tables (continued)**

Current Table	Possible Next Step Tables
Allowed cgpa-selector	- Blocked cgpa-selector - Allowed cdpa-pc-ssn - Blocked cdpa-pc-ssn - Allowed cgpa-gta-prefix - Blocked cgpa-gta-prefix - Action-set to allow block message
Blocked cgpa-selector	For default - Allowed cdpa-pc-ssn - Blocked cdpa-pc-ssn - Allowed cgpa-gta-prefix - Blocked cgpa-gta-prefix For each entry - Action-set to block message
Allowed cgpa-gta-range	- Blocked cgpa-digit-screening - Allowed cdpa-pc-ssn - Blocked cdpa-pc-ssn - Action-set to allow block message
Allowed cgpa-gta-prefix	- Blocked cgpa-gta-prefix - Allowed cdpa-pc-ssn - Blocked cdpa-pc-ssn - Action-set to allow block message
Blocked cgpa-gta-range	For default - Allowed cdpa-pc-ssn - Blocked cdpa-pc-ssn For each entry - Action-set to block message
Blocked cgpa-gta-prefix	For default - Allowed cdpa-pc-ssn - Blocked cdpa-pc-ssn For each entry - Action-set to block message

Table 13 *Next Step Tables (continued)*

Current Table	Possible Next Step Tables
Allowed cdpa-pc-ssn	- Blocked cdpa-pc-ssn - Allowed cdpa-selector - Blocked cdpa-selector - Allowed aff-pc-ssn (if SSN = 1) - Blocked aff-pc-ssn (if SSN = 1) - Action-set to allow block message
Blocked cdpa-pc-ssn	For default - Allowed cdpa-selector - Blocked cdpa-selector - Allowed aff-pc-ssn (if SSN = 1) - Blocked aff-pc-ssn (if SSN = 1) For each entry - Action-set to block message
Allowed cdpa-selector	- Blocked cdpa-selector - Allowed cdpa-gta-range - Blocked cdpa-gta-range - Allowed cdpa-gta-prefix - Blocked cdpa-gta-prefix - Action-set to allow block message
Blocked cdpa-selector	For default - Allowed cdpa-gta-range - Blocked cdpa-gta-range - Allowed cdpa-gta-prefix - Blocked cdpa-gta-prefix For each entry - Action-set to block message
Allowed cdpa-gta-range	- Blocked cdpa-gta-range - Action-set to allow block message
Allowed cdpa-gta-prefix	- Blocked cdpa-gta-range - Blocked cdpa-gta-prefix - Action-set to allow block message
Blocked cdpa-gta-range	For default - No table allowed For each entry - Action-set to block message

Table 13 *Next Step Tables (continued)*

Current Table	Possible Next Step Tables
Blocked cdpa-gta-prefix	For default - No table allowed For each entry - Action-set to block message
Allowed aff-pc-ssn	- Blocked aff-pc-ssn - Action-set to allow block message
Blocked aff-pc-ssn	For default - No table allowed For each entry - Action-set to block message
Allowed isup-msg-type	- Blocked isup-msg-type - Action-set to allow block message
Blocked isup-msg-type	For default - No table allowed For each entry - Action-set to block message

GWS Table Matching Order for Incoming Packets

For information on the GWS Table Matching Order for Incoming Packets, see the [“MLR and GWS Table Matching Order for Incoming Packets”](#) section on page 241.

How GWS Works with Access Lists

GWS can work in conjunction with existing access lists.

Access lists are defined and applied on per linkset (inbound or outbound) basis. Access lists numbered between 2700 and 2999 are used for SS7. These access lists permit or deny traffic based on parameters - OPC, DPC, SI, bit pattern, affected PC, CdPA, CgPA.

Access list and gateway screening may be applied on the same linkset. However, neither access list nor gateway screening will verify that the screening rules are consistent with each other, if both are defined on the same linkset. Access lists take precedence for both incoming and outgoing linksets. If access list and gateway screening are defined for the same linkset, both will be executed with access list rules applied before gateway screening. Gateway screening rules will be applied only if the access list allows the message for further processing. GWS processing of MLR only applies to incoming messages.

[Figure 26](#) illustrates outgoing message processing with ACL, GWS, TTMAPPING. [Figure 27](#) illustrates incoming messages and including MLR routing processing through GWS.

Figure 26 Outgoing Message Processing with ACS, GWS, TTMAPPING

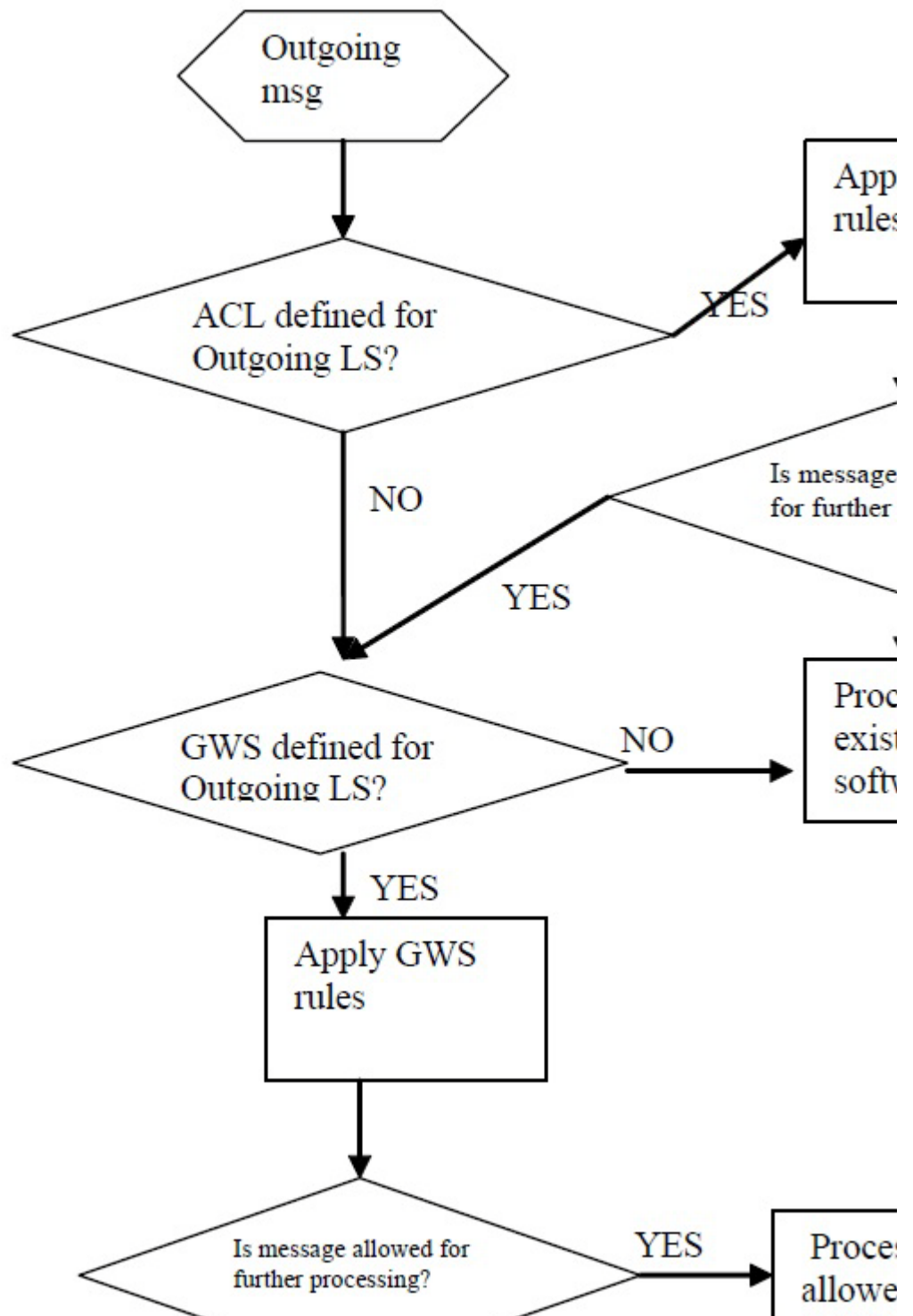
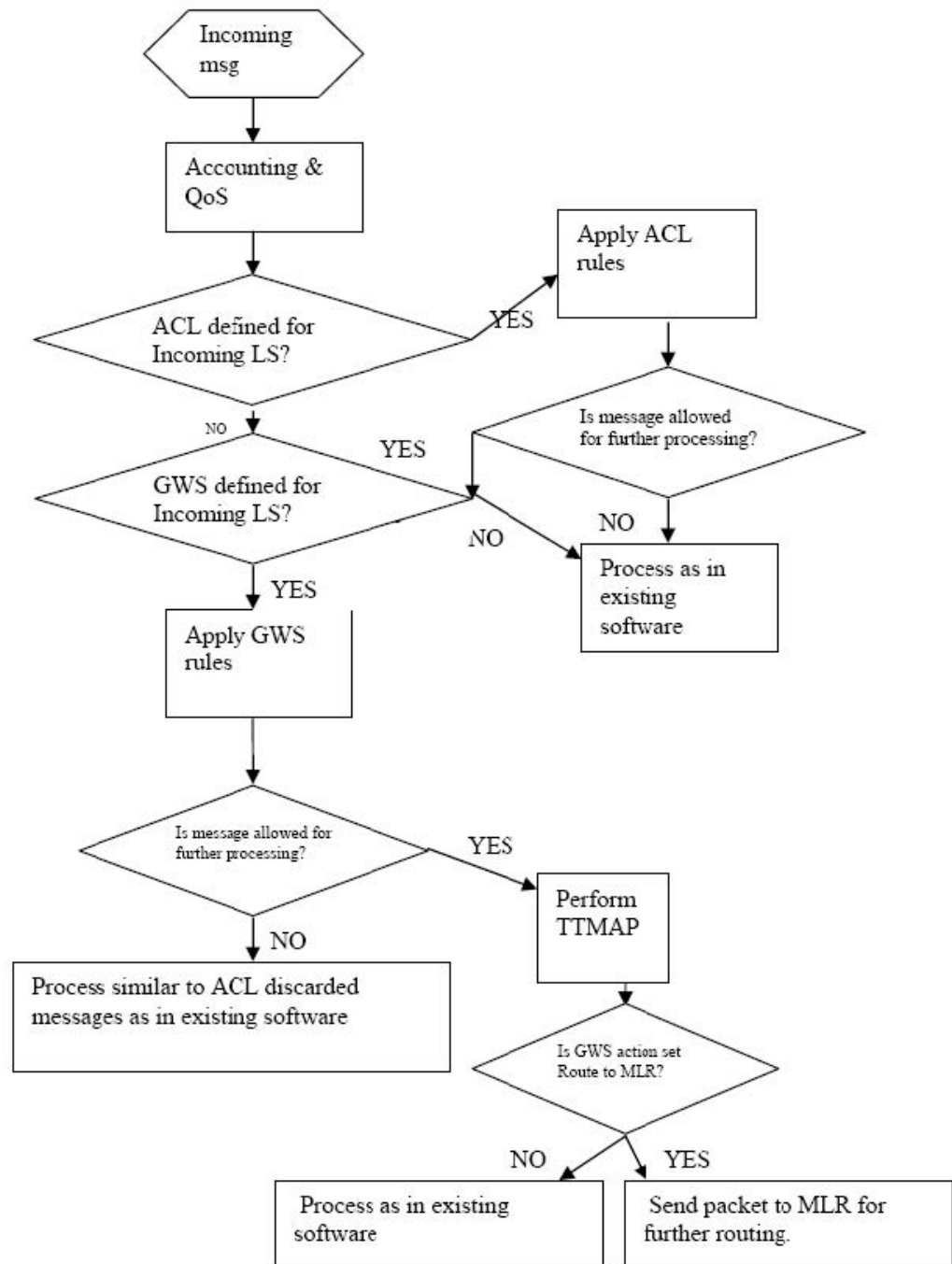


Figure 27 **Processing of Incoming Messages**



How to Configure GWS

This section describes how to configure GWS. You configure GWS by defining an access list and applying it to a linkset definition. GWS supports linksets, ASes, and existing screening and routing features, including access lists and Global Title Translation.

This section contains the following procedures:

- [Defining GWS Access Lists, page 179](#)
- [Defining GWS Action Sets, page 180](#)
- [Defining GWS Tables, page 182](#)
- [Defining Entries in GWS Tables, page 184](#)
- [Defining Gateway Linkset Tables, page 187](#)
- [Defining an AS Table for GWS, page 189](#)
- [Saving a GWS Table or a GWS Configuration to a Remote or Local File, page 192](#)
- [Loading a GWS Table and GWS Configuration from a Remote or Local File, page 192](#)
- [Replacing a Running GWS Configuration or Existing GWS Table with a Remote or Local File, page 194](#)
- [Validating and Auditing the Consistency of the GWS Files in the Line Card and Main Processor, page 194](#)

**Note**

GWS supports instance specific action sets in Cisco IOS software releases and later. If a user has GWS instance specific action sets configured in a supporting release, but then reverts to Cisco IOS software release or earlier, which do not support instance specific action sets, the configured instance specific action sets will be lost. Also link set tables, AS tables, and global tables that refer to the instance specific action sets will be lost.

GWS on an SS7 node allows you to permit or deny messages based on message characteristics. You can control access to or from the Cisco ITP by defining one or more access lists and then applying the access list to an inbound or outbound linkset.

Access lists filter traffic by controlling whether packets are forwarded or blocked at the router's interfaces. The router examines each packet to determine whether to forward or drop the packet, on the basis of the criteria you specified within the access lists.

If the access list is inbound, when the ITP receives a packet it checks the access list criteria statements for a match. If the packet is permitted, the ITP continues to process the packet. If the packet is denied, the ITP discards it.

If the access list is outbound, after receiving and routing a packet to the outbound interface the ITP checks the access list criteria statements for a match. If the packet is permitted, the ITP transmits the packet. If the packet is denied, the ITP discards it.

Defining GWS Access Lists

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list**
4. **cs7 linkset**
5. **access-group**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: ITP> enable	Enables privileged EXEC mode.
Step 2	configure terminal Example: ITP# configure terminal	Enters global configuration mode.
Step 3	ITP(config)# access-list <i>access-list-number</i> { deny permit } [dpc <i>point-code wildcard-mask</i> opc <i>point-code wildcard-mask</i> si { 0-15 } pattern <i>offset hex-pattern</i> aftpc <i>point-code wildcard-mask</i> cdpa <i>point-code wildcard-mask</i> cgpa <i>point-code wildcard-mask</i> <i>selector</i> <i>all</i>] Example: ITP(config)# access-list 2703 instance 0 permit dpc 0.0.6 1.1.1 opc 0.1.5 1.2.2	Defines an access list.
Step 4	cs7 linkset <i>ls-name adj-pc</i> ITP(config)# cs7 linkset <i>to_morehead</i> 1.1.1	Specifies a linkset and enters linkset configuration mode.
Step 5	access-group { 2700-2999 <i>name</i> } [in out] Example: ITP(config-cs7-ls)# access-group 2703 in	Applies the access list to the linkset.

Defining GWS Action Sets

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `cs7 [instance n] gws default`
4. `[inbound] result nextStep`
5. `cs7 gws action-set`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: ITP> <code>enable</code>	Enables privileged EXEC mode.
Step 2	<code>configure terminal</code> Example: ITP# <code>configure terminal</code>	Enters global configuration mode.
Step 3	<code>cs7 [instance n] gws default</code> Example: Router(config)# <code>cs7 gws default</code>	Applies globally to all link sets, all ASs, and all local applications in the CS7 instance.

	Command or Action	Purpose
Step 4	<pre>[inbound] result {action table} nextStep</pre> Example: Router(config-gws-default)# inbound result table nextStep	<i>nextStep</i> is either a GWS table or GWS action set. It is the same variable used in a GWS link set table or GWS AS table.
Step 5	<pre>[no] cs7 [instance instance-number] gws action-set action-set-name {allow block [sccp-error error] mlr {ruleset rule-set-name group result-group-name} [logging {silent file [verbose] console [verbose] file [verbose] console [verbose]}}</pre> Example: Router(config)# cs7 instance 0 gws action-set ACTION_SET mlr ruleset GWS_MLR_RULE	Configures a GWS action-set. When SCCP packets are dropped, the optional sccp-error parameter configures the block action to send a UDTs to the originator of the SCCP packet. It is also necessary for the UDT to have return-on-error set and a return cause configured to return UDTs with unqualified return cause. Table 14 lists UDTs return cause values. Note GWS action sets are instance based. mlr {ruleset rule-set-name group result-group-name}—(Optional) keyword allows the screened packet to be processed for routing by MLR. Note To enable MLR, perform the configuration tasks described in the following sections of the MLR Routing and Screening chapter: “Define MLR Global Options” section on page 206, “Define the MLR Group” section on page 207, and “Defining the MLR Modify-Profile” section on page 211 Note The GWS action set name must not contain the : file termination character.

Table 14 UDTs Return Cause Values

Value (hex)	Description
0x00	No translation for an address of such nature
0x01	No translation for this specific address
0x02	Subsystem congestion
0x03	Subsystem failure
0x04	Unequipped User
0x05	MTP failure
0x06	Network Congestion
0x07	Unqualified
0x08	Error in message transport (applicable only to XUDT and XUDTS)
0x09	Error in local processing (applicable only to XUDT and XUDTS)

Table 14 **UDTS Return Cause Values**

Value (hex)	Description
0X0A	Destination cannot perform reassembly (applicable only to XUDT and XUDTS)
0X0B	SCCP failure (only ITU)
0x0C	SCCP Hop counter violation (applicable only to XUDT and XUDTS)
0x0D (ITU)	Segmentation not supported
0x0E (ITU)	Segmentation failure
0x0F to 0xFF (ITU)	Spare
0x0D-0xF8, 0xFF (ANSI)	Spare
0xF9	Invalid ISNI routing request (applicable only to XUDT and XUDTS)
0xFA	Unauthorized message
0xFB	Message incompatibility
0xFC	Cannot perform ISNI constrained routing (applicable only to XUDT and XUDTS)
0xFD	Redundant ISNI constrained routing (applicable only to XUDT and XUDTS)
0xFE	Cannot perform ISNI identification (applicable only to XUDT and XUDTS)

Defining GWS Tables

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cs7 gws table type**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: ITP> enable	Enables privileged EXEC mode.
Step 2	configure terminal Example: ITP# configure terminal	Enters global configuration mode.
Step 3	[no] cs7 [instance n] gws table <i>table-name</i> type <i>table-type</i> [action allowed blocked] [gtt pregtt postgtt] Example: ITP(config)# cs7 instance 0 gws table cdpa-selector action allowed gtt pregtt	Configures a GWS table and enables GWS table configuration mode for the table type specified, in this example, a cdpa selector table. If no action is specified, the default is allowed. • type <i>cdpa_selector</i>—(Optional) defines the table type as CdPA. CdPA is the SCCP Called Party Address field. – Even if the CdPA tables are set up as postgtt, for packets that are not destined to ITP, only pre-gtt screening is applied. – Even if the CdPA tables are set up as pregtt, for outbound packets all GWS is post-GTT. – MLR does not apply for outbound packets and if the action-set at the end of GWS processing results in a MLR action for outbound packets, it is ignored and the packet is routed normally. – [gtt pregtt postgtt] keywords are only available with type <i>cdpa_selector</i>. • type <i>sio</i>—(Optional) specifies a service indicator in a table type sio. The following service indicator types are available: – isup—ISUP service indicator – mgmt— MTP n/w management service indicator – sccp— SCCP service indicator – test1— MTP n/w testing & maint. Regular SI – test2— MTP n/w testing & maint. Special SI – tup— TUP service indicator – bicc— BICC service indicator Note The GWS table name is not case sensitive. Note The GWS table name must not contain the : file termination character.

Defining Entries in GWS Tables

In this task you configure the screening parameter entries valid for the gateway table type that you specified in the **cs7 gws table** command. Each table can contain one or more entries.

In table entries with range parameters for entering minimum and maximum values, the second parameter is optional for single values. For single values, start and end parameters will be the same. A wildcard indicator (*) can be used for some ranges.

If the incoming/outgoing message parameters (based on the direction of the message) do not match any of the entries in the table, then the default rule is executed.

In compliance with GR-82-CORE Appendix C, blocked table entries have next step action-sets that block the message. The default entry in blocked tables can have table name or action-set as the next step.

Next-step tables differ depending on the table type you configured. Next step tables are listed in [Table 13](#).


Note

A table or action-set must be defined prior to its use in a next-step result.


Note

An action-set or a table cannot be deleted if it is referenced by other entries.


Note

The output of the **show running-config** command might show a table definition twice if it is referenced in other tables.


Note

The GWS table name is not case sensitive.

To configure a screening parameter entry in a GWS table, enter one or more of the following commands in gateway table configuration mode. The screening parameter commands are listed in alphabetical order and are not intended to be entered in the order shown. The table types to which they apply are listed in the **Purpose** column. The CLI prompt may differ slightly from the example, depending on the gateway table type you specified.

Command or Action	Purpose
default result { action <i>action-set-name</i> table <i>tablename</i> } Example: ITP(config-gws-opc-table)# default result action ALLOWED	Valid for all table types. Configures default screening for the table. If the incoming/outgoing message parameters (based on the direction of the message) do not match any of the entries in the table, the default rule is executed.
gta-prefix { <i>gta-pref</i> [exact] * } [min-digits <i>min-digits</i>] [max-digits <i>max-digits</i>] result { action <i>action-set-name</i> table <i>tablename</i> } Example: ITP(config-gws-cgpa-gta-pref-table)# gta-prefix 455 result action ALLOWED	Valid for the following table types: cgpa-gta-prefix , cdpa-gta-prefix .

Command or Action	Purpose
gta-start <i>gta-start</i> [<i>gta-end gta-end</i>] result { action <i>action-set-name</i> table <i>tablename</i> } Example: ITP(config-gws-cdpa-gta-table)# gta-start 3922000 gta-end 3924000 result action ALLOWED	Valid for the following table types: cgpa-gta-range , cdpa-gta-range .
isup-msg-type <i>isup-msg-type</i> result { action <i>action-set-name</i> table <i>tablename</i> } Example: ITP(config-gws-isup-msg-table)# isup-msg-type SAM result action ALLOWED	Valid for the following table types: isup-msg-type .
pc-range <i>pc-start</i> [<i>pc-end</i>] result { action <i>action-set-name</i> table <i>tablename</i> } Example: ITP(config-gws-opc-table)# pc-range 6.6.6 result table DPC1	Valid for the following table types: aff-dest , opc , dpc . Configures PC table entry - PC range. In a range parameter, which provides an option to enter minimum and maximum values, the second parameter is optional for single values. For single values, start and end parameters are the same. A wildcard indicator (*) can be used for a range of point codes, as shown in Table 15 .
pc-range <i>pc-start</i> [<i>pc-end</i>] ssn <i>ssn</i> result { action <i>action-set-name</i> table <i>tablename</i> } Example: ITP(config-gws-aff-pc-ssn-table)# pc-range 6.6.6 ssn 6 result table AFFPC	Valid for the following table types: cgpa-pc-ssn , cdpa-pc-ssn , aff-pc-ssn . Configures PC table entry - PC range + ssn screening. In a range parameter, which provides an option to enter minimum and maximum values, the second parameter is optional for single values. For single values, start and end parameters are the same. A wildcard indicator (*) can be used for a range of point codes, as shown in Table 15 .
sccp-msg <i>sccp-msg-type</i> result { action <i>action-set-name</i> table <i>tablename</i> } Example: ITP(config-gws-sccp-msg-hdr-table)# sccp-msg xudt result action ALLOWED	Valid for the following table types: sccp-msg-hdr
si <i>si</i> mtp-msg-h0 <i>mtp-msg-h0</i> mtp-msg-h1-range <i>mtp-msg-h1-start</i> [<i>mtp-msg-h1-end</i>] result { action <i>action-set-name</i> table <i>tablename</i> } -OR- si <i>si</i> mtp-msg-type <i>mtp-msg-type</i> result { action <i>action-set-name</i> table <i>tablename</i> } Example: ITP(config-gws-mtp-msg-table)# si test1 mtp-msg-type LTA result table AFF-DEST	Valid for the following table types: mtp-msg-type

Command or Action	Purpose
si <i>si</i> [priority-range <i>priority-start</i> [<i>priority-end</i>]] result { action <i>action-set-name</i> table <i>tablename</i> } Example: ITP(config-gws-sio-table)# si sccp result table PCSSN1	Valid for the following table types: sio
tt-range <i>tt-start</i> [<i>tt-end</i>] [gti <i>gti</i> [np <i>np</i> nai <i>nai</i>]] result { action <i>action-set-name</i> table <i>tablename</i> } Example: ITP(config-gws-cdpa-sel-table)# tt-range 5 10 gti 2 result table PGTA1	Valid for the following table types: cgpa-selector , cdpa-selector The gti <i>gti</i> parameter may only be specified if the variant is ITU. In a range parameter, which provides an option to enter minimum and maximum values, the second parameter is optional for single values. For single values, start and end parameters are the same. A wildcard indicator (*) can be used for a range of translation types, as shown in Table 16 .

A wildcard indicator (*) can be used to indicate a range of point codes, as shown in [Table 15](#).

Table 15 *PC Ranges with Wildcards*

pc-range with Wildcards	PC Range for ANSI and CHINA	PC Range for ITU
pc-range 1.1.*	1.1.0 – 1.1.255	1.1.0 – 1.1.7
pc-range 2.*.*	2.0.0 – 2.255.255	2.0.0 – 2.255.7
pc-range 3.3.2 3.3.*	3.3.2 – 3.3.255	3.3.2 – 3.3.7
pc-range 4.4.* 4.*.*	4.4.0 – 4.255.255	4.4.0 – 4.255.7

A wildcard indicator (*) can be used for a range of translation types (TT), as shown in [Table 16](#).

Table 16 *TT Ranges with Wildcards*

tt-range with Wildcards	Actual tt-range
tt-range *	0 – 255
tt-range 5 10	5 – 10
tt-range 8 *	8 – 255
tt-range 7	7 – 7

What to Do Next

Define a gateway linkset table or an AS table for GWS.

Defining Gateway Linkset Tables

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cs7** [*instance instance-number*] **gws linkset name** *ls-name*
4. **inbound** [**logging type** {*all* | *allow* | *block* | *rate-limit* | *mlr* {**group** *group* | **ruleset** *ruleset* } [**test**] {*silent* | *file* [*verbose*] | *console* [*verbose*] | *file* [*verbose*] *console* [*verbose*]}}] **result** {**action** *action-set-name* | **table** *tablename*}
5. **outbound** [**logging type** {*all* | *allow* | *block* | *rate-limit* | *mlr* {**group** *group* | **ruleset** *ruleset* } [**test**] {*silent* | *file* [*verbose*] | *console* [*verbose*] | *file* [*verbose*] *console* [*verbose*]}}] **result** {**action** *action-set-name* | **table** *tablename*}
6. **rate-limit-timer** *timer*
7. **rate-limit rate** *rate* [**onset-threshold** *othresh* [**abate-threshold** *athresh*]][**sccp-error** *sccp-error*]
8. **exit**
9. **cs7** [*instance instance-number*] **gws linkset default**
10. **inbound** [**logging type** {*all* | *allow* | *block* | *rate-limit* | *mlr* {**group** *group* | **ruleset** *ruleset* } [**test**] {*silent* | *file* [*verbose*] | *console* [*verbose*] | *file* [*verbose*] *console* [*verbose*]}}] **result** {**action** *action-set-name* | **table** *tablename*}
11. **outbound** [**logging type** {*all* | *allow* | *block* | *rate-limit* | *mlr* {**group** *group* | **ruleset** *ruleset* } [**test**] {*silent* | *file* [*verbose*] | *console* [*verbose*] | *file* [*verbose*] *console* [*verbose*]}}] **result** {**action** *action-set-name* | **table** *tablename*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: ITP> enable	Enables privileged EXEC mode.
Step 2	configure terminal Example: ITP# configure terminal	Enters global configuration mode.
Step 3	cs7 [instance <i>instance-number</i>] gws linkset name <i>ls-name</i> Example: ITP(config)# cs7 instance 0 gws linkset name dallas	Defines a gateway linkset table entry for a specified linkset, and enables gws linkset configuration mode.

	Command or Action	Purpose
Step 4	<pre>inbound [logging type {all allow block rate-limit mlr {group group ruleset ruleset } [test] {silent file [verbose] console [verbose] file [verbose] console [verbose]}} result {action action-set-name table tablename}</pre> Example: ITP(config-gws-ls)# inbound result table allowed-dpc1	Specifies the inbound screening result on the linkset.
Step 5	<pre>outbound [logging type {all allow block rate-limit mlr {group group ruleset ruleset } [test] {silent file [verbose] console [verbose] file [verbose] console [verbose]}} result {action action-set-name table tablename}</pre> Example: ITP(config-gws-ls)# outbound result action allow	Specifies the outbound screening result on the linkset.
Step 6	<pre>rate-limit-timer timer</pre> Example: ITP(config-gws-ls)# rate-limit-timer 5	Enables rate limiting for GWS linksets, configures the rate limit timer, and GWS linkset rate-limit-timer configuration mode. <i>timer</i>—The length of the time period set for the Cisco ITP to count received MSUs, expressed in seconds. The range is from 1 to 60 seconds.
Step 7	<pre>rate-limit rate rate [onset-threshold othresh [abate-threshold athresh]][sccp-error sccp-error]</pre> Example: ITP(config-gws-ls-rmt)# rate-limit rate 2000 onset-threshold 80 abate-threshold 60 sccp-error 3	Enables the rate limit for the traffic rate on specified linksets, for a message type. Rate-limiting is disabled by default. The default onset threshold is set to 90%. The default abate threshold is 10% lower than the onset threshold.
Step 8	<pre>exit</pre> Example: ITP(config-gws-ls)# exit	Exits gateway linkset configuration mode and enables global configuration mode.
Step 9	<pre>cs7 [instance instance-number] gws linkset default</pre> Example: ITP(config)# cs7 instance 0 gws linkset default	Defines the gateway linkset table default entry and enables gws linkset configuration mode.

	Command or Action	Purpose
Step 10	<pre>inbound [logging type {all allow block rate-limit mlr {group group ruleset ruleset } [test] {silent file [verbose] console [verbose] file [verbose] console [verbose]}} result {action action-set-name table tablename}</pre> Example: <pre>ITP(config-gws-ls)# inbound result action blocked-ver</pre>	Specifies the default inbound screening.
Step 11	<pre>outbound [[logging type {all allow block rate-limit mlr {group group ruleset ruleset ruleset } [test] {silent file [verbose] console [verbose] file [verbose] console [verbose]}} result {action action-set-name table tablename}</pre> Example: <pre>ITP(config-gws-ls)# outbound result action blocked-ver</pre>	Specifies the default outbound screening.

What to Do Next

Define an AS table for GWS.

Defining an AS Table for GWS

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cs7** [instance *instance-number*] **gws as name** *as-name*
4. **inbound** [logging type {all | allow | block | rate-limit | mlr {group *group* | ruleset *ruleset* } [test] {silent | file [verbose] | console [verbose] | file [verbose] console [verbose]}} result {action *action-set-name* | table *tablename*}
5. **outbound** [logging type {all | allow | block | rate-limit | mlr {group *group* | ruleset *ruleset* } [test] {silent | file [verbose] | console [verbose] | file [verbose] console [verbose]}} result {action *action-set-name* | table *tablename*}
6. **rate-limit-timer** *timer*
7. **rate-limit** *rate*
8. **exit**
9. **cs7** [instance *instance*] **as default**
10. **inbound** [logging type {all | allow | block | rate-limit | mlr {group *group* | ruleset *ruleset* } [test] {silent | file [verbose] | console [verbose] | file [verbose] console [verbose]}} result {action *action-set-name* | table *tablename*}

11. **outbound** [**logging type** {**all** | **allow** | **block** | **rate-limit** | **mlr** {**group** *group* | **ruleset** *ruleset* } [**test**] {**silent** | **file** [**verbose**] | **console** [**verbose**] | **file** [**verbose**] **console** [**verbose**]}}] **result** {**action** *action-set-name* | **table** *tablename*}
12. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: ITP> enable	Enables privileged EXEC mode.
Step 2	configure terminal Example: ITP# configure terminal	Enters global configuration mode.
Step 3	cs7 [instance <i>instance-number</i>] gws as name <i>as-name</i> Example: ITP(config)# cs7 instance 0 gws as name as2	Defines an AS table for GWS and enables GWS AS configuration mode.
Step 4	inbound [logging type { all allow block rate-limit mlr { group <i>group</i> ruleset <i>ruleset</i> } [test] { silent file [verbose] console [verbose] file [verbose] console [verbose]}}] result { action <i>action-set-name</i> table <i>tablename</i> } Example: ITP(config-gws-as)# inbound result action ALLOW	Specifies the inbound screening result for the AS.
Step 5	outbound [logging type { all allow block rate-limit mlr { group <i>group</i> ruleset <i>ruleset</i> } [test] { silent file [verbose] console [verbose] file [verbose] console [verbose]}}] result { action <i>action-set-name</i> table <i>tablename</i> } Example: ITP(config-gws-as)# outbound result action allow	Specifies the outbound screening result for the AS.
Step 6	rate-limit-timer <i>timer</i> Example: ITP(config-gws-as)# rate-limit-timer 5	Enables rate limiting for the GWS AS, configures the rate limit timer, and enters GWS AS rate-limit-timer configuration mode. <i>timer</i> —The length of the time period set for the Cisco ITP to count received MSUs, expressed in seconds. The range is 1 to 60 seconds.

	Command or Action	Purpose
Step 7	rate-limit <i>rate rate</i> [onset-threshold <i>othresh</i> [abate-threshold <i>athresh</i>]] [sccp-error <i>sccp-error</i>] Example: ITP(config-gws-as-rmt)# rate-limit rate 2000 onset-threshold 80 abate-threshold 60 sccp-error 3	Enables the rate limit for traffic rate on a specified GWS AS, for a message type. Rate-limiting is disabled by default. The default onset threshold is set to 90%. The default abate threshold is 10% lower than the onset threshold.
Step 8	exit Example: ITP(config)# exit	Exits GWS AS configuration mode and enables global configuration mode.
Step 9	cs7 [instance <i>instance-number</i>] gws as default Example: ITP(config)# cs7 instance 0 gws as default	Defines the AS table default entry.
Step 10	inbound [logging type { all allow block rate-limit mlr { group <i>group</i> ruleset <i>ruleset</i> } [test] { silent file [verbose] console [verbose] file [verbose] console [verbose]}} result { action <i>action-set-name</i> table <i>tablename</i> } Example: ITP(config-gws-as)# inbound logging type block file console verbose result table SIO0	Specifies the default inbound screening for the AS.
Step 11	outbound [logging type { all allow block rate-limit mlr { group <i>group</i> ruleset <i>ruleset</i> } [test] { silent file [verbose] console [verbose] file [verbose] console [verbose]}} result { action <i>action-set-name</i> table <i>tablename</i> } Example: ITP(config-gws-as)# outbound result action BLOCK	Specifies the default outbound screening for the AS.
Step 12	exit Example: ITP(config)# exit	Exits GWS AS configuration mode and enables global configuration mode.

What to Do Next

Perform saving, loading, or replacing GWS configurations and table tasks, as needed.

Saving a GWS Table or a GWS Configuration to a Remote or Local File

You can save a GWS table file or a general GWS configuration file to a local or remote file system.

Cisco IOS CLI modifications to GWS configurations may take up to 15 seconds to take effect on all linecards after the last change is made. The standard Cisco IOS CLI command `copy running-config startup-config` or `write memory`, which saves the running configuration, does not automatically save the GWS table or the GWS configuration. The user needs to save this GWS information manually. The saved provisioning will load during a Cisco ITP restart or reload.

To save this GWS information manually use the following procedure:

SUMMARY STEPS

1. **enable**
2. **cs7** [*instance-number*] **save gws-table** *table-name* *url*
3. **cs7** [*instance-number*] **save [all] gws** *url*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: ITP> enable	Enables privileged EXEC mode.
Step 2	cs7 [<i>instance-number</i>] save gws-table <i>table-name</i> <i>url</i> Example: itp# cs7 save gws-table dpc0 disk0:gws-dpc0	Saves a GWS table. <i>url</i> is the specified destination for the saved file. Note The default location of general GWS configuration files is <code>cs7:gws-config</code> . For GWS table files it is under <code>cs7:gws-tables</code> .
Step 3	cs7 [<i>instance-number</i>] save [all] gws config <i>url</i> Example: itp# cs7 save gws disk0:gws-config	Saves a general GWS configuration. Valid URLs are <code>bootflash</code> , <code>disk0</code> , <code>disk1</code> , <code>disk2</code> , <code>slot0</code> , <code>slot1</code> , <code>tftp</code> , <code>flash</code> , <code>sup-bootdisk</code> , <code>sup-bootflash</code> , <code>rcp</code> . If the save operation fails, the system generates an error message with the cause of the problem.

Loading a GWS Table and GWS Configuration from a Remote or Local File

You can configure Cisco ITP to load all the GWS configuration, including general GWS configuration files and GWS table files, from a local or remote file. Cisco IOS CLI modifications to GWS configurations may take up to 15 seconds to take effect on all linecards after the last change is made. Cisco IOS CLI configuration is not allowed during file loading or replacement.

The load command does not initiate the restart or reload needed to trigger the actual load operation. It configures the load operation to occur when a restart or reload occurs.

Configure Cisco ITP to load a GWS configuration from a local or remote file with the following procedure:

**Note**

Loading and replacement of GWS configuration files and tables may take a significant amount of time to complete. The user is notified of completion through a console message.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cs7 [instance *instance-number*] gws load *url***

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: ITP> enable	Enables privileged EXEC mode.
Step 2	configure terminal Example: ITP# configure terminal	Enters global configuration mode.
Step 3	cs7 [instance <i>instance-number</i>] gws load <i>url</i> Example: itp(config)#cs7 gws load disk0:gws-config	Loads GWS configuration, including GWS tables, from a specified remote or local file during a Cisco ITP restart or reload. Valid URLs are bootflash, disk0, disk1, disk2, slot0, slot1, tftp, flash, sup-bootdisk, sup-bootflash, rcp.  Caution Specifying a remote file for the load command is not recommended as a best practice for high availability deployments, such as the Cisco 7600. Note If the load operation fails, the system generates an error message with the cause of the problem. Syntax errors in the loaded file cause the load operation to fail.

Replacing a Running GWS Configuration or Existing GWS Table with a Remote or Local File

This procedure replaces the running GWS configuration or existing GWS tables with a local or remote file. Cisco IOS CLI modifications to GWS configurations may take up to 15 seconds to take effect on all linecards after the last change is made. Cisco IOS CLI configuration is not allowed during file loading or replacement. Configuration file and table replacement does not take place until all entries in the new file have been read and validated.

To accomplish this, complete the following procedure:



Caution

When replacing a running GWS configuration, the replacement configuration or table is restricted to a maximum of 1000 table entries.



Note

Loading and replacement of GWS configuration files and tables may take a significant amount of time to complete. The user is notified of completion through a console message.

SUMMARY STEPS

1. **enable**
2. **cs7** [*instance instance-number*] **gws replace url**
3. **cs7** [*instance instance-number*] **gws-table replace url**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: itp> enable	Enables privileged EXEC mode.
Step 2	cs7 [<i>instance-number</i>] gws replace url Example: itp(config)# cs7 gws replace disk0:gws-replace	(Optional) Replaces the running GWS configuration with the configuration file specified by the URL.
Step 3	cs7 [<i>instance-number</i>] gws-table table-name replace url Example: itp# cs7 gws-table replace disk0:gws-replace	(Optional) Replaces a single GWS table with the table configuration file specified by the URL. Valid URLs are bootflash, disk0, disk1, disk2, slot0, slot1, tftp, flash, sup-bootdisk, sup-bootflash, rcp.

Validating and Auditing the Consistency of the GWS Files in the Line Card and Main Processor

This procedure validates and audits the consistency of the GWS configuration files and GWS table files contained in the line card and main processor. These files should sync from the line card to the main processor when the configuration of the GWS files change in the main processor. If the procedure

recognizes inconsistencies between the the GWS files in the line card and main processor, a second sync takes place. Configure Cisco ITP to validate and audit the consistency of the GWS configuration files and GWS table files contained in the line card and main processor with the following procedure:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cs7 audit [timer [timer-minutes]] [GWS [sync]]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: ITP> enable	Enables privileged EXEC mode.
Step 2	configure terminal Example: ITP# configure terminal	Enters global configuration mode.
Step 3	cs7 audit [timer [timer-minutes]] [GWS] Example: itp(config)#cs7 audit GWS	Validates and audits the consistency of the GWS configuration files and GWS table files contained in the line card and main processor.  Note To see the latest audit begin time, end time, and status, use the <code>show cs7 audit</code> command.

Monitoring GWS

- [Message Logging, page 195](#)
- [Verifying GWS Configuration, page 197](#)

Message Logging

Message logging allows you to capture information about screening results. GWS supports three types of logging:

- Silent mode: Message screened without any logging
- Test mode: Screening is done, but the screening results are NOT applied. For instance, if a linkset is configured to be in test mode, and after screening, screened result is to discard the message, the message is NOT discarded, but the log is updated to indicate that the message would be discarded if the screening rules were to apply. Test mode is applicable at the linkset or AS level or global levels. Test mode does not apply to action sets.

- Non-test mode: Screening results are applied to the message. That is, if the screening result is to discard the message, the message is actually discarded.

Two types of logging are possible in test and non-test mode: File and Console. File mode has an optional verbose mode which also logs up to 40 bytes of the message that was screened along with other parameters. In file mode, as the name suggests, the log is copied to a file. In console mode, the log is printed on the terminal. Console mode also has an optional verbose mode to include up to 40 bytes of the screened message.

SUMMARY STEPS

1. **enable**
2. **cs7 save log type destination**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: ITP> enable	Enables higher privilege levels, such as privileged EXEC mode.
Step 2	cs7 save log type destination Example: ITP# cs7 save log gws-test tftp://10.1.1.3/logs/gws-test-log1.txt	Saves a log to a specified destination.

To enable logging, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cs7 log type {checkpoint seconds destination | size size | verbose}**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: ITP> enable	Enables higher privilege levels, such as privileged EXEC mode.
Step 2	configure terminal Example: ITP# configure terminal	Enters global configuration mode.
Step 3	cs7 log type {checkpoint seconds destination size size verbose} Example: ITP(config)# cs7 log gws-nontest size 10000	Enables logging.

Verifying GWS Configuration

After enabling privileged exec mode, the following show commands can be used in any order to display GWS linkset, as, or table information.

SUMMARY STEPS

1. **enable**
2. **show cs7 gws action-set** *[name]*
3. **show cs7 gws as** *[default | name as-name]*
4. **show c7 gws default**
5. **show cs7 gws linkset** *[default | name ls-name]*
6. **show cs7** *[instance number]* **gws table** *[name table-name | type table-type]* *[detail | result-summary | entry-summary]*
7. **show cs7** *[instance number]* **gws config**
8. **show cs7** *[instance number]* **gws table-config** *table-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: ITP> enable	Enables higher privilege levels, such as privileged EXEC mode.
Step 2	show cs7 gws action-set [<i>name</i>] Example: ITP# show cs7 gws action-set	Displays GWS action-set information. Details include UDTs configuration for block results and MLR ruleset name and/or result group name for MLR results.
Step 3	show cs7 gws as [default name <i>as-name</i>] Example: ITP# show cs7 gws as	Displays GWS AS information, including MLR routed MSUs.
Step 4	show cs7 gws default Example: ITP# show cs7 gws default	Displays the global (default) GWS table for an instance.
Step 5	show cs7 gws linkset [default name <i>ls-name</i>] Example: ITP# show cs7 gws linkset	Displays GWS linkset information, including MLR routed MSUs.
Step 6	show cs7 [<i>instance number</i>] gws table [name <i>table-name</i> type <i>table-type</i>] [detail result-summary entry-summary] Example: ITP# show cs7 gws table	Shows GWS table information.
Step 7	show cs7 [<i>instance number</i>] gws config Example: ITP# show cs7 5 gws config	Displays the whole configuration of GWS, including global action sets, linksets, global table entries, tables, and table entries.
Step 8	show cs7 [<i>instance number</i>] gws table-config [<i>table-name</i>] Example: ITP# show cs7 5 gws table-config 5	Displays the table entries or the entries for the specified table.

Configuration Examples for GWS

This section provides configuration examples of GWS in the following scenarios:

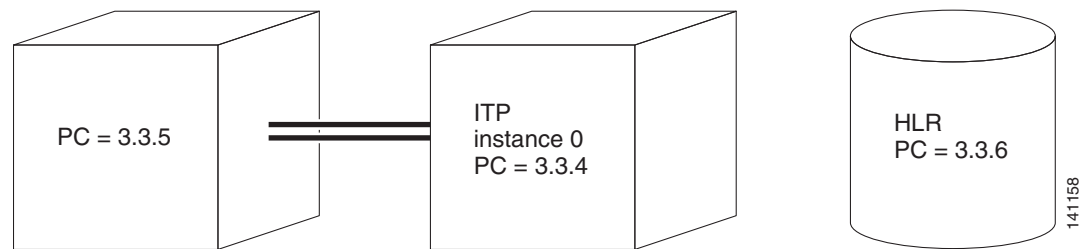
- [GWS Scenario: Linkset with Allowed DPC, page 199](#)
- [GWS Scenario: XUA AS with Allowed DPC, page 200](#)

- [GWS Scenario with CgPA, CdPA, page 200](#)

GWS Scenario: Linkset with Allowed DPC

In this usage scenario, an allowed DPC table is created. The DPC table is linked to a linkset.

Figure 28 *GWS Scenario: Linkset with Allowed DPC*



```

cs7 multi-instance
cs7 instance 0 variant ITU
cs7 instance 0 network-name INST0
cs7 instance 0 point-code 3.3.4
cs7 instance 1 variant ITU
cs7 instance 1 network-name INST1
cs7 instance 1 point-code 1.1.3

controller E1 0/0
  clock source line primary
  channel-group 0 timeslots 1
!
controller E1 0/1
  channel-group 0 timeslots 1
...

cs7 instance 0 linkset dallas 3.3.5
  accounting

! Define links as required

cs7 instance 0 route-table
cs7 instance 1 route-table

! Define action set for allowed verbose and blocked verbose
cs7 instance 0 gws action-set allowed-ver allow
cs7 instance 0 gws action-set blocked-ver block

! Define the allowed DPC table
! Screening is independent of MTP routes and XUA AS DPC.
! Although there is no route defined to 3.3.6, it can be added to
! allowed DPC table
cs7 in 0 gws table allowed-dpc-1 type dpc action allowed
  default result action-set blocked-ver
  pc-range 2.*.* result action-set allowed-ver
  pc-range 3.3.6 result action-set allowed-ver

! Define the gateway linkset table entry for linkset dallas
cs7 in 0 gws linkset name dallas
  inbound result table allowed-dpc-1

```

```

! Define the gateway linkset table default entry
cs7 in 0 gws linkset default
    inbound result action-set blocked-ver
cs7 in 0 gws linkset default
    outbound result action-set blocked-ver

```

GWS Scenario: XUA AS with Allowed DPC

In this usage scenario, an allowed DPC table is created. The DPC table is linked to an AS.

```

cs7 multi-instance
cs7 instance 0 variant ITU
cs7 instance 0 network-name INST0
cs7 instance 0 point-code 1.1.2
cs7 instance 1 variant ITU
cs7 instance 1 network-name INST1
cs7 instance 1 point-code 1.1.3
cs7 accounting global-mtp3
!
cs7 m3ua 2907
    local-ip 172.18.10.47
!
cs7 asp ASP1 2907 2907 m3ua
    remote-ip 172.18.10.52
!
cs7 instance 0 as AS1 m3ua
    routing-key 1 1.1.4
    asp ASP1
!

! Define action set for allowed verbose and blocked verbose
cs7 instance 0 gws action-set allowed-ver allow
cs7 instance 0 gws action-set blocked-ver block

! Define the allowed DPC table
! Define PC range
cs7 in 0 gws table allowed-dpc-1 type dpc action allowed
    default result action-set blocked-ver
    pc-range 1.1.4 1.1.6 result action-set allowed-ver
    pc-range 3.3.2 3.3.* result action-set blocked-ver

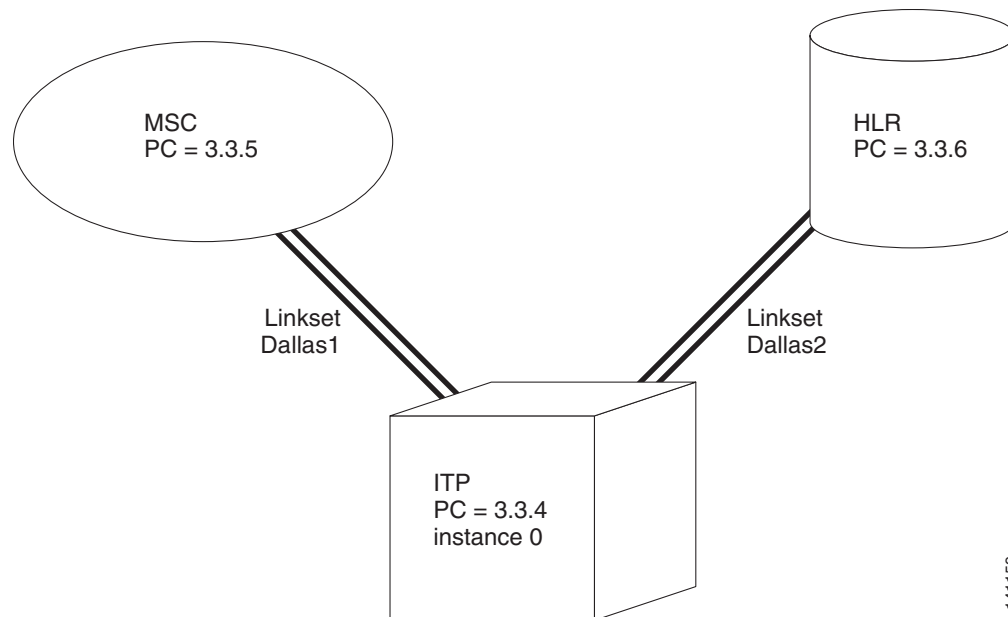
! Define the gateway AS table entry for M3UA AS AS1
cs7 in 0 gws as name AS1
    inbound m3ua result table allowed-dpc-1

! Define the gateway AS table default entry
cs7 in 0 gws as default
    inbound result action-set blocked-ver
cs7 in 0 gws as default
    outbound result action-set blocked-ver

```

GWS Scenario with CgPA, CdPA

In this usage scenario, a linkset is tied to an allowed DPC table, an allowed CgPA PC-SSN table, allowed CgPA SCCP selector, allowed SCCP message header and allowed CdPA PC-SSN tables.

Figure 29 GWS Scenario with CgPA, CdPA

141159

```

cs7 multi-instance
cs7 instance 0 variant ITU
cs7 instance 0 network-name INST0
cs7 instance 0 point-code 3.3.4
cs7 instance 1 variant ITU
cs7 instance 1 network-name INST1
cs7 instance 1 point-code 3.3.7

controller E1 0/0
  clock source line primary
  channel-group 0 timeslots 1
!
controller E1 0/1
  channel-group 0 timeslots 1
...

cs7 instance 0 linkset dallas1 3.3.5
  accounting
! define links

cs7 instance 0 linkset dallas2 3.3.6
  accounting
! define links

cs7 instance 0 route-table
cs7 instance 1 route-table

! Define action set for allowed verbose and blocked verbose
cs7 instance 0 gws action-set allowed-ver allow
cs7 instance 0 gws action-set blocked-ver block

! Define the allowed CdPA PC-SSN
cs7 in 0 gws table allowed-cdpa-pc-ssn-1 type cdpa-pc-ssn action allowed
  default result action-set blocked-ver
  pc-range 3.3.6 ssn 6 result action-set allowed-ver
  pc-range 4.4.* 4.*.* ssn 8 result action-set allowed-ver

```

```

! Define the allowed SCCP message header
cs7 in 0 gws table allowed-sccp-msg-hdr-1 type sccp-msg-hdr action allowed
default result action-set blocked-ver
sccp-msg xudt result table allowed-cdpa-pc-ssn-1
sccp-msg xudts result table allowed-cdpa-pc-ssn-1

! Define the allowed CgPA PC-SSN table
cs7 in 0 gws table allowed-cgpa-pc-ssn-1 type cgpa-pc-ssn action allowed
default result action-set blocked-ver
pc-range 3.3.5 ssn 8 result table allowed-sccp-msg-hdr-1

! Define the allowed SIO table
cs7 in 0 gws table allowed-sio-1 type sio action allowed
default result action-set blocked-ver
si sccp result table allowed-cgpa-pc-ssn-1

! Define the allowed OPC table
cs7 in 0 gws table allowed-opc-1 type opc action allowed
default result action-set blocked-ver
pc-range 3.3.5 result table allowed-sio-1

! Define the gateway linkset table entry for linkset dallas1
cs7 in 0 gws linkset name dallas1
inbound result table allowed-opc-1

! Define the gateway linkset table default entry
cs7 in 0 gws linkset default
inbound result action-set blocked-ver
cs7 in 0 gws linkset default
outbound result action-set blocked-ver

```

Additional References

The following sections provide references related to the GWS feature.

Standards

Standard	Title
ANSI T1.111	<i>1996 Signaling System No. 7 - Message Transfer Part</i>
ANSI T1.112	<i>1996 Signaling System No. 7 - Signaling Connection Control Part</i>
ITU-T Q.704	<i>Specifications of Signaling System No. 7 - Message Transfer Part</i>
ITU-T Q.713	<i>Specifications of Signaling System No. 7 - Signaling Connection Control Part</i>
GR-82-CORE, Appendix C	<i>TelCordia Technologies Generic Requirements GR-82-CORE</i>



MLR Routing and Screening

The IP Transfer Point (ITP) Multi-Layer Routing (MLR) feature implements the routing of Short Message Service (SMS) messages based on information found in the Transaction Capability Application Part (TCAP), Mobile Application Part (MAP), and SMS layers.

Feature History for MLR

Release	Modification
12.2(33)IRA	This feature was introduced.
12.2(33)IRC	The congestion-mode defer-to-backup command was added.
12.2(33)IRE	The Packet Address Modification (PAM) feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



Note

Configuration Mode Restrictions: Simultaneous changes to the configuration from multiple CLI sessions are not supported. Only one configuration session is allowed to enter in configuration mode at a time; other sessions should not enter in configuration mode. The **show line** or **show users EXEC** command may be used to determine the active user sessions on an ITP, and the **clear line EXEC** command may be used to ensure that only a single active session exists.

Contents

- [How to Configure MLR-Based Routing, page 205](#)
- [How to Configure MLR-Based Screening, page 244](#)
- [Verifying and Monitoring MLR Routing, page 247](#)
- [Configuration Examples of MLR, page 249](#)
- [How to Configure Packet Address Modification \(PAM\), page 259](#)
- [Configuration Examples of PAM, page 264](#)

Information About MLR Routing and Screening

Short Message Service (SMS) applications such as audience interaction services place a heavy demand on the capacity of the legacy SS7 infrastructure, as well as the SMSC servers. These applications create extremely high bursts of signaling traffic over a very short time span, which can result in denial of service and lost messages.

The ITP MLR feature enables intelligent routing of SMS messages based on the application or service from which they originated or to which they are destined. The MLR feature can make SMS message routing decisions based on information found in the TCAP, MAP, and MAP-user layers. MAP operation include all GSM-MAP (3GPP TS 29.002 version 5.9.0 Release 5) operations in MLR rules.

The valid operation-name specifications are presented in the CLI depending on the specified protocol and are listed in tables in the [“Define One or More MLR Rulesets” section on page 224](#).

For ITU TCAP and GSM-MAP, MLR supports routing on the following operations (See [Table 20](#)):

- MAP-MO-FORWARD-SM
- MAP-MT-FORWARD-SM
- SEND-ROUTING-INFO-FOR-SM
- MAP-ALERT-SERVICE-CENTRE

For ANSI TCAP and IS-41 MAP, MLR incorporates Mobile Directory Number (MDN) based SMS routing and supports routing on the following operations:

- Smdpp
- SmsRequest
- SmsNotify

ITP MLR-based screening enables the blocking of incoming SS7 traffic based on the originating SCCP cgPa and SCCP cdPa destination, including the global title address (gta). MLR screening also enables blocking on the basis of SCCP cdPa global title digits and all GSM operations. This allows the blocking of short message transactions from a specific originating global title.

Trigger Search Order

It is possible that a message may match to more than one primary trigger since a primary trigger can be either cdPa or cgPa based. cdPa matches are attempted before cgPa matches. The lookup mechanism for GT-based primary triggers is the GTT table, while the lookup mechanism for PC/SSN based primary triggers is the GTT MAP table. Once a primary trigger is matched, the secondary triggers are searched sequentially in the order defined until a match is found.

[Table 17](#) describes the Multi-layer routing trigger types and their function.

Table 17 **Multi-Layer Routing Trigger Types**

Trigger Type	Function
SCCP Global Title	The received packets arrive into SCCP with RI=GT and a specific range of global titles. The primary routing trigger for SMS MO traffic is the cdPa destination SMSC E.164 address. The originating MSC address, which is found in the cgPa, may also be used as a routing trigger.
SCCP Point Code and SSN	The received packets arrive into SCCP with RI=PC/SSN. For example, SMS MO traffic for which the MSC/STP has performed final GTT will arrive destined for the ITP PC and SMSC SSN.
Global Configuration	All traffic received will be checked for MLR, provided that a routing table is defined.
Combination Triggers	A combination of two mutually exclusive SCCP cdPa and cgPa trigger types may be specified to form a trigger match. This allows packets destined to the same SMSC from different MSCs to be handled by different routing tables.

Destination Selection

A match in the multi-layer routing table will map to one of the following:

- A single point-code.
- An M3UA or SUA application server name. Upon selection, the message is routed to the AS which may be composed of multiple ASPs.
- A multi-layer result group. This table will provide the set of possible results along with the associated algorithm used to select among the results. This table is independent of the global title translation function, but uses PC and SSN state to route to available destinations.
- A global title address. Upon selection, the SCCP global title translation function will be invoked for the specified address. This address may then map to an application group consisting of multiple destinations.

How to Configure MLR-Based Routing

To enable the MLR feature, perform the configuration tasks described in the following sections:

- [Define MLR Global Options, page 206](#)
- [Define the MLR Group, page 207](#)
- [Defining the MLR Modify-Profile, page 211](#)
- (optional) [Creating and Managing Address Tables, page 214](#)
- [Define One or More MLR Rulesets, page 224](#)
- [Define the MLR Triggers, page 240](#)

**Note**

Whenever the MLR configuration is changed, verify the output of the **show cs7 offload mtp3** command on the SUP to ensure the MLR configuration is in a *sync* state for the linecard.

Define MLR Global Options

You can define an MLR option globally per instance so that it can be applied to all MLR routed results, including trigger results, rule results, and address-table results.

When the **insert-dpc-in-cdpa** option is configured, MLR can modify the cdpa pc and the calling party (cgpa) pc of an MSU. The cdpa pc is updated for MLR results of point code (pc), point code and subsystem number (pcssn), global title (gt), and asname. This option does not apply to the MLR results **block** or **continue**.

Preserving the original destination point code (dpc) in the cdpa is not possible with an MLR GT result. The SCCP always overwrites the cdpa pc with the new GT translated dpc.

When the **preserve-opc** function is configured within the global MLR options submode, the original Originating Point Code (OPC) is retained. You can configure this feature globally, or within an MLR ruleset.

modify-failure allows you to specify which action you want to take when an MLR packet cannot be modified. By default, the packet is discarded. MLR modification failures include exceeding the maximum MSU or address size when inserting new data, failures when attempting to modify the destination GT, and failures when executing a modify-profile.

The following steps specify how to add MLR options that are applied to all MLR result types.

SUMMARY STEPS

-
Step 1	enable
Step 2	configure terminal
Step 3	cs7 [instance <i>instance-number</i>] mlr options
Step 4	insert-dpc-in-cdpa
Step 5	preserve-opc
Step 6	modify-failure {discard resume sccp-error <i>sccp-error</i>}
Step 7	disable-mlr
-

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: ITP> enable	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	configure {terminal memory network} Example: ITP# configure terminal	Enters global configuration mode.
Step 3	cs7 [instance instance-number] mlr options Example: ITP(config)# cs7 instance 1 mlr options	(Optional) Specifies an MLR result option command and enables the CS7 MLR options configuration mode.
Step 4	insert-dpc-in-cdpa Example: ITP(cfg-cs7-mlr-options)# insert-dpc-in-cdpa	(Optional) Specifies that when a packet is MLR routed, the MTP dpc is inserted into the cdpa pc if the cdpa pc is null.
Step 5	preserve-opc Example: ITP(cfg-cs7-mlr-options)# preserve-opc	(Optional) Preserves the original originating point code (OPC) when an MLR result is selected in this instance.
Step 6	modify-failure {discard resume sccp-error sccp-error} Example: ITP(cfg-cs7-mlr-options)# modify-failure resume	(Optional) modify-failure indicates the action to take when an MLR packet modification fails. Options include: discard —discard the packet (default). resume —resume sending original packet to original destination. sccp-error —send a UDTS to the originator with the configured sccp error code, if return-on-error was set in the UDT.
Step 7	disable-mlr Example: ITP(cfg-cs7-mlr-options)# disable-mlr	(Optional) Disables all MLR routing for the specified instance.

Define the MLR Group

A multi-layer result group is a group of destination resources to process traffic that will be routed based on multi-layer information. The result group lists the appropriate destination resources and the mechanism used to select a single destination for a given packet. State information is determined for each possible destination. Only available destination are considered for routing. Note, however, that the distribution algorithms consider GT results as always available. Ensure that the proper GT configuration is in place and available for GT routing.

The MLR feature provides two result group distributions modes: weighted round-robin and dynamic B-address binding.

The **weighted round-robin** (WRR) distribution algorithm properly balances SMS workload to servers of varying capacity. Each server within a result group (application group or multi-layer result table) is assigned a server weight from 0 to 10. The value of 0 indicates that the server is a backup, and should only be used when all of the servers in the group with a non-zero weight have failed. By default congested resources are used only when all non-zero weighted servers are congested. Instead of relying only on unavailability to trigger the use of a backup server, the **congestion-mode defer-to-backup** command in CS7 mlr result configuration mode sets congestion as an additional trigger for the use of a backup server.

Dynamic B-address binding uses a hashing algorithm based on the message's B-address to determine which result (SMSC) a message is to be routed to for delivery. The algorithm will select the same result (SMSC) each time based on the B-address to prevent out-of-order messaging. SMSCs with greater capacity are configured as such using the result's weight parameter. The results (SMSCs) are inserted into the result group using the order parameter. If an unplanned SMSC outage occurs (in other words, if a result is unavailable), then these messages destined for the unavailable SMSC are rerouted to the remaining SMSCs. Note that an SMSC outage does not affect the mapping for available SMSCs. This algorithm handles routing of alphanumeric B-addresses, as well as numeric B-addresses.

SMS MO Proxy sms-mo messages can use MLR result groups with WRR or dest-sme-binding modes. This simplifies configuration since both SMS MO Proxy and MLR dest-sme-binding result groups must be identically configured in an SMS MO Proxy solution. To use dest-sme-binding, you must configure a ruleset.

To define the Multi-layer result group, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cs7** [*instance instance-number*] **mlr result** *name* [**protocol** {*gsm-map* | *ansi41*}] [**mode** {*wrr* | *dest-sme-binding*}]
4. **asname** *as-name* [**order** *order*] [**weight** *weight*]
5. **gt** *addr-string* [**tt** *tt* [**gti** *gti*] [**np** *np* [**nai** *nai*]]] [**order** *order*] [**weight** *weight*]
6. **congestion-mode defer-to-backup**
7. **pc** *dest-pc* [**ssn** *ssn*] [**order** *order*] [**weight** *weight*]
8. **unavailable-routing** {*discard* | *resume*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: ITP> enable	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	configure { terminal memory network } Example: ITP# configure terminal	Enters global configuration mode.
Step 3	cs7 [instance <i>instance-number</i>] mlr result <i>name</i> [protocol { gsm-map ansi41 }] [mode { wrr dest-sme-binding }] Example: ITP(config)# cs7 mlr result VAS-GRP	Specifies an MLR result group command and enables the MLR results configuration mode.
Step 4	asname <i>as-name</i> [order <i>order</i>] [weight <i>weight</i>] Example: ITP(cfg-cs7-mlr-result)# asname VOTING-AS1 weight 1	Specifies a particular destination M3UA or SUA application server. The application server should already be defined, and its state is extracted from the SUA or M3UA routing layer for availability purposes. • order <i>order</i> Required for (and present only in the CLI for) dest-sme-binding mode. Specifies the order in which the results are stored in the result group. An integer value in the range of 1 to 1000. • weight <i>weight</i> Specify load balancing weight. For dest-sme-binding mode, an integer value in the range 1 to 2147483647. Default is 1. For wrr mode, an integer value in the range of 0 to 10. Default is 1.

	Command or Action	Purpose
Step 5	gt <i>addr-string</i> [tt <i>tt</i> [gti <i>gti</i>] [np <i>np</i> nai <i>nai</i>]] [order <i>order</i>] [weight <i>weight</i>] Example: <pre>ITP(cfg-cs7-mlr-result)# gt 9991234 tt 0 gti 4 np 1 nai 4 weight 1</pre>	Specifies an outbound global title destination from within a result group. • tt <i>tt</i> Identifies a translation type specified within the address. Integer in the range 0 through 255. • gti <i>gti</i> Identifies the global title indicator for the specified address. This value is only specified when the variant is ITU or China. Integer value of 2 or 4. • np <i>np</i> Identifies the numbering plan of the specified address. Only configured when the gti parameter value is 4. Integer in the range 0 to 15. • nai <i>nai</i> Identifies the nature of the specified address. Configured only when the gti parameter value is 4. Integer in the range 0 through 127. • order <i>order</i> Required for (and only present in the CLI for) dest-sme-binding mode. Specifies the order in which the results are stored in the result group. An integer value in the range of 1 to 1000. • weight <i>weight</i> Specify load balancing weight. For dest-sme-binding mode, an integer value in the range 1 to 2147483647. Default is 1. For wr mode, an integer value in the range of 0 to 10. Default is 1.
Step 6	congestion-mode defer-to-backup Example: <pre>ITP(cfg-cs7-mlr-result)# congestion-mode defer-to-backup</pre>	Sets congestion as an additional trigger for the use of a backup server instead of relying only on unavailability to trigger the use of a backup server.  Note A server weight of 0 indicates that the server is a backup.

	Command or Action	Purpose
Step 7	[instance <i>instance</i>] pc <i>dest-pc</i> [ssn <i>ssn</i>] [order <i>order</i>] [weight <i>weight</i>] Example: ITP(cfg-cs7-mlr-result)# pc 3.3.1 weight 0	Specifies a destination point code. The specified point code must represent a real point code, not an alias point code. The destination point code must exist in the MTP3 routing table; its state is extracted from MTP3 for availability purposes. • instance Indicates the PC/PCSSN result in local or other instance. • instance Instance number. The valid range is 0 through 7. The default instance is 0. • order <i>order</i> Required for (and only present in the CLI for) dest-sme-binding mode. Specifies the order in which the results are stored in the result group. An integer value in the range of 1 to 1000. • weight <i>weight</i> Specify load balancing weight. For dest-sme-binding mode, an integer value in the range 1 to 2147483647. Default is 1. For wrp mode, an integer value in the range of 0 to 10. Default is 1.
Step 8	unavailable-routing {discard resume} Example: ITP(cfg-cs7-mlr-result)# unavailable-routing resume	Specifies the routing of a packet when no members are available. • discard Discard packet (default) • resume Resume sending packet to original destination.

Defining the MLR Modify-Profile

SCCP and MAP address modification is permitted using a MLR modify-profile. For each modify profile, you must configure a unique profile name, the protocol, and the operation name. Multiple profiles can be created for each instance. Only one profile may be specified within a rule. Within a modify profile, you can specify SCCP and MAP addresses to modify. MLR currently supports modifying only the service center address (orig-smsc) and the calling party address (CgPA) for SRI-SM messages.

For the orig-smsc, you can modify the address digits, the type of number (ton), and the numbering plan (np).

For cgpa, MLR supports inserting a point code (PC) and subsystem number (SSN), as well as modifying the existing GT information, PC, and SSN. The CgPA routing indicator (RI) is unchanged during these modifications. The PC and the SSN may be inserted or modified, regardless of the RI. GT modifications, however, apply only to packets with RI=GT. If GT modifications are configured and the received packet has a CgPA with RI=SSN, then the GT modifications are simply ignored. The GT information which can be modified includes the GT address digits, the GT translation type (tt), the global title indicator (gti), the numbering plan (np), and the nature of address indicator (nai).

You can configure prefix-based address modification or a replacement address. For prefix-based address translation, you configure the number of prefix digits that will be removed from the address and the digit string that should be prefixed to the address. Specifying a "*" for number of prefix digits indicates that

no prefix digits to be removed. Specifying a “*” for the digit string indicates that no prefix digits are prefixed to the address string. To replace the entire address, the user should specify the maximum value for the number of prefix digits to remove. If the resulting modified address exceeds the maximum allowed number of digits, then MLR will fail the modification and discard the packet by default. The user can optionally configure the desired action for failed modifications using the modify-failure command within the MLR options submode.

The modify profile is assigned to a rule using the modify-profile rule parameter. If an MLR rule matches, then the modify profile is applied to messages which are MLR routed. Address translation is only performed if the matched rule contains a modify-profile.

To define an MLR modify profile, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cs7 mlr modify-profile** *profile-name* *protocol* *operation-name*
4. **orig-smsc** [**prefix** {*prefix-remove-num* | *}] {*prefix-add-digits* | *}] [**ton** *new-ton*] [**np** *new-np*]
5. **cgpa** [**gt** [**prefix** {*prefix-remove-num* | *}] {*prefix-add-digits* | *}] [**tt** *tt*] [**gti** {**2** | **4** **np** *np* **nai** *nai*}] [**pc** *pc*] [**ssn** *ssn*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: ITP> enable	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	configure { terminal memory network } Example: ITP# configure terminal	Enters global configuration mode.
Step 3	cs7 mlr modify-profile <i>profile-name</i> <i>protocol</i> <i>operation-name</i> Example: ITP(config)# cs7 mlr modify-profile SRISM gsm-map sri-sm	Defines SCCP and MAP addresses to modify in MLR routed messages. • <i>profile-name</i> identifies a name to be associated with a defined MLR modify-profile. • <i>protocol</i> Specifies an application layer protocol filter. • <i>operation-name</i> Specifies the operation for which the modify profile is valid. MLR only allows you to define a modify-profile for a sri-sm operation. Note You can create multiple modify profiles for each instance but can specify only one profile within a rule.

	Command or Action	Purpose
Step 4	orig-smsc [prefix {<i>prefix-remove-num</i> *}{<i>prefix-add-digits</i> *}] [ton <i>new-ton</i>] [np <i>new-np</i>] Example: ITP(cfg-cs7-mlr-modify)# orig-smsc prefix 2 351	Specifies the originating service center address. • prefix—specifies that the prefix modification will be performed on the address. • <i>prefix-remove-num</i>—an integer in the range of 1 to 38 which defines the number of prefix digits to remove from the address. If no prefix digits are to be removed, then you should specify “*”. • <i>prefix-add-digits</i>—a string of 1 to 38 hexadecimal digits which are added to the beginning of the address. If no digits are added, then you should specify “*”. If the number of digits in the modified address exceeds 38 digits, then the address modification cannot be performed. In this failure case, the action taken is based on the configured modify-failure parameter. By default, the packet is discarded. • ton—indicates a type of number (ton) replacement. • <i>new-ton</i>—an integer in the range of 0 to 7 which defines the new type of number (ton) value for the modified address. • np—indicates a numbering plan (np) replacement. • <i>new-np</i>—an integer in the range of 0 to 15 that defines the new numbering plan (NP) value for the modified address.

Command or Action	Purpose
Step 5 <pre>cgpa [gt [prefix {prefix-remove-num *}{prefix-add-digits *}]] [tt tt] [gti {2 4 np np nai nai}]] [pc pc] [ssn ssn]</pre> Example: <pre>ITP(cfg-cs7-mlr-modify)# cgpa gt prefix 2 351</pre>	Indicates that the SCCP calling party address (CgPA) needs modification. The CgPA routing indicator (RI) does not change during these modifications. gt—indicates global title information to modify. GT modifications apply only to packets with RI=GT. If GT modifications are configured and the received packet has a CgPA with RI=SSN, then the GT modifications are ignored. prefix—specifies that the prefix modification performs on the address. prefix-remove-num—an integer in the range of 1 to 15 that defines the number of prefix digits to remove from the address. If no prefix digits are removed, then * should be specified. prefix-add-digits—identifies a string of 1 to 15 hexadecimal digits added to the beginning of the address. The string is input in normal form (not BCD-string format). If no digits are added, then specify * in this field. If the number of digits in the modified address exceeds the 31 digits, then the modified address truncates to 31 digits. If the number of digits in the modified address is less than 1 digit, then the address modification fails, and the configured modify-failure parameter action takes place. The default modify-failure parameter action is to discard the packet. tt —indicates the global title translation type (tt) for the modified CgPA. <i>tt</i> is an integer from 0 to 255 which will replace the existing tt value in the CgPA. gti—identifies the global title indicator value for the modified CgPA. This value is only specified when the CS7 variant is ITU or China. <i>gti</i> is an integer value of 2 or 4. np—identifies the global title numbering plan for the modified CgPA. <i>np</i> is an integer value from 0 to 15. nai—identifies the global title nature of address indicator for the modified CgPA. Only specified when the gti parameter value is 4. <i>nai</i> is an integer value from 0 to 127. pc—identifies the point code for the modified CgPA. <i>pc</i> is the point code in variant-specific point-code format. ssn—identifies the subsystem number for the modified CgPA. <i>ssn</i> is the subsystem number in decimal format. Valid range is 2 to 255.

Creating and Managing Address Tables

This section discusses the configuration, storage, and retrieval of address lists that can block or route SMS messages.

MLR address tables can be stored in either NVRAM on the IOS platform or in a file that typically would be stored in flash. NVRAM limitations on some platforms might restrict the number of address entries that can be stored there. In this case, the file storage option is recommended.

This section includes 3 tasks:

- [Creating and Loading an Address Table File Using the CLI, page 215](#)
- [Creating and Loading a Stored Address Table File, page 218](#)
- [Replacing an Address Table File, page 219](#)
- [Saving an MLR Configuration to a File, page 221](#)
- [Loading an MLR Configuration from a File, page 221](#)
- [Replacing a Running MLR Configuration with a File, page 222](#)
- [Validating and Auditing the Consistency of the MLR Files in the Line Card and Main Processor, page 223](#)

Creating and Loading an Address Table File Using the CLI

In this task you use the CLI to configure address table entries that you plan to save to an external file. You then specify a location from which you will load the file of address table entries upon reboot. Finally you save the address entries to an external file.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cs7 mlr address-table *table-name***
4. **addr *address-name* [exact] [result {*asname asname* | *block* | *continue* | *group group-name* | *gt addr-string* [tt tt gti {2 | 4 np np nai nai}] | [instance *instance-number*] pc *pc* [ssn *ssn*] | [sccp-error *error*]}]**
5. **load *URL***
6. **exit**
7. **cs7 save address-table mlr *table-name url***

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables higher privilege levels, such as privileged EXEC mode.
	Example: ITP> enable	Enter your password if prompted.
Step 2	configure {terminal memory network}	Enters global configuration mode.
	Example: ITP# configure terminal	

	Command or Action	Purpose
Step 3	<pre>cs7 mlr address-table tablename</pre> Example: <pre>ITP(config)# cs7 mlr address-table addrtbl1</pre>	Identifies the name of the address table. This name is used to identify the address table from within MLR ruleset commands. Enables CS7 MLR address table configuration mode.
Step 4	<pre>addr address-name [exact] [result {asname asname block continue group group-name gt addr-string [tt tt gti {2 4 np np nai nai}] [instance instance-number] pc pc [ssn ssn] [sccp-error error]}]</pre> <pre>ITP(cfg-cs7-mlr-addr-table)# addr 1111 exact result group grp1</pre> <pre>ITP(cfg-cs7-mlr-addr-table)# addr 1800 result gt 12341234 tt 11 gti 4 np 1 nai 2</pre>	Specifies an MLR address within the MLR address table. <i>address-name</i> of 1 to 20 hexadecimal digits. exact specifies that the configured address must exactly match. result indicates that the address will be handled by the chosen option. Note If a rule contains multiple table-based parameters (such as dest-sme-table, orig-sme-table, or orig-imsi-table), then any result configured on an addr entry of an address-table is ignored. asname <i>asname</i> routes messages to the named AS. block indicates the rejection of the message. An option to return UDTs with the configured sccp-error is provided, if the received UDT has the return-on-error option set. continue indicates that message processing will continue. group <i>group-name</i> indicates that the message will be routed according to a named result-group. gt <i>addr-string</i> indicates a global title result and address. tt <i>tt</i> specifies a translation type in the range 0 to 255. gti {2 4} specifies a global title indicator. (2 is primarily used in the ANSI domain; 4 in the ITU domain.) np <i>np</i> specifies a numbering plan value in the range 0 to 15. nai <i>nai</i> specifies a nature of address indicator in the range 0 to 127. instance <i>instance</i> indicates the PC/PCSSN result in local or other instance. The valid range is 0 through 7. The default instance is 0. pc <i>dest-pc</i> indicates that the message will be routed according to a specified point code. ssn <i>ssn</i> indicates an ssn associated with the point code. sccp-error <i>error</i> configures block results that will support configuring a sccp-error on the block result.

	Command or Action	Purpose
Step 5	load <i>URL</i> Example: ITP(cfg-cs7-mlr-addr-table)# load disk0:mlraddrtbl	(Optional) Specifies an address table file to load at startup. • bootflash: URL to load • cs7: URL to load • disk0: URL to load • disk1: URL to load • flash: URL to load • ftp: URL to load • null: URL to load • nvram: URL to load • rcv: URL to load • slavebootflash: URL to load • slavecdfs: URL to load • slavedisk0: URL to load • slavedisk1: URL to load • slavenvram: URL to load • slavercsf: URL to load • slaveslot0: URL to load • slaveslot1: URL to load • slot0: URL to load • slot1: URL to load • system: URL to load • tftp: URL to load
Step 6	exit Example: ITP(cfg-cs7-mlr-addr-table)# exit	Exit to global configuration mode.
Step 7	cs7 save address-table mlr <i>tablename url</i> Example: ITP#cs7 save address-table mlr addrtbl1 disk0:mlraddrtbl	Saves the address table to an external location and file (url). Valid URLs are bootflash, disk0, disk1, disk2, slot0, slot1, tftp, flash, sup-bootdisk, sup-bootflash, rcv.

Creating and Loading a Stored Address Table File

Address tables are typically created and stored to a file using the ITP CLI. However, advanced users can also create address tables externally and then load the created address table file into the ITP. This option may be useful for integrated tooling.

To create and load a stored address table, perform the following steps.

SUMMARY STEPS

- 1. Create a file of addresses following the format and syntax described in the above tables.
- 2. **enable**
- 3. **configure terminal**
- 4. **cs7 mlr address-table *tablename***
- 5. **load *URL***

DETAILED STEPS

	Command or Action	Purpose
Step 1	Create a file of addresses, following the format and syntax described in Tables 1 - 4.	
Step 2	enable Example: ITP> enable	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 3	configure {terminal memory network} Example: ITP# configure terminal	Enters global configuration mode.

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables higher privilege levels, such as privileged EXEC mode.
	Example: ITP> enable	Enter your password if prompted.
Step 2	cs7 address-table replace mlr <i>tablename url</i>	Replaces an existing address table with one specified in a URL.
	Example: ITP# cs7 address-table replace mlr addrtbl1 disk0:mlraddrtbl	Valid URLs are bootflash, disk0, disk1, disk2, slot0, slot1, tftp, flash, sup-bootdisk, sup-bootflash, rcp.

Examples

The following example shows three address tables. Two of the address tables are loaded from stored files at startup. The third address table and the addresses in the table are configured from within the configuration.

```
cs7 mlr address-table imsi-screen
load disk0:imsi-screen
!
cs7 mlr address-table orig-screen
load disk0:orig-screen
!
cs7 mlr address-table shortcodes
addr 11112 result group grp2
addr 1111 result group grp1
addr 2222 result group grp1
addr 5551212 exact result group grp3
```

Saving an MLR Configuration to a File

You can save a general MLR configuration file to a local or remote file system. The MLR configuration for each CS7 instance will be saved to a separate file. By default, the file format text of general MLR configuration can be obtained from files under `cs7:/mlr-config/`.

Cisco IOS CLI modifications to MLR configurations may take up to 15 seconds to take effect on all linecards after the last change is made. The standard Cisco IOS CLI command `copy running-config startup-config` or `write memory`, which saves the running configuration, does not automatically save the MLR configuration. The user needs to save this MLR information manually. The saved provisioning will load during a Cisco ITP restart or reload.

To save this MLR information manually use the following procedure:

SUMMARY STEPS

1. **enable**
2. **cs7** [*instance-number*] **save mlr** [**all**] *url*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: ITP> enable	Enables privileged EXEC mode.
Step 2	cs7 [<i>instance-number</i>] save mlr [all] <i>url</i> Example: itp# cs7 save mlr all disk0:mlr-config	Saves a general MLR configuration to a separate file. Valid URLs are bootflash, disk0, disk1, disk2, slot0, slot1, tftp, flash, sup-bootdisk, sup-bootflash, rcp. Note If the save operation fails, the system generates an error message with the cause of the problem, which can be insufficient resources.

Loading an MLR Configuration from a File

You can configure Cisco ITP to load the whole MLR configuration including general MLR configuration and address tables. The load command does not initiate the restart or reload needed to trigger the actual load operation. It configures the load operation to occur when a restart or reload occurs. Cisco IOS CLI configuration is not allowed during file loading or replacement. If the MLR loading operation occurs before system configuration, it will wait until the system configuration finish.

Configure Cisco ITP to load an MLR configuration from a local or remote file with the following procedure:



Note

Loading and replacement of MLR configuration files may take up to 15 seconds to take effect on all linecards after the last change is made. The user is notified of completion through a console message.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cs7** [*instance instance-number*] **mlr load url**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: ITP> enable	Enables privileged EXEC mode.
Step 2	configure terminal Example: ITP# configure terminal	Enters global configuration mode.
Step 3	cs7 [<i>instance instance-number</i>] mlr load url Example: itp(config)#cs7 mlr load disk0:mlr-config	Loads an MLR configuration file from a specified remote or local file during a Cisco ITP restart or reload. Valid URLs are bootflash, disk0, disk1, disk2, slot0, slot1, tftp, flash, sup-bootdisk, sup-bootflash, rcp.  Caution Specifying a remote file for the load command is not recommended as a best practice for high availability deployments, such as the Cisco 7600. Note If the load operation fails, the system generates an error message with the cause of the problem. Syntax errors in the loaded file cause the load operation to fail.

Replacing a Running MLR Configuration with a File

This procedure replaces the running MLR configurations. It replaces the entire MLR configuration, including general MLR configuration and MLR address tables. Cisco ITP maintains a new configuration and an old configuration and uses the old configuration until the new configuration loads completely with no problems. Configuration file replacement does not take place until all entries in the new file have been read and validated.

Cisco IOS CLI modifications to MLR configurations may take up to 15 seconds to take effect on all linecards after the last change is made. The user is notified of completion through a console message. Cisco IOS CLI configuration is not allowed during file loading or replacement.

To accomplish this, complete the following procedure:

SUMMARY STEPS

1. **enable**

2. `cs7 [instance instance-number] mlr replace url`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: itp> enable	Enables privileged EXEC mode.
Step 2	cs7 [instance-number] mlr replace url Example: itp# cs7 mlr replace disk0:mlr-config	(Optional) Replaces the running MLR configuration with the configuration file specified by the URL. Valid URLs are bootflash, disk0, disk1, disk2, slot0, slot1, tftp, flash, sup-bootdisk, sup-bootflash, rcp.

Validating and Auditing the Consistency of the MLR Files in the Line Card and Main Processor

This procedure validates and audits the consistency of the MLR configuration files and MLR address table files contained in the line card and main processor. These files should sync from the line card to the main processor when the configuration of the MLR files change in the main processor. If the procedure recognizes inconsistencies between the the MLR files in the line card and main processor, a second sync takes place. Configure Cisco ITP to validate and audit the consistency of the MLR configuration files and MLR address table files contained in the line card and main processor with the following procedure:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cs7 audit [timer *timer-minutes*] [mlr *sync*]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: ITP> enable	Enables privileged EXEC mode.
Step 2	configure terminal Example: ITP# configure terminal	Enters global configuration mode.
Step 3	cs7 audit [timer [timer-minutes]] [mlr] Example: itp(config)#cs7 audit mlr	Validates and audits the consistency of the MLR configuration files and MLR address table files contained in the line card and main processor.  Note To see the latest audit begin time, end time, and status, use the <code>show</code> command.

Define One or More MLR Rulesets

With this task you specify sets of rules for processing traffic that matches triggers defined in the MLR routing table.

MLR/SMS rule-matching implementations

If the address-table lookup finds a match and returns a result, it may only be used if no other routing parameters are defined on this rule. If more than one parameter is configured in a rule, then the result specified under the rule is used.

If an incoming message matches an SMS rule that references an MLR address-table, then any MLR address-table result is mapped to an SMS result:

- BLOCK, PC, and PCSSN results map easily from MLR to SMS.
 - For result groups, the MLR result group name is mapped to an SMS result group name.
 - If the SMS result group is not configured, then the result specified on the rule is used.
- AS and CONTINUE results are not valid in SMS. For these cases, the result specified on the rule is used. If no result is specified, the result on the rule is used (same as MLR).

If multiple rule parameters are configured for a rule, then the rule result will be used (rather than a result specified in the address table).

If the result type specified within the table is valid, it is used. Otherwise, the result in the rule is used.

For all tables, the ton and np must match before the table is accessed.

[Table 18](#) and [Table 19](#) list the GSM-MAP and GSM-MAP Version 1 operation names mapped to ITP operation names.

[Table 20](#) lists operations that allow you to route and screen based on MAP parameters and MAP-User parameters.

Valid operation-name specifications are presented in the CLI depending on the specified protocol.

Table 18 *GSM-MAP Operation Name Mapping to ITP CLI Operation Name*

Operation Name in GSM-MAP Specification	ITP CLI Operation Name	Opcode Value
activatess	actSS	12
activateTraceMode	actTraceMode	50
alertServiceCentre	alertSC	64
anyTimeInterrogation	anyTimeInterr	71
authenticationFailureReport	authFailRep	15
anyTimeModification	anyTimeMod	65
anyTimeSubscriptionInterrogation	anyTimeSubInterr	62
cancelLocation	cancelLoc	3
checkIMEI	checkIMEI	43
deactivateSS	deactSS	13
deactivateTraceMode	deactTraceMode	51
deleteSubscriberData	delSubData	8
eraseCC-Entry	eraseCCEntry	77
eraseSS	eraseSS	11
failureReport	failRep	25
forwardAccessSignalling	fwdAccessSig	34
forwardCheckSs-Indication	fwdCheckSsInd	38
forwardGroupCallSignalling	fwdGrpCallSig	42
mt-forwardSM	sms-mt	44
mo-forwardSM	sms-mo	46
getPassword	getPwd	18
informServiceCentre	informSC	63
insertSubscriberData	insSubData	7
interrogateSs	interrSS	14
istAlert	istAlert	87
istCommand	istCmd	88
noteMsPresentForGprs	noteMsPresentForGprs	26
noteSubscriberDataModified	noteSubDataMod	5
prepareGroupCall	prepGrpCall	39
prepareHandover	prepHandover	68
prepareSubsequentHandover	prepSubsHandover	69
processAccessSignalling	processAccessSig	33
processGroupCallSignalling	processGrpCallSig	41
processUnstructuredSS-Request	processUnstructSSReq	59
provideRoamingNumber	provideRoamNumber	4
provideSIWFSNumber	provideSIWFSNumber	31

Table 18 GSM-MAP Operation Name Mapping to ITP CLI Operation Name (continued)

Operation Name in GSM-MAP Specification	ITP CLI Operation Name	Opcode Value
provideSubscriberLocation	provideSubLoc	83
provideSubscriberInfo	provideSubInfo	70
purgeMS	purgeMS	67
readyForSM	readyForSM	66
registerCC-Entry	regCCEntry	76
registerPassword	regPwd	17
registerSS	regSS	10
remoteUserFree	remoteUserFree	75
reportSmDeliveryStatus	repSmDeliveryStatus	47
reset	reset	37
restoreData	restoreData	57
resumeCallHandling	resumeCallHandling	6
secureTransportClass1	secureTransClass1	78
secureTransportClass2	secureTransClass2	79
secureTransportClass3	secureTransClass3	80
secureTransportClass4	secureTransClass4	81
sendGroupCallEndSignal	sendGrpCallEndSig	40
sendEndSignal	sendEndSig	29
sendAuthenticationInfo	sendAuthInfo	56
sendIdentification	sendId	55
sendIMSI	sendIMSI	58
sendRoutingInfoForSM	sri-sm	45
sendRoutingInfoForGprs	sri-gprs	24
sendRoutingInfoForLCS	sri-lcs	85
sendRoutingInfo	sri-call (route a call to the MS)	22
setReportingState	setRepState	73
SIWFSSignallingModify	SIWFSSigMod	32
statusReport	statusRep	74
subscriberLocationReport	subLocRep	86
ss-Invocation-Notification	ssInvocNot	72
unstructuredSS-Request	networkUSSD	60, 61
unstructuredSS-Notify		
updateGprsLocation	updGprsLoc	23
updateLocation	updLoc	2
NoteMM-Event	noteMMEvent	89

Table 19 *GSM-MAP Version 1 Operation Code Mapping to ITP CLI Operation Name*

GSM-MAP Version 1 Operation Code	ITP CLI Operation Name	Opcode Value
AlertServiceCenterWithoutResult	alertScWoResult	49
allocateForHandoverNumber	allocHandOverNum	31
attachIMSI	attachIMSI	6
Authenticate	authenticate	39
BeginSubscriberActivity	beginSubActivity	54
CompleteCall	completeCall	23
ConnectToFollowingAddress	connectFollowAddress	24
detachIMSI	detachIMSI	5
forwardNewTMSI	fwdNewTMSI	41
forwardSSNotification	fwdSSNot	16
invokeSS	invokeSS	15
NoteInternalHandover	noteIntHandOver	35
NoteMSPresent	noteMSPresent	48
Page	page	26
PerformHandover	performHandOver	28
PerformSubsequentHandover	performSubHandOver	30
ProcessAccessRequest	processAccessReq	53
processCallWaiting	processCallWait	25
ProcessUnstructuredSS-Data	processUnstructSSData	19
provideIMSI	provideIMSI	40
RegisterChargingInformation	regChargingInfo	36
searchForMobileSubscriber	searchForMobileSub	27
sendHandOverReport	sendHandOverRep	32
SendInfoForIncomingCall	sendInfoForIncCall	20
SendInfoForOutgoingCall	sendInfoForOutgCall	21
SendParameters	sendParams	9
setCipheringMode	setCipherMode	42
SetMessageWaitingData	setMsgWaitData	47
TraceSubscriberActivity	traceSubAct	52
updateLocationArea	updateLocArea	1

MLR can route based on any GSM operation. The operations listed in [Table 20](#) allow you to route and screen based on MAP parameters and MAP-user parameters.

[Table 20](#) lists the parameters that are valid based on the specified **rule** operation.

Table 20 Valid Rule Parameters by Operation

	alertSc	all	smdpp	sms-mo	sms-mt	smsNot	smsReq	sri-sm	updLoc
dest-port				X	X				
dest-sme	X		X	X	X	X	X	X	
dest-sme-table			X	X					
dest-smsc	X			X					
match-unknown-ton-np	X		X	X	X	X	X	X	
allow-multi-message-dialogue		X		X	X				
orig-imsi				X					X
orig-imsi-table				X					X
orig-sme			X	X	X				
orig-sme-table			X	X					
orig-smsc					X			X	
pid				X	X				
teleservice			X			X	X		

To define a multi-layer SMS ruleset, perform the following steps.

SUMMARY STEPS

Steps 1 through 4 are required. Later steps are optional parameters, or input conditions, for the rule. Each rule and its input conditions must be completed by a result.

1. **enable**
2. **configure terminal**
3. **cs7** [*instance instance*] **mlr ruleset name** [*protocol {gsm-map | ansi-41}*]
4. **rule order** {*{gsm-map | ansi-41} operation-name [default] | all-operations*}
5. **allow-multi-message-dialogue**
6. **dest-port** *dest-port-number*
7. **dest-sme** {** | dest-addr*} [*dest-sme-addr-type*] [**exact**] | [**min-digits min**] | [**max-digits max**]
8. **dest-sme-table** *table-name*
9. **dest-smsc** {** | dest-addr*} [*addr-type*] [**exact**] | [**min-digits min**] | [**max-digits max**]
10. **match-unknown-ton-np**
11. **allow-multi-message-dialogue**
12. **orig-imsi** {** | imsi-address | unknown*} [**exact**] | [**min-digits min**] | [**max-digits max**]
13. **orig-imsi-table** *tablename* [**ton ton-value np np-value**]
14. **orig-sme** {** | orig-addr*} [*orig-sme-addr-type*] [**exact**] | [**min-digits min**] | [**max-digits max**]
15. **orig-sme-table** *tablename* [**ton ton-value np np-value**]
16. **orig-smsc** {** | orig-addr*} [*smc-addr-type*] [**exact**] | [**min-digits min**] | [**max-digits max**]
17. **pid** *protocol-id*

18. **preserve-opc**
19. **teleservice** *id*
20. **modify-profile** *profile-name*]
21. **result** {**gt** *addr-string* [*gt-addr-type*] | [**instance** *instance-number*] **pc** *dest_pc* [**ssn** *ssn*] | **asname** *as-name* | **group** *result-group* | **block** [**sccp-error** *error* | **map-error** {[**default** *ecdef* [*subdef*]] [**v1** *ec1* [*sub1*]] [**v2** *ec2* [*sub2*]] [**v3** *ec3* [*sub3*]] } | **continue** | **route**}

DETAILED STEPS

To define an MLR ruleset, perform the following steps, beginning in global configuration mode:

	Command or Action	Purpose
Step 1	enable	Enables higher privilege levels, such as privileged EXEC mode.
	Example: ITP> enable	Enter your password if prompted.
Step 2	configure { terminal memory network }	Enters global configuration mode.
	Example: ITP# configure terminal	

Command or Action	Purpose
Step 3 <pre>cs7 [instance instance-number] mlr ruleset name [protocol {gsm-map ansi-41}]</pre> Example: Router(config)#cs7 mlr ruleset MLR_RULES	Specifies an MLR ruleset and application layer protocol filter for the ruleset. • <i>name</i> Ruleset name. • protocol (Optional) Specifies an application layer protocol filter for this ruleset. The default behavior is that all operations may be specified within the ruleset. – gsm-map Uses GSM-MAP as application layer protocol filter within the ruleset. Only gsm-map operations may be specified within the ruleset. – ansi41 Uses ANSI-41 as application layer protocol filter within this ruleset. Only ansi41 operations may be specified within the ruleset. Configuring the cs7 mlr ruleset command enables CS7 MLR ruleset configuration mode.
Step 4 <pre>rule order {{gsm-map ansi-41} operation-name [default] all-operations}</pre> Example: ITP(cfg-cs7-mlr-set)# rule 5 gsm-map sms-mo	Specifies the rules within a Multi-layer ruleset table. Specifies the attributes of an application-layer message to be matched, and the resulting behavior for handling the message. At least one rule must be specified for the ruleset to be valid. Enables the MLR ruleset-rule configuration mode. • <i>order</i> Specifies the order in which rules are searched. • gsm-map Specifies the GSM MAP protocol. Protocol specification is required only if not specified in the cs7 mlr ruleset command. • ansi-41 Specifies the ANSI-41 protocol. Protocol specification is required only if not specified in the cs7 mlr ruleset command. • <i>operation-name</i> Specifies the operation for which the rule is valid. • default Specifies a match of any valid operation code. If you specify a protocol in MLR ruleset level, specifying all-operations in a rule applies only for that protocol. • all-operations Specifies the processing of messages that match the indicated operation name only. Configuring the rule command enables MLR ruleset-rule configuration mode in which you configure the input conditions of the rule.

	Command or Action	Purpose
Step 5	map-version <i><version number></i> Example: ITP(cfg-cs7-mlr-set-rule)# map-version 1 2	Filters specific versions of a gsm-map message. <i>version number</i> Specifies the specific MAP version used to filter the gsm-map messages. Valid range is 1 through 3.
Step 6	allow-multi-message-dialogue Example: ITP(cfg-cs7-mlr-set-rule)# allow-multi-message-dialogue	Specifies that all messages including multi-message dialogues match the rule. Only valid for default rules.
Step 7	dest-port <i>dest-port-number</i> Example: ITP(cfg-cs7-mlr-set-rule)# dest-port 100	Specifies the application destination port number. <i>dest-port-number</i> Specifies the destination port number. Valid range is 0 to 65535.

Step 8

Command or Action	Purpose
dest-sme { * <i>dest-address</i> } [<i>dest-sme-addr-type</i>] [exact] [min-digits <i>min</i>] [max-digits <i>max</i>]	Specifies the address of the destination short message entity (SME) within an SMS operation. This parameter is part of the rule used to match this route. • <i>dest-addr</i> Specifies the destination address. Valid range is 1 to 20 hexadecimal digits. • <i>dest-sme-addr-type</i> (Optional) Parameters that identify attributes of the SME address being used to match a rule. The address is composed of the following keywords: – [ton <i>ton</i>] The ton keyword specifies the type of number value associated with the SME address. The <i>ton</i> argument is an integer value in the range 0 to 7. – [np <i>np</i>] The np keyword specifies the numbering plan identification value associated with the SME address. The np keyword is not valid when defining the dest-sme in an smsNot operation. The <i>np</i> argument is an integer value in the range 0 to 15. – min Specifies that the address is a Mobile Identification Number (MIN). This keyword can be specified for the <i>sme-addr-type</i> of ANSI-41 operations. – imsi Specifies that the address is an International Mobile Subscriber Identification (IMSI) address. This keyword can be specified for the <i>sme-addr-type</i> of ANSI-41 operations. • exact (Optional) Indicates that the specified <i>dest-addr</i> should be matched only of the number of digits AND the digit values exactly match as specified in <i>dest-addr</i>. If exact is not specified then the <i>dest-addr</i> carries an implicit "*" at the end of the string, allowing a match on the string as a prefix (range of addresses). • min-digits <i>min</i> (Optional) Specifies the minimum number of digits in the address string. The default is 1. • max-digits <i>max</i> (Optional) Specifies the maximum number of digits in the address string. The default is the length of the address string.

Example:

```
ITP(cfg-cs7-mlr-set-rule)# dest-sme 1111 exact
```

	Command or Action	Purpose
Step 9	dest-sme-table <i>table-name</i> [<i>dest-sme-addr-type</i>]	Specifies an SMS address table or an MLR address table of destination SME addresses. • <i>tablename</i> Specifies an address table name. • <i>dest-sme-addr-type</i> (Optional) Parameters that identify attributes of the SME address being used to match a rule. The address is composed of the following keywords: – [ton ton] Specifies the type of number value associated with the SME address. The <i>ton</i> argument is an integer value in the range 0 to 7. – [np np] Specifies the numbering plan identification value associated with the SME address. The np keyword is not valid when defining the dest-sme in an smsNot operation. The <i>np</i> argument is an integer value in the range 0 to 15. – min Specifies that the address is a Mobile Identification Number (MIN). This keyword can be specified for the <i>sme-addr-type</i> of ANSI-41 operations. – imsi Specifies that the address is an International Mobile Subscriber Identification (IMSI) address. This keyword can be specified for the <i>sme-addr-type</i> of ANSI-41 operations. Example: ITP(cfg-cs7-mlr-set-rule)# dest-sme-table MLR-ADDRS

	Command or Action	Purpose
Step 10	dest-smsc { * <i>dest-addr</i> } [<i>addr-type</i>] [exact] [min-digits <i>min</i>] [max-digits <i>max</i>] Example: ITP(cfg-cs7-mlr-set-rule)# dest-smsc 18005551212	Specifies the destination SMSC. • <i>dest-addr</i> Specifies the destination address. Valid range is 1 to 20 hexadecimal digits. • <i>addr-type</i> (Optional) Parameters that identify attributes of the SMSC address being used to match a rule. The address is composed of the following keywords: – [ton <i>ton</i>] Specifies the type of number value associated with the SMSC address. The <i>ton</i> argument is an integer value in the range 0 to 7. – [np <i>np</i>] Specifies the numbering plan identification value associated with the SMSC address. The <i>np</i> argument is an integer value in the range 0 to 15. • exact Specifies address must match dest-smsc exactly. • min-digits <i>min</i> (Optional) Specifies the minimum number of digits in the address string. The default is 1. • max-digits <i>max</i> (Optional) Specifies the maximum number of digits in the address string. The default is the length of the address string.
Step 11	match-unknown-ton-np Example: ITP(cfg-cs7-mlr-set-rule)# match-unknown-ton-np	Specifies that incoming messages containing parameters with unknown type-of-number (ton=0), or unknown numbering plan (np=0), will be a match to the corresponding rule parameter regardless of the rule's configured ton/np values.
Step 12	allow-multi-message-dialogue Example: ITP(cfg-cs7-mlr-set-rule)# allow-multi-message-dialogue	Specifies that the short messages segmented at the MAP layer and SMS MT messages with the More-Messages-To-Send indicator set match the rule. If the allow-multi-message-dialogue command is specified, no other routing parameters may be configured for the rule.

	Command or Action	Purpose
Step 13	orig-imsi {<i>*</i> <i>imsi-address</i> unknown} [exact] [min-digits <i>min</i>] [max-digits <i>max</i>] Example: ITP(cfg-cs7-mlr-set-rule)# orig-imsi unknown	Specifies the origin IMSI address. • <i>imsi-addr</i> Specifies the IMSI address, with up to 16 hexadecimal digits. • unknown Indicates unknown origin IMSI. • exact Specifies configured address must match orig-imsi exactly. • min-digits <i>min</i> The minimum number of digits in the address string. The default is 1. • max-digits <i>max</i> The maximum number of digits in the address string. The default is the length of the address string.
Step 14	orig-imsi-table <i>tablename</i> Example: ITP(cfg-cs7-mlr-set-rule)# orig-imsi-table addrtbl2	Specifies SMS address table or an MLR address table of origin IMSI addresses (address-table). • <i>tablename</i> Specifies an address table name.
Step 15	orig-sme {<i>*</i> <i>orig-addr</i>} [<i>orig-sme-addr-type</i>] [exact] [min-digits <i>min</i>] [max-digits <i>max</i>] Example: ITP(cfg-cs7-mlr-set-rule)# orig-sme 12345	Specifies the address of the origin short message entity (SME) within an SMS operation. This parameter is part of the rule used to match this route. • <i>orig-addr</i> Specifies the origin address. For sms-mo operations, valid range is 1 to 20 hexadecimal digits. For sms-mt operations, valid range is 1 to 16 hexadecimal digits. • <i>orig-sme-addr-type</i> Specifies parameters of the SME address used to match a rule. Valid parameters are: – ton <i>ton</i> Type of number value associated with the SME address. Valid range is 0 to 7. – np <i>np</i> Numbering plan value associated with the SME address. Valid range is 0 to 15. • exact Specifies address must match orig-sme exactly. • min-digits <i>min</i> (Optional) Specifies the minimum number of digits in the address string. The default is 1. • max-digits <i>max</i> (Optional) Specifies the maximum number of digits in the address string. The default is the length of the address string.

	Command or Action	Purpose
Step 16	orig-sme-table <i>tablename</i> [ton <i>ton-value</i> np <i>np-value</i>] Example: ITP(cfg-cs7-mlr-set-rule)# orig-sme-table ADDR-TBL1	Specifies an SMS address table or an MLR address table of origin SME addresses (address-table). • <i>tablename</i> Specifies an address table name. • ton <i>ton</i> Specifies a nature of address value. Valid range is 0 to 7. • np <i>np</i> Specifies a numbering plan identification value. valid range is 0 to 15.
Step 17	orig-smsc { <i>*</i> <i>orig-address</i> } [<i>smc-addr-type</i>] [exact] [min-digits <i>min</i>] [max-digits <i>max</i>] Example: ITP(cfg-cs7-mlr-set-rule)# orig-smsc 8881234	Specifies the address of the originating service center with an SMS MT operation. • <i>orig-address</i> Specifies the origin address. Valid range is 1 to 20 hexadecimal digits. • <i>smc-addr-type</i> Specifies parameters of the SME address used to match a rule. Valid parameters are: – ton <i>ton</i> Type of number value associated with the SME address. Valid range is 0 to 7. – np <i>np</i> Numbering plan value associated with the SME address. Valid range is 0 to 15. • exact Specifies that the address must match exactly. • min-digits <i>min</i> The minimum number of digits in the address string. The default is 1. • max-digits <i>max</i> The maximum number of digits in the address string. The default is the length of the address string.
Step 18	pid <i>protocol-id</i> Example: ITP(cfg-cs7-mlr-set-rule)# pid 0	Specifies the protocol identifier value for an SMS operation. The value of the PIC maps to the values specified for the TP-PID SMS parameter.. • <i>protocol-id</i> Protocol identifier integer. Valid range is 0 to 255.
Step 19	preserve-opc Example: ITP(cfg-cs7-mlr-set)# preserve-opc	Preserves the originating point code (OPC) when a rule is matched.
Step 20	teleservice <i>id</i> Example: ITP(cfg-cs7-mlr-set-rule)# teleservice 5	Specifies a particular service identifier value for an IS-41 SMS operation. • <i>id</i> Integer in the range 0 - 65535.

	Command or Action	Purpose
Step 21	modify-profile <i>profile-name</i> Example: ITP(cfg-cs7-mlr-set-rule)# modify-profile SRISM	Assigns a modify profile to this rule. The modify-profile specifies SCCP and MAP addresses to modify in messages which are MLR routed. Only one modify-profile may be specified in a rule. • <i>profile-name</i> identifies a name to associate with a defined MLR modify-profile. The name is specified as a character string with a maximum of 12 characters.

Command or Action	Purpose
Step 22 result { gt <i>addr-string</i> [<i>gt-addr-type</i>] [instance <i>instance-number</i>] pc <i>dest_pc</i> [ssn <i>ssn</i>] asname <i>as-name</i> group <i>result-group</i> block [sccp-error <i>error</i> map-error { [default <i>ecdef</i> [<i>subdef</i>]] [v1 <i>ec1</i> [<i>sub1</i>]] [v2 <i>ec2</i> [<i>sub2</i>]] [v3 <i>ec3</i> [<i>sub3</i>]] } continue route }	Specifies the processing that will be performed on a packet that matches the specified trigger and rule. One result must be specified. • gt Specifies that the message will be routed using SCCP global title. The specified address will be placed in the SCCP Called Party Address, the routing indicator will be changed to RI=GT, and then routed based on the locally provisioned global title translation table. • <i>gt-addr-type</i> (Optional) Parameters that identify attributes of the global title address being used as a result. The parameters are variant-specific, and are identical to those parameters specified on a cs7 gtt selector command. If not specified, the default is the standard E.164 address type for the network variant being used. – tt <i>tt</i> [gti <i>gti</i>] [np <i>np</i> nai <i>nai</i>] – tt Identifies the translation type specified within the address. – <i>tt</i> An integer value from 0 to 255. – gti Identifies the global title indicator value for the specified address. This value is only specified when cs7 variant is ITU or China. – <i>gti</i> An integer value of 2 or 4. – np Identifies the numbering plan of the specified address. Only specified when the gti parameter value is 4. – <i>np</i> An integer value from 0 to 15. • nai Identifies the nature of specified address. Only specified when the gti parameter value is 4. • <i>nai</i> Integer value from 0 to 127. • instance (Optional) Indicates the PC/PCSSN result in local or other instance. • <i>instance-number</i> (Optional) Instance number. The valid range is 0 through 7. The default instance is 0. • pc Specifies that the message will be routed using the specified destination point code (DPC). The packet is routed in MTP3 with the specified DPC.

Command or Action	Purpose
Example: <pre>ITP(cfg-cs7-mlr-set-rule)# cs7 mlr ruleset ruleset1 rule 10 gsm-map sms-mo dest-sme 1234 orig sme 60920025 result group SMS-WEIGHTED</pre> Example: <pre>ITP(cfg-cs7-mlr-set-rule)# cs7 mlr ruleset mapecset protocol gsm-map rule 10 sms-mo default result block map-error v1 systemFailure</pre> Example: <pre>ITP(cfg-cs7-mlr-set-rule)#cs7 instance 0 mlr ruleset tttt protocol gsm-map rule 1 sms-mo default result instance 1 pc 3.3.3 ssn 7</pre>	• dest-pc DPC in variant-specific point-code format. • ssn Specifies that the message will be routed using the subsystem number. • ssn Subsystem number in decimal. Valid range is 2 to 255. • asname Specifies that the message will be routed to a particular destination M3UA or SUA application server. • as-name 1 to 12 character name identifying an M3UA or SUA application server name. • group Specifies that the message will be routed using a result group. A group is used to specify multiple destinations for a given rule match. The MLR result group must be defined prior to configuring the result command. • result-group Identifies the name of the MLR result group containing the desired result possibilities. The name is specified as a character string with a maximum of 12 characters. • block sccp-error error Specifies that messages matching this rule will be dropped. Send a UDTS for dropped packets to the originator with the configured sccp error code if return-on-error was set in the UDT. • block map-error Performs MAP error handling. Defines the MAP error Code for MLR/SMS blocked MSUs based on operation type and version. If an MLR or SMS module matches the rule and the MSU is blocked, an error message is sent instead of dropping the MSU silently. • default Specifies there is a default return MAP Error code. • ecdef The default return MAP Error code. • subdef Specifies a secondary default MAP error code. • v1 MAP version 1 • v2 MAP version 2 • v3 MAP version 3 • ec1 Specifies the MAP error code for ec1. • ec2 Specifies the MAP error code for ec2. • ec3 Specifies the MAP error code for ec3.

Command or Action	Purpose
	• <i>sub1</i> Specifies a secondary MAP error code for sub1. • <i>sub2</i> Specifies a secondary MAP error code for sub2. • <i>sub3</i> Specifies a secondary MAP error code for sub3. • continue Specifies that the original message should be routed as received. • route Specifies that the packet should resume original routing with the MLR-modified message.

Define the MLR Triggers

An MLR table comprises a list of primary triggers, which can represent either the SCCP, cgPa, or SCCP cdPa within a given message. When you define the MLR triggers, it specifies the SS7 network-layer parameters to identify traffic that requires parsing into the application layers.

Cisco ITP supports two methods of defining the MLR triggers. The integrated GWS method and the older, proprietary method. The integrated GWS method is recommended. The proprietary method is supported primarily for legacy configurations from earlier Cisco ITP releases.

This section contains the following information and procedure:

- [Define the MLR Triggers with GWS, page 240](#)
- [Information About MLR Triggers with GWS, page 240](#)
- [Define MLR Triggers with Proprietary Method, page 242](#)



Note

The proprietary method of configuring MLR triggers using MLR tables is still supported but not recommended.

Define the MLR Triggers with GWS

You can configure MLR triggers using the GWS infrastructure, GWS tables, and MLR variables. For information on this, you need to refer to the [Gateway Screening \(GWS\)](#) chapter. See “[Defining GWS Action Sets](#)” section on page 180 or “[Defining Entries in GWS Tables](#)” section on page 184 in .

Information About MLR Triggers with GWS

MLR triggers and GWS are integrated. GWS determines which packets are intercepted by MLR.

Migration of Existing MLR Trigger Configuration

MLR table and MLR trigger configurations created in MLR tables in prior releases are still supported by later releases with integrated GWS and MLR triggers. But this is primarily so users can delete the existing triggers configured prior to the integration and replace these triggers with new triggers configured in GWS. This is the best practice since the newer GWS tables are given precedence over the older MLR tables. User should also configure any new MLR triggers through GWS.

**Note**

A warning states that the MLR table command will be deprecated.

Logging and Test Mode for MLR with GWS

GWS logging supports MLR. You enable GWS logging when you configure a link set, AS, or global table as GWS.

Test mode is a logging option. With test mode, once the GWS tables and action-sets are configured, you can test them before applying them to live traffic. If GWS rules block the packet, the test mode may create a log and allow the packet. If GWS rules send the packet to MLR routing, the test mode may create a log and operate as if there is no MLR configured. Test mode is useful when MLR triggers configured the proprietary way are migrated to GWS tables. You test the new GWS triggers before deleting the existing proprietary MLR triggers.

For more information on logging and test mode, see the [“Message Logging” section on page 195](#).

Disabling of MLR Triggers

MLR table configuration used the global configuration command **cs7** [*instance instance-number*] **mlr table** *table-name* and also the global configuration command **trigger**. Under MLR table configuration the **no** form of these commands deletes the configured triggers. GWS configuration also supports the **no** forms of these commands. But the GWS **no** command does not delete the triggers like the MLR table configuration **no** command does. The GWS version only disables triggers and prevents the trigger lookup for that trigger instance. The GWS disabling applies to MLR triggers configured in either GWS or through MLR tables.

MLR and GWS Table Matching Order for Incoming Packets

Cisco ITP supports local application-based table matching for GWS in addition to table matching based on a link set or AS. The sequence of conditions for table matching depends on whether the packet is received from a local application or is received from a link set or AS.

Precedence Followed for Link Set or AS

An attempt to match the table occurs in the following sequence for any incoming packet received on a specific link set or AS:

1. If a GWS configuration exists, the GWS configuration is applied.
2. If a GWS configuration does not exist for the specific link set or AS, but a GWS default configuration exists, the default configuration is applied.
3. If neither a specific GWS configuration nor a default GWS configuration exists, but a global table exists, the global table is applied.

4. If none of the above situations apply, but MLR triggers not configured through GWS exist, these MLR triggers apply. (This step applies only to MLR. It does not apply to GWS.)
5. If none of the above situations apply, then packet is neither screened nor routed by MLR but routed normally.

Precedence Followed for a Local Application



Note

Local application precedence applies only to MLR. It does not apply to GWS.

An attempt to match the table occurs in the following sequence for any incoming packet received from a local application:

1. If a global table exists, the global table is applied.
2. If no global tables exist, but MLR triggers not configured through GWS exist, these MLR triggers are applied.
3. If none of the above situations apply, then packet is neither screened nor routed by MLR but routed normally.

How MLR Using GWS Works with Access Lists

MLR configured through GWS works with access lists in the same way that GWS does. For more information, see [“How GWS Works with Access Lists” section on page 175](#)

Define MLR Triggers with Proprietary Method

To define the MLR table with proprietary method, perform the following steps. Steps 1 - 4 are required in the order show. Steps 5 - 7 are optional; they are used to configure secondary triggers.



Caution

Configuring MLR using the GWS infrastructure is the recommended method.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cs7** [*instance instance-number*] **mlr table** *name*
4. **trigger** {**mtp3** {[*dpc point-code*] [*opc point-code*] [*si indicator*]} | **cdpa** {**gt**¹ {**selector** | *addr-string*} [*gt-addr-type*] | **pc point-code** *ssn ssn*} | **cgpa** {**gt** {**selector** | *addr-string*} [*addr-type*] | **pc point-code** *ssn ssn*} | **default**} [**block** | **continue** | **ruleset** *ruleset-name* | **result** {**pc point-code** [*ssn ssn*] | **asname** *asname* | **gt** *gta* [*gt-addr-type*] | **group** *groupname*}}}
5. **cdpa** {**gt** {**selector** | *addr-string*} [*gt-addr-type*] | **pc point-code** *ssn ssn*} [**block** | **continue** | **ruleset** *ruleset-name* | **result** {**pc point-code** [*ssn ssn*] | **asname** *asname* | **gt** *gta* [*gt-addr-type*] | **group** *groupname*}}}
6. **cgpa** {**gt** {**selector** | *addr-string*} [*addr-type*] | **pc point-code** *ssn ssn*} [**block** | **continue** | **ruleset** *ruleset-name* | **result** {**pc point-code** [*ssn ssn*] | **asname** *asname* | **gt** *gta* [*gt-addr-type*] | **group** *groupname*}}}

1. To enable a cdpa or cgpa trigger, the CS7 GTT selector and GTA entry must be defined. For more information about configuring GTT, refer to the [“Global Title Translation”](#) chapter.

7. **default** {**block** | **continue** | **ruleset** *ruleset-name* | **result** {**pc** *point-code* [**ssn** *ssn*] | **asname** *asname* | **gt** *gta* [*gt-addr-type*] | **group** *groupname*}}

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: ITP> enable	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	configure { terminal memory network } Example: ITP# configure terminal	Enters global configuration mode.
Step 3	cs7 [instance <i>instance-number</i>] mlr table <i>table-name</i> Example: ITP(config)# cs7 mlr table SMS-TABLE	Specifies the MLR routing table name and enables the MLR table configuration mode.
Step 4	trigger { mtp3 {[dpc <i>point-code</i>] [opc <i>point-code</i>] [si <i>indicator</i>]} cdpa { gt ¹ { selector <i>addr-string</i> } [<i>gt-addr-type</i>] pc <i>point-code</i> ssn <i>ssn</i>] cgpa { gt { selector <i>addr-string</i> } [<i>addr-type</i>] pc <i>point-code</i> ssn <i>ssn</i>] default } block continue ruleset <i>ruleset-name</i> result { pc <i>pc</i> [ssn <i>ssn</i>] asname <i>asname</i> gt <i>gta</i> [<i>gt-addr-type</i>] group <i>groupname</i> }}] Example: Router(config-cs7-mlr)# trigger cdpa gt 9991117770 ruleset RULESET-5	Specifies the routing key, or trigger, which will be used to route or block messages according to a specified ruleset. Enables the MLR trigger configuration mode in which you can define combination triggers.
Step 5	cdpa { gt { selector <i>addr-string</i> } [<i>gt-addr-type</i>] pc <i>point-code</i> ssn <i>ssn</i>] { block continue ruleset <i>ruleset-name</i> result { pc <i>pc</i> [ssn <i>ssn</i>] asname <i>asname</i> gt <i>gta</i> [<i>gt-addr-type</i>] group <i>groupname</i> }}] Example: Router(cfg-cs7-mlr-trigger)# cdpa gt 9991117770 ruleset RULESET-5	Define a combination trigger. (MTP3 may be specified as a primary trigger only.) The secondary triggers in conjunction with the trigger address constitute the combination trigger used to match a packet. If any secondary address in the trigger submode is specified, then BOTH addresses must match for the packet to be blocked or routed using the specified ruleset. The parameter keywords and values are the same as those defined for the trigger command.

	Command or Action	Purpose
Step 6	<pre>cgpa {gt {selector addr-string} [addr-type] pc point-code ssn ssn} {block continue ruleset ruleset-name result {pc pc [ssn ssn] asname asname gt gta [gt-addr-type] group groupname}}</pre> Example: Router(cfg-cs7-mlr-trigger)# cGpa gt 9991116 ruleset RULESET-5	Within the mlr-trigger submode, the cgpa , cdpa and default ruleset commands are used to define combination triggers. (MTP3 may be specified as a primary trigger only.) The secondary triggers in conjunction with the trigger address constitute the combination trigger used to match a packet. If any secondary address in the trigger submode is specified, then BOTH addresses must match for the packet to be blocked or routed using the specified ruleset. The parameter keywords and values are the same as those defined for the trigger command.
Step 7	<pre>default {block continue ruleset ruleset-name result {pc pc [ssn ssn] asname asname gt gta [gt-addr-type] group groupname}}</pre> Example: Router(cfg-cs7-mlr-trigger)# default ruleset DEFAULT-RULES	Within the mlr-trigger submode, the cgpa , cdpa and default ruleset commands are used to define combination triggers. (MTP3 may be specified as a primary trigger only.) The secondary triggers in conjunction with the trigger address constitute the combination trigger used to match a packet. If any secondary address in the trigger submode is specified, then BOTH addresses must match for the packet to be blocked or routed using the specified ruleset. The parameter keywords and values are the same as those defined for the trigger command.

1. To enable a cdpa or cgpa trigger, the CS7 GTT selector and GTA entry must be defined. For more information about configuring GTT, refer to the [“Global Title Translation”](#) chapter.

How to Configure MLR-Based Screening

The following sections describe and provide example of MLR-based screening. When a message is blocked MLR discards the packet.

- [Blocking Based on SCCP cdPa and cgPa, page 244](#)
- [Blocking Based on cgPa, cdPa, and SMS MAP Operation Code, page 247](#)
- [Blocking Based on cgPa, cdPa and SMS MO/MT Routing Parameters, page 247](#)

Blocking Based on SCCP cdPa and cgPa

This section includes the following tasks to configure blocking based on SCCP cdPa and cgPa:

- [Define GTT Entries for cdPa and cgPa digits to Screen](#)
- [Define MLR table and Blocking Based on SCCP cdPa or cgPa](#)
- [Define MLR Table and Blocking on Combination of SCCP cdPa and cgPa](#)

Define GTT Entries for cdPa and cgPa digits to Screen

To define the GTT entries for cdPa and cgPa digits to screen, perform the following steps. Steps 1 - 3 are required in the order shown. Perform steps 4 - 6 as appropriate to your needs, to specify a GTA.

SUMMARY STEPS

1. **enable**
2. **configure** { **terminal** | **memory** | **network** }
3. **cs7 gtt selector** *selector tt tt gti gti np np*
4. **gta gta app-grp** *app-grp*
5. **gta gta asname** *as-name* { **gt** | **pcssn** } [**ssn** *ssn*] [**ntt** *newtt*] [**qos-class** *qos*]
6. **gta gta pcssn** *pc* { **gt** | **pcssn** } [**ssn** *ssn*] [**ntt** *newtt*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: ITP> enable	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	configure { terminal memory network } Example: ITP# configure terminal	Enters global configuration mode.
Step 3	cs7 gtt selector <i>selector tt tt gti gti np np</i> nai nai Example: ITP(config)# cs7 gtt selector e164 tt 10 gti 2	Names and configures the GTT selector and enables CS7 GTT selector submode. MLR primary GT triggers re-use the existing GTT selector table entity containing lists of GTA entries used to perform Global Title Translation.
Step 4	gta gta app-grp <i>app-grp</i> Example: ITP(config-cs7-gtt-selector)# gta 11111 app-grp GROUP1	Defines a GTA that translates to a GTT application group.
Step 5	gta gta asname <i>as-name</i> { gt pcssn } [ssn <i>ssn</i>] [ntt <i>newtt</i>] [qos-class <i>qos</i>] Example: ITP(config-cs7-gtt-selector)# gta 22222 asname GREENASP3 pcssn	Defines a GTA that translates to an M3UA or SUA Application Server name.
Step 6	gta gta pcssn <i>pc</i> { gt pcssn } [ssn <i>ssn</i>] [ntt <i>newtt</i>] Example: ITP(config-cs7-gtt-selector)# gta 33333 pcssn 1.1.1 pcssn	Defines a GTA that translates to a point code and optional subsystem number.

Example:

```
cs7 gtt selector e164 tt 10
gta 11111 pcssn 1-1-1 pcssn
gta 22222 pcssn 2-2-2 pcssn
gta 33333 pcssn 3-3-3 pcssn
```

**Note**

The GTT mapping results will not be used if blocking triggers are configured via MLR for the cgPa and cdPa global title addresses.

Define MLR table and Blocking Based on SCCP cdPa or cgPa

An MLR table consists of a list of primary triggers, which can represent either the SCCP cgPa or the SCCP cdPa within a given message. To block a message based on either cgPa or cdPa, specify the block keyword in lieu of a ruleset.

Example:

```
cs7 mlr table sms-blocking
trigger gt 11111 tt 10 block
trigger cgpa gt 22222 tt 10 block
trigger cgpa gt 33333 tt 10 block
```

When coding a mixture of primary cgPa and primary cdPa triggers, the triggers are not searched sequentially. The first primary trigger match found is used based on the following hierarchy:

1. The default trigger is defined (only trigger configured)
2. cdPa GT triggers when SCCP cdPa is RI=GT
3. cdPa PC/SSN triggers when SCCP cdPa is RI=SSN
4. cgPa GT triggers when SCCP cgPa is RI=GT
5. cgPa PC/SSN triggers when SCCP cgPa is RI=SSN

Define MLR Table and Blocking on Combination of SCCP cdPa and cgPa

To block a message based on a combination of SCCP cdPa and cgPa, specify the combination triggers and place the block keyword at the end of the secondary trigger.

Example:

```
cs7 mlr table sms-blocking
trigger cdpa gt 11111 tt 10 ruleset MY_RULES
cgpa gt 22222 tt 10 block
cgpa gt 33333 tt 10 block
```

**Note**

Ruleset `MY_RULES` is a placeholder and will not be used. A packet destined for 11111 from 44444 will not match a trigger, and will be routed normally.

Blocking Based on cgPa, cdPa, and SMS MAP Operation Code

MLR triggers must be specified, but will be configured with an associated MLR ruleset instead of the **block** keyword. When a non-blocking MLR trigger matches, the received packet is parsed through the application layer for the rule operations identified in the ruleset.

Example:

The following example will block all SMS MO messages from 22222 to 11111, and will block all SMS MT message from 11111 to 33333. All other messages will be routed according to standard SCCP and MTP3 procedures.

```
cs7 mlr ruleset BLOCK-SMSMO gsm-map
  rule 10 sms-mo default
  result block

cs7 mlr ruleset BLOCK-SMSMT gsm-map
  rule 10 sms-mt default
  result block

cs7 mlr table sms-blocking
  trigger cdpa gt 11111 tt 10
  cgpa gt 22222 tt 10 ruleset BLOCK-SMSMO
  trigger cdpa gt 33333 tt 10
  cgpa gt 11111 tt 10 ruleset BLOCK-SMSMT
```

Blocking Based on cgPa, cdPa and SMS MO/MT Routing Parameters

To block based on select parameters within the SMS MO or SMS MT message, specify the appropriate routing parameters within sms-mo or sms-mt operation. Rules are searched sequentially for a match.

Example:

The following example will block all SMS MO messages from 22222 to 11111 with an origin SME (A-address) prefix of 919 and return an UDTs with return cause set as 0x07 (Unqualified), if the return on error option is set in the received UDT portion of SMS MO. It will also block all SMS MT messages from 11111 to 33333 with a destination SME (or mobile) IMSI of 238012650007149. All other messages not matching a trigger will be routed according to standard SCCP and MTP3 procedures.

```
cs7 mlr ruleset BLOCK-SMSMT gsm-map
  rule 10 sms-mt
  dest-sme 238012650007149
  result block
cs7 mlr ruleset BLOCK-SMSMO gsm-map
  rule 10 sms-mo
  orig-sme 919
  result block 7
.....
```

Verifying and Monitoring MLR Routing

With this task you verify configuration, monitor status, and troubleshoot errors in the MLR configuration. When MLR triggers are implemented through GWS, some GWS show commands also display details about MLR, see the [“Verifying GWS Configuration” section on page 197](#) for these commands.

To display information about the MLR configuration, perform the following steps in privileged EXEC mode:

Command	Purpose
Router# show cs7 <i>instance-number</i> mlr address-table <i>name table-name</i>	Displays the addresses matched within the table.
router# show cs7 [<i>instance-number</i>] mlr config	This command displays the whole configuration of MLR.
Router# show cs7 <i>instance-number</i> mlr dest-sme-binding <i>dest-sme [result-group-name]</i>	Displays the result that will be selected from an MLR result group for the specified dest-sme address. <i>dest-sme</i> Specifies the dest-sme address whose result you wish to display. Valid dest-sme addresses are between 1 and 20 hexadecimal digits in length. Only the final 4 digits of the address are needed to determine the dest-sme-binding result. Alphanumeric dest-sme addresses can not currently be specified. <i>result-group-name</i> (Optional) Specifies which result group to use. If the <i>result-group-name</i> is not specified, then this display will output the dest-sme-binding result for the input dest-sme for each result group in dest-sme-binding mode.
Router# show cs7 [<i>instance-number</i>] mlr modify-profile [<i>profile-name</i>]	Displays the current modify-profiles and their statistics. The matches count indicates the number of times that the modify profile was applied to a message. Matches does not indicate success or failure of the applied modifications. The modify failures count indicates the number of times that the matching message could not be modified as specified in the modify-profile.
Router# show cs7 mlr options	Displays specify MLR global options information.
Router# show cs7 <i>instance-number</i> mlr result <i>name</i>	Displays the contents of all MLR result groups, or a specific named result group along with the weight and number of matches for each server result.
Router# show cs7 <i>instance-number</i> mlr ruleset <i>name</i>	Displays MLR ruleset information Details include UDTs configuration, including whether the UDTs return cause is implemented with a result block.
Router# show cs7 <i>instance-number</i> mlr statistics	Displays statistics associated with MLR. Since MLR triggers either through MLR tables or through GWS, statistics include GWS-MLR trigger matches, statistics for MLR ruleset, and resultgroup matches through GWS triggers.
Router# show cs7 <i>instance-number</i> mlr table <i>name detail</i>	Displays the parameters and results associated with each routing trigger.
Router# show cs7 <i>instance-number</i> mlr table <i>name result-summary</i>	Displays the result parameters associated with a particular rule along with the number of times the rule has been matched for the given trigger.

Command	Purpose
Router# show cs7 <i>instance-number mlr table name rule-summary</i>	Displays the rule parameters associated with a particular rule along with the number of times the rule has been matched for the given trigger.
Router# show monitor event-trace [all-traces] [<i>component {all back time clock time from-boot seconds latest parameters}</i>]	Displays event trace messages for Cisco IOS software subsystem components. For more information about the show monitor event-trace command, refer to feature documentation for the Event Tracer, introduced in IOS Release 12.0(18)S http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s18/evnttrcr.htm

To display debug messages for Multi-layer routing, use the **debug cs7 mlr** command in privileged EXEC mode.

Command	Purpose
Router# debug cs7 mlr all	Enables all debugs.
Router# debug cs7 mlr error	Debugs error events.
Router# debug cs7 mlr info	Displays informational events
Router# debug cs7 mlr packet	Displays packet events.

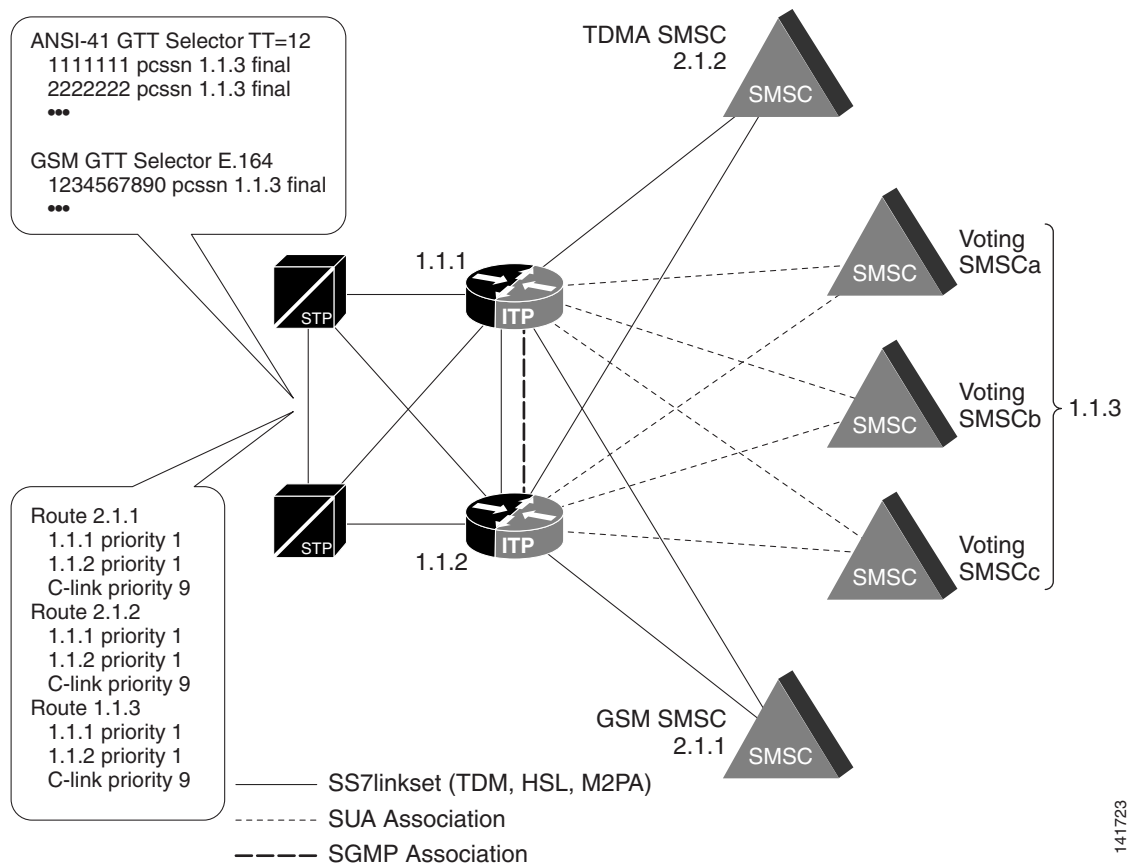
Configuration Examples of MLR

This section includes the following examples:

- [Configuration Example of Address Modification, page 257](#) [Configuration Example for MLR: ITP Receives All SMS-MO Traffic in GT-Routed Network, page 249](#)
- [Configuration Example for MLR: Legacy SMSC Retains Point Code in PC-Routed Network, page 252](#)
- [Configuration Example for MLR: MLR Distribution to MTP3-Based SMSCs, page 254](#)
- [Examples of Configuring Routing Based on Operation Types, page 256](#)
- [Example of Routing with B-Address Binding, page 257](#)

[Configuration Example of Address Modification, page 257](#) **Configuration Example for MLR: ITP Receives All SMS-MO Traffic in GT-Routed Network**

In this example, a mated pair of ITPs is positioned between the core SS7 network STPs and both the legacy and voting SMSCs. The network configuration is illustrated in [Figure 30](#).

Figure 30 *MLR: ITP Receives All SMS-MO Traffic in GT-Routed Network*

The STPs in the network are configured to perform final GTT toward the ITP SMSC complex. In GSM, the translation will be done based on the E.164 addresses of the legacy SMSCs. In IS-41, the translation will be done using TT=12 to map the MIN to the serving MC. In either case, the GTT translations must be changed to map to the mated-ITP pair's PC for SMSC processing, 1.1.3. No GTT is performed on the ITPs.

GAIT/GHOST SMS MO messages carried over ANSI-41 arrive at ITP1 destined for the SMSC point-code 1.1.3. An SCCP cdPa trigger based on PC/SSN will signal parsing of the TCAP, MAP and SMS routing layers. There will be a trigger for GSM MAP, as well as IS-41/GHOST based on the SSNs 8 and 11, respectively. The GSM-RULES and TDMA-RULES rulesets are then referenced to determine if the destination SME address represents a voting event. Note that each ruleset uses the same dest-sme address tables for efficient best-match lookup.

If a voting event is determined, the message is routed to the selected voting SMSC, otherwise the message is routed to the legacy SMSC. Note that SMS_Notification messages with the same destination SME pattern are routed to the same SMSC ASes. This configuration assumes that the voting SMSCs are all ASPs within the same AS using a routing-key of PC 1.1.3.

```

cs7 multi-instance
cs7 instance 1 variant ansi
cs7 instance 1 point-code 1.1.1

cs7 instance 1 as VOTING_AS sua
routing-key 113 1.1.3
asp SMSCa

```



```

asp SMSCb
asp SMSCc
traffic-mode loadshare roundrobin

cs7 instance 1 as SMSCa sua
routing-key 1 gtt
asp SMSCa

cs7 instance 1 as SMSCb sua
routing-key 2 gtt
asp SMSCb

cs7 instance 1 as SMSCc sua
routing-key 3 gtt
asp SMSCc

cs7 instance 1 mlr result SMS-WEIGHTED
as SMSCa weight 1
as SMSCb weight 1
as SMSCc weight 2
pc 2.1.1 weight 0

cs7 instance 1 mlr result MINGRP1
as SMSCa weight 1
as SMSCb weight 0

cs7 instance 1 mlr result MINGRP2
as SMSCb weight 1
as SMSCc weight 0

cs7 instance 1 mlr result MINGRP3
as SMSCc weight 1
as SMSCa weight 0

cs7 mlr address-table VSMSC-ADDRS
addr 24 exact result group SMSC-GROUP1
addr 26 exact result group SMSC-GROUP1
... <161 other exact-match short-codes>
addr 74648633 exact result group SMSC-GROUP1
addr 2004 result group SMSC-GROUP1
addr 901 result group SMSC-GROUP1
addr 902 result group SMSC-GROUP1
addr 110480 result group SMSC-GROUP1
addr 111480 result group SMSC-GROUP1
... <5 other prefix-match SME addresses>
addr 11150 result group SMSC-GROUP1

cs7 mlr ruleset TDMA-RULES
rule 1 ansi-41 smdpp
dest-sme table VSMSC-ADDRS
rule 2 ansi-41 smsnot
dest-sme table VSMSC-ADDRS
rule 3 ansi-41 smdpp default
result group TDMA-SMSCS
rule 4 ansi-41 smsnot default
result group TDMA-SMSCS

cs7 mlr ruleset GSM-RULES
rule 1 gsm-map sms-mo
dest-sme table VSMSC-ADDRS
rule 2 gsm-map alertsc
dest-sme table VSMSC-ADDRS
rule 3 gsm-map sms-mo default
result group GSM-SMSCS

```

```

rule 4 gsm-map alertsc default
  result group GSM-SMSCS

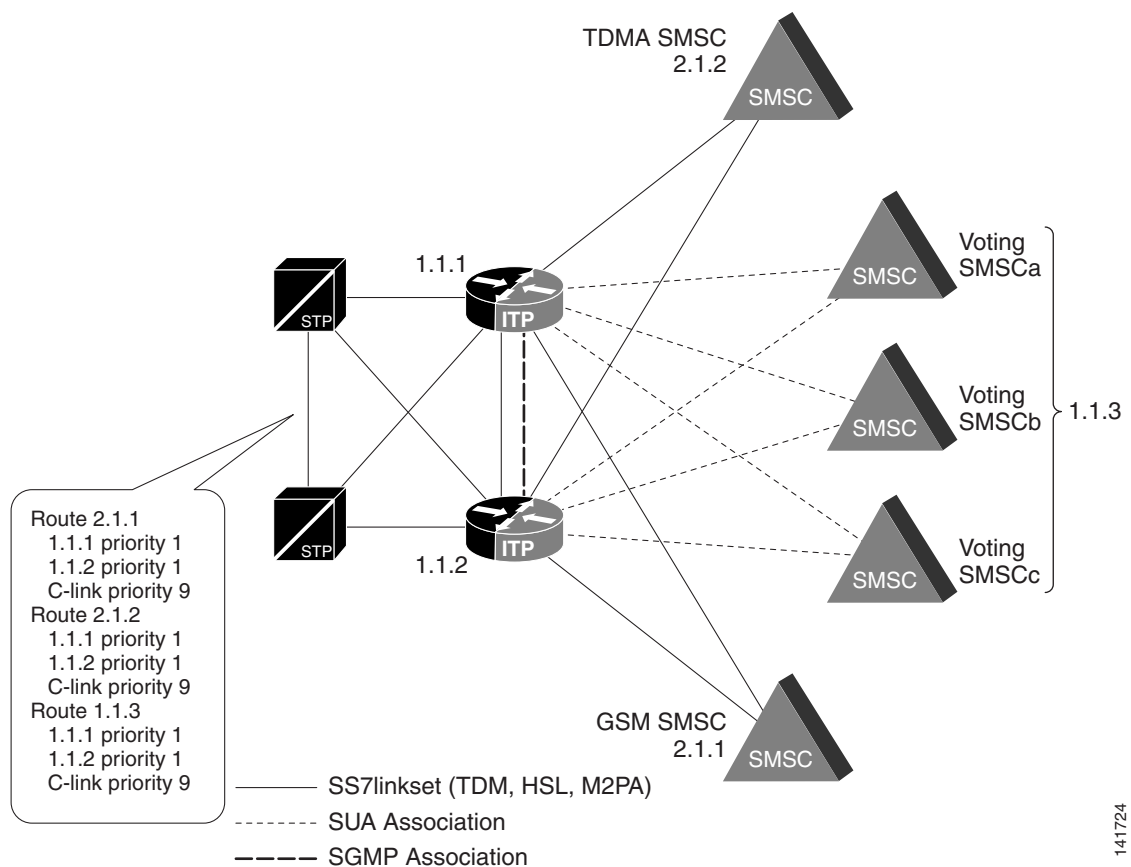
cs7 mlr table SMS-ROUTING
  trigger cdpa pc 1.1.3 ssn 8 ruleset GSM-RULES
  trigger cdpa pc 1.1.3 ssn 11 ruleset TDMA-RULES

```

Configuration Example for MLR: Legacy SMSC Retains Point Code in PC-Routed Network

In this example, a mated pair of ITPs is positioned between the core SS7 network STPs and both the legacy and voting SMSCs. The network configuration is illustrated in [Figure 31](#)

Figure 31 .MLR: Legacy SMSC Retains Point Code in PC-Routed Network



GAIT/GHOST SMS MO messages carried over ANSI-41 arrive at ITP1 destined for the legacy SMSC point-code 2.1.1. An MTP3 MLR trigger based on the DPC, SI and SCCP sub-trigger of cdPa SSN will signal parsing of the TCAP, MAP and SMS routing layers. The GSM-RULES ruleset is then referenced to determine if the destination SME address represents a voting event.

IS-136 and IS-95 SMS MO messages arrive at ITP1 destined for the legacy SMSC PC 2.1.2. The TDMA-RULES ruleset is then referenced to determine if the destination SME address represents a voting event.

If a voting event is determined, the message is routed to the selected voting SMSC, otherwise the message is routed to the legacy SMSC. Note that SMS_Notification messages with the same destination SME pattern are routed to the same SMSC ASes. This configuration assumes that the voting SMSCs are all ASPs within the same AS using a routing-key of PC 1.1.3.

```
cs7 multi-instance
cs7 instance 1 variant ansi
cs7 instance 1 point-code 1.1.1

cs7 instance 1 as VOTING_AS sua
  routing-key 113 1.1.3
  asp SMSCa
  asp SMSCb
  asp SMSCc
  traffic-mode loadshare roundrobin

cs7 instance 1 as SMSCa sua
  routing-key 1 gtt
  asp SMSCa

cs7 instance 1 as SMSCb sua
  routing-key 2 gtt
  asp SMSCb

cs7 instance 1 as SMSCc sua
  routing-key 3 gtt
  asp SMSCc

cs7 instance 1 mlr result SMS-WEIGHTED
  as SMSCa weight 1
  as SMSCb weight 1
  as SMSCc weight 2
  pc 2.1.1 weight 0

cs7 instance 1 mlr result MINGRP1
  as SMSCa weight 1
  as SMSCb weight 0

cs7 instance 1 mlr result MINGRP2
  as SMSCb weight 1
  as SMSCc weight 0

cs7 instance 1 mlr result MINGRP3
  as SMSCc weight 1
  as SMSCa weight 0

cs7 instance 1 mlr ruleset GHOST-RULES ansi-41
  rule 1 smdpp
    dest-sme 111
    result group SMS-WEIGHTED
  rule 2 smdpp
    dest-sme 222
    result group SMS-WEIGHTED
  rule 3 smdpp
    dest-sme 333
    result group SMS-WEIGHTED
  rule 10 sms-notify
    dest-sme 111
    result group SMS-WEIGHTED
  rule 20 sms-notify
    dest-sme 222
    result group SMS-WEIGHTED
  rule 30 sms-notify
```

```

dest-sme 333
result group SMS-WEIGHTED

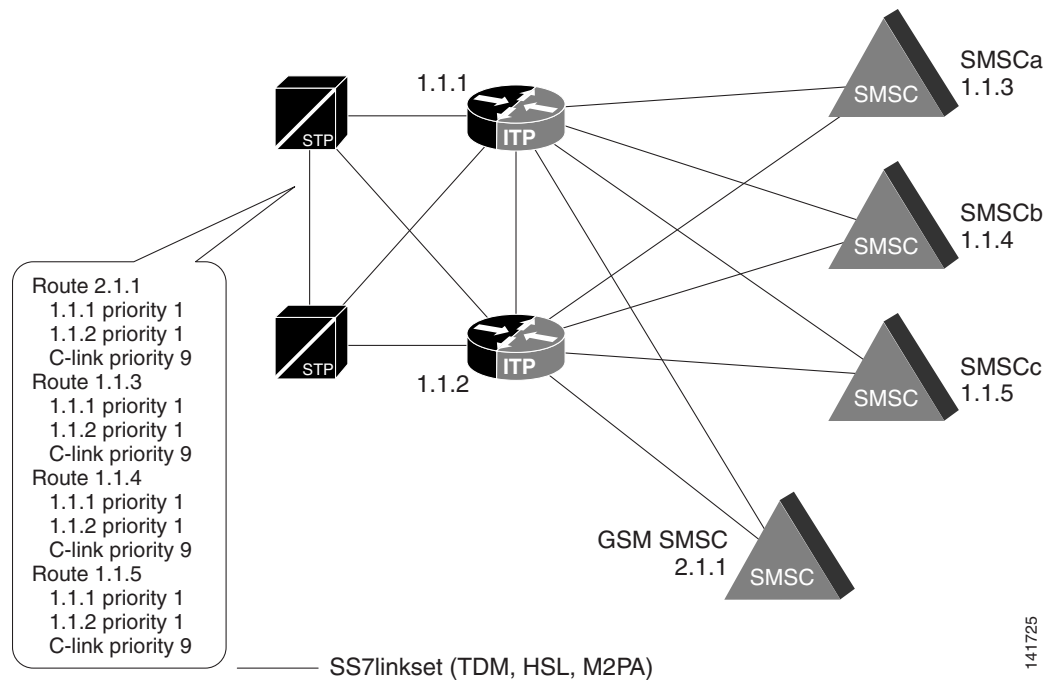
cs7 instance 1 mlr ruleset TDMA-RULES ansi-41
rule 1 smdpp
  dest-sme 100 min
  result group MINGRP1
rule 2 smdpp
  dest-sme 200 min
  result group MINGRP2
rule 3 smdpp
  dest-sme 300 min
  result group MINGRP3
rule 10 sms-notify
  dest-sme 100 min
  result group MINGRP1
rule 20 sms-notify
  dest-sme 200
  result group MINGRP2
rule 30 sms-notify
  dest-sme 3
  result group MINGRP3

cs7 instance 1 mlr table SMS-TABLE
trigger mtp3 dpc 2.1.1 si 3
  cdpa pc 2.1.1 ssn 8 ruleset GHOST-RULES
trigger mtp3 dpc 2.1.2 si 3
  cdpa pc 2.1.2 ssn 11 ruleset TDMA-RULES

```

Configuration Example for MLR: MLR Distribution to MTP3-Based SMSCs

In this example, additional SMSCs are introduced in order to distribute load based on MIN. The legacy SMSC PC is 2.1.1, and is the DPC for all MO SMS messages. MTP3-based MLR triggers are used to distribute the traffic based on the destination SME address, which in this case will be a MIN. The network configuration is illustrated in [Figure 32](#).

Figure 32 MLR Distribution to MTP3-Based SMSCs

```

cs7 multi-instance
cs7 instance 1 variant ansi
cs7 instance 1 point-code 1.1.1

cs7 instance 1 mlr result MINGRP1
pc 1.1.3 weight 1
pc 1.1.4 weight 0

cs7 instance 1 mlr result MINGRP2
pc 1.1.4 weight 1
pc 1.1.5 weight 0

cs7 instance 1 mlr result MINGRP3
pc 1.1.5 weight 1
pc 1.1.3 weight 0

cs7 instance 1 mlr ruleset TDMA-RULES ansi-41
rule 1 smdpp
dest-sme 100 min
result group MINGRP1
rule 2 smdpp
dest-sme 200 min
result group MINGRP2
rule 3 smdpp
dest-sme 300 min
result group MINGRP3
rule 10 sms-notify
dest-sme 100 min
result group MINGRP1
rule 20 sms-notify
dest-sme 200
result group MINGRP2
rule 30 sms-notify
dest-sme 300
result group MINGRP3

```

```
cs7 instance 1 mlr table SMS-TABLE
trigger mtp3 dpc 2.1.1 si 3
cdpa pc 2.1.1 ssn 11 ruleset TDMA-RULES
```

Examples of Configuring Routing Based on Operation Types

The following are examples of configuring routing based on operation types.

Example: Configure Routing Based on SMS MT Parameters

Specify one or more of the SMS MT routing parameters when defining a rule with the sms-mt operation type. Then specify the result destination for the message via the result parameter. Rules are searched sequentially for a match, and rulesets may contain a mixture of rules defining any operation type.

In the following example, all SMS MT messages destined to the MSC 11111 with a destination SME (or mobile) IMSI of 238012650007149 are routed via the MLR distribution group named CLUSTER. SMS MT messages originating from the mobile MSISDN 9193922900 are routed to pc 1-3-1. All other SMS MT messages are routed to pc 1-2-1.

```
cs7 mlr result CLUSTER
pc 1-1-1 weight 5
pc 2-2-2 weight 1
pc 3-3-3 weight 0

cs7 mlr ruleset SMSMT gsm-map
rule 10 sms-mt
dest-sme 238012650007149
result group CLUSTER
rule 20 sms-mt
orig-sme 9193922900
result pc 1-3-1
rule 30 sms-mt default
result pc 1-2-1

cs7 mlr table MT-ROUTING
trigger cdpa gt 11111 tt 10 ruleset SMSMT
```

Example: Configure Routing Based on SRI SM Parameters

Specify one or more of the SRI SM routing parameters when defining a rule with the sri-sm operation type. Then specify the result destination for the message via the result parameter. Rules are searched sequentially for a match, and rulesets may contain a mixture of rules defining any operation type.

In the following example, all SRI-SM messages destined to the HLR 44444 with a destination SME (MSISDN) of 9191112222 are routed via the MLR distribution group 'cluster'. All other SRI-SM messages are routed to pc 1-3-1.

```
cs7 mlr result CLUSTER
pc 1-1-1 weight 5
pc 2-2-2 weight 1
pc 3-3-3 weight 0

cs7 mlr ruleset SRISM gsm-map
rule 10 sri-sm
dest-sme 9191112222
result group CLUSTER
rule 20 sri-sm default
result pc 1-3-1
```

```
cs7 mlr table SMS-BLOCKING
trigger cdpa gt 44444 tt 10 ruleset SRISM
```

Example of Routing with B-Address Binding

MLR with Dynamic B-Address Binding

The following example shows a configuration in which MLR uses dynamic B-address binding to select a result for a set of SMS-MO messages. The dest-sme-binding mode uses a weighted distribution algorithm which binds a set of B-addresses to the same available result.

```
cs7 instance 0 mlr result MLR-BIND mode dest-sme-binding
pc 5.5.3 order 100 weight 20
pc 1.5.6 order 200 weight 40
pc 5.5.5 order 300 weight 15
pc 5.5.6 order 400 weight 60
!
cs7 instance 0 mlr address-table MLR-ADDRS
addr 1416
addr 1800
addr 2345
addr 919
!
cs7 instance 0 mlr ruleset MLR-RULES gsm-map
rule 100 sms-mo
dest-sme-table MLR-ADDRS
result group MLR-BIND
!
cs7 instance 0 mlr table MLR-TBL
trigger default ruleset MLR-RULES
```

Configuration Example of Address Modification

The following example illustrates how to use the MLR SRI-SM address modification enhancement. Rule 10 indicates that MLR should modify both the SCCP CgPA and MAP Service Center Address fields. The MSU is then routed by MLR toward the original SCCP CdPA, which may include a local GT translation being performed by ITP.

```
cs7 variant itu
cs7 point-code 1-1-1

cs7 gtt selector e164 tt 0 gti 4 np 1 nai 4
gta 397777777 pcssn 3-1-1 gt
gta 351777777 pcssn 3-1-1 gt

cs7 mlr modify-profile gsm-map SRISM sri-sm
orig-smsc prefix 2 351
cgpa gt prefix 2 351

cs7 mlr ruleset FROM_MMSC
rule 10 sri-sm default
orig-smsc 397777777
modify-profile SRISM
result route
!
cs7 mlr table SMS
trigger cdpa gt 351777777 tt 0 gti 4 np 1 nai 4 result gt 397777777 tt 0 gti 4 np 1 nai
4
```

```
trigger cgpa gt 3977777777 tt 0 gti 4 np 1 nai 4 ruleset FROM_MMSC
```


How to Configure Packet Address Modification (PAM)

PAM is a general purpose mechanism to modify SCCP and MTP Header addresses. It is similar to the modify-profile MLR feature, but applies to all Cisco ITP supported MSU types.

PAM can modify these packet address fields:

- Originating Point Code (OPC)
- Destination Point Code (DPC)
- Calling Party Address (CgPA)
- Called Party Address (CdPA)
- Address Modification Points

These packet address fields can be modified at the following points:

- The point of ingress after GWS screening
- The point of egress after GWS screening
- MLR modify-profile operations
- GTT operations (as part of post-GTT address conversion)

PAM CdPA and CgPA Modifications

CdPA and CgPA modification includes support for inserting a point code (PC) and subsystem number (SSN), as well as modifying the existing GT information, PC, and SSN. The CdPA and CgPA routing indicator (RI) is unchanged during these modifications. The PC and the SSN may be inserted or modified regardless of the RI.

The GT information that can be modified includes the GT address digits, the GT translation type (tt), the global title indicator (gti), the numbering plan (np), and the nature of address indicator (nai).

**Note**

Modifications of these parameters are allowed only when RI is set to GT. Otherwise, they are ignored.

For prefix-based GT address translation, you can configure the number of prefix digits to be removed from the address and the digit string that should be prefixed to the address. Specifying a wildcard (*) for the number of prefix digits indicates that no digits will be removed. Specifying a wildcard (*) for the digit string indicates that no prefix digits are added to the address string. If the resulting modified address exceeds the maximum allowed number of digits, then PAM fails the modification and discards the packet by default. You can optionally configure the preferred action for failed modifications using the modify-failure command within PAM submode.

If the number of digits in the modified address is less than 1 digit or more than 30 digits, the address modification cannot be performed. In this case, the action taken is based on the configured modify-failure option. By default, the packet is discarded if it cannot be modified as specified.

The CdPA and CgPA routing indicator (RI) is unchanged during these modifications.

**Note**

Take care when applying PAM to send traffic and response messages in the desired direction. For instance, if a UDTs packet is generated in response to UDT with routing indicator "Route on GT," GTT must be properly configured to route UDTs towards the desired node.

PAM in GWS

PAM can operate through GWS inbound and outbound screening. Using a configured GWS rule, a PAM modify-profile can change the packet header address. After the modification by PAM, the packet can be routed out or sent to the MLR/SCCP layer according to the result of the GWS action set. To learn more about GWS action sets, see [“Defining GWS Action Sets” section on page 180](#).

PAM in MLR

PAM can also operate through MLR functionality in a manner similar to the MLR modify profile feature. When PAM is defined in an MLR rule, the PAM can modify the packet address. To learn more about the MLR modify profile feature and MLR rules, see the [“How to Configure MLR-Based Routing” section on page 205](#).

PAM Modify Failure

If any error occurs during the modification of packets by PAM, a modify failure behavior can be selected with the configuration of the PAM's **modify-failure** command.

PAM Limitations

Cisco ITP supports a maximum of 100 PAM tables.

PAM does not support the following:

- Instance conversion, variant conversion, or screening on virtual linksets
- SMS rule reference PAM
- PAM in GWS for SGMP AS
- The following modifications are also not supported:
 - MTP Service Indicator (SI), Message Priority, SLS
 - M3UA network appearance
 - SUA Address Indicator
 - SCCP Routing indicator, SCCP/SUA Protocol Class

Configuring PAM



Note

The MLR modify-profile and PAM cannot be configured simultaneously.

To define a PAM, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cs7 instance** *instance-number* **pam** *pam-name*
4. **cgpa** [**gt** [**prefix** {*prefix-remove-num* | *}]{*prefix-add-digits* | *}] [**tt** *tt*] [**gti** {2 | 4 **np** *np* **nai** *nai*}] [**pc** *pc*] [**ssn** *ssn*]
5. **cdpa** [**gt** [**prefix** {*prefix-remove-num* | *}]{*prefix-add-digits*|*}] [**tt** *tt*] [**gti** {2 | 4 **np** *np* **nai** *nai*}] [**pc** *pc*] [**ssn** *ssn*]
6. **dpc** *point-code*
7. **opc** *point-code*
8. **modify-failure** {**discard** | **resume** | **sccp-error** *sccp-error*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables higher privilege levels, such as privileged EXEC mode.
	Example: ITP> enable	Enter your password if prompted.
Step 2	configure terminal	Enters global configuration mode.
	Example: ITP# configure terminal	
Step 3	cs7 instance <i>instance-number</i> pam <i>pam-name</i>	Identifies a PAM table and enters the CS7 PAM submode.
	Example: ITP(config)# cs7 instance 0 pam alpha	<i>pam-name</i> Creates the PAM table name. The name is specified as an alpha-numeric character string with a maximum of 12 characters.

Step 4

Command or Action	Purpose
cgpa [gt [prefix { <i>prefix-remove-num</i> *}{ <i>prefix-add-digits</i> *}]] [tt <i>tt</i>] [gti {2 4 np <i>np</i> nai <i>nai</i> }] [pc <i>pc</i>] [ssn <i>ssn</i>] Example: <pre>ITP(config-pam-table)# cgpa gt prefix tt 0 pc 1.2.3 ssn 12</pre>	Configures a calling party address (cgpa) entry in the PAM table. gt—Indicates global title information to modify. prefix—Performs prefix modification on the address. <i>prefix-remove-num</i>—An integer in the range from 1 to 15 that defines the number of prefix digits to remove from the address. If no prefix digits are to be removed, then specify a wildcard (*). Only GTAs with fewer than 16 digits can be replaced. <i>prefix-add-digits</i>—A string of 1 to 15 hexadecimal digits which are to be added to the beginning of the address. The string is input in normal form (not BCD-string format). If no digits are added, then "*" should be specified in this field. If the number of digits in the modified address would exceed the 30 digits, then the address modification cannot be performed. In this failure case, the action taken is based on the configured modify-failure parameter. By default, the packet is discarded. tt—Indicates the global title translation type (tt) for the modified CgPA. <i>tt</i>—Integer from 0 to 255 that replaces the existing <i>tt</i> value. gti—Identifies the global title indicator value for the modified cgpa. This value is used only when the cs7 variant command specifies ITU or China. <i>gti</i>—Integer value of 2 or 4. np—Identifies the global title numbering plan. <i>np</i>—Integer value from 0 to 15. nai—Identifies the global title nature of address indicator for the modified cgpa. Specified only when <i>gti</i> is 4. <i>nai</i>—Integer value from 0 to 127. pc—Identifies the point code for the modified cgpa. <i>pc</i>—Point code in variant-specific point code format. ssn—Identifies the subsystem number for the modified cgpa. <i>ssn</i>—Subsystem number in decimal. Valid range is 2 to 255.

	Command or Action	Purpose
Step 5	cdpa [gt [prefix {<i>prefix-remove-num</i> *}{<i>prefix-add-digits</i> *}][tt <i>tt</i>] [gti {2 4 np <i>np</i> nai <i>nai</i>}]] [pc <i>pc</i>] [ssn <i>ssn</i>] Example: <pre>ITP(config-pam-table)# cdpa gt prefix 15 123456789abcdef tt 250 gti 4 np 15 nai 127 pc 1.123.4 ssn 255\n</pre>	Configures a called party address (cdpa) entry in the PAM table. gt—Indicates global title information to modify. prefix—Performs prefix modification on the address. <i>prefix-remove-num</i>—An integer in the range from 1 to 15 that defines the number of prefix digits to remove from the address. If no prefix digits are to be removed, then specify a wildcard (*). Only GTAs with fewer than 16 digits can be replaced. <i>prefix-add-digits</i>—A string of 1 to 15 hexadecimal digits which are to be added to the beginning of the address. The string is input in normal form (not BCD-string format). If no digits are added, then "*" should be specified in this field. If the number of digits in the modified address would exceed the 30 digits, then the address modification cannot be performed. In this failure case, the action taken is based on the configured modify-failure parameter. By default, the packet is discarded. tt—Indicates the global title translation type (tt) for the modified CgPA. <i>tt</i>—Integer from 0 to 255 that replaces the existing <i>tt</i> value. gti—Identifies the global title indicator value for the modified cgpa. This value is used only when the cs7 variant command specifies ITU or China. <i>gti</i>—Integer value of 2 or 4. np—Identifies the global title numbering plan. <i>np</i>—Integer value from 0 to 15. nai—Identifies the global title nature of address indicator for the modified cgpa. Specified only when <i>gti</i> is 4. <i>nai</i>—Integer value from 0 to 127. pc—Identifies the point code for the modified cgpa. <i>pc</i>—Point code in variant-specific point code format. ssn—Identifies the subsystem number for the modified cgpa. <i>ssn</i>—Subsystem number in decimal. Valid range is 2 to 255.
Step 6	dpc <i>point-code</i> Example: <pre>dpc 2.3.4</pre>	Configures a destination point code (DPC) entry in the PAM table.

	Command or Action	Purpose
Step 7	opc point-code Example: opc 1.2.3	Configures an origination point code (OPC) entry in the PAM table.
Step 8	modify-failure {discard resume sccp-error sccp-error} Example: modify-failure resume	Specifies the desired action when the PAM table packet modification fails.

Configuration Examples of PAM

The following example shows a configuration for the PAM table pam1:

```
cs7 instance 0 pam pam1
  cgpa gt prefix tt 0 pc 1.2.3 ssn 12
  cdpa gt prefix 15 123456789abcdef tt 250 gti 4 np 15 nai 127 pc 1.123.4 ssn 255\n
  opc 1.2.3
  dpc 2.3.4
  modify-failure resume
```

The following example shows how to configure a GTA pcssn entry that refers to a PAM table named pam1:

```
cs7 instance 1 gtt selector test1 tt 0 gti 2
  gta 123 pcssn 1.2.3 gt pam pam1
```

The following example shows how to configure separate GTA asname entries that refer respectively to PAM tables named pam2 and pam3:

```
cs7 instance 1 gtt selector test1 tt 0 gti 2
  gta 124 asname as1 gt pam pam2
  gta default asname as2 gt pam pam3
```



IP Security

Note

Configuration Mode Restrictions: Simultaneous changes to the configuration from multiple CLI sessions are not supported. Only one configuration session is allowed to enter in configuration mode at a time; other sessions should not enter in configuration mode. The **show line** or **show users EXEC** command may be used to determine the active user sessions on an ITP, and the **clear line EXEC** command may be used to ensure that only a single active session exists.

Note

Cisco ITP supports IP Security (IPSec) and Secure Shell (SSH) only on the Cisco 2800 Series routers.

Feature History for IPSec

Release	Modification
12.4(11)SW	Feature introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Information About IPSec, page 265](#)
- [How to Configure IPSec, page 266](#)
- [Configuration Examples for IPSec, page 269](#)

Information About IPSec

IPSec is a framework of open standards developed by the Internet Engineering Task Force (IETF). IPSec provides security for transmission of sensitive information over unprotected networks such as the Internet. IPSec acts at the network layer, protecting and authenticating IP packets between participating IPSec devices (peers), such as Cisco routers.

ITP IPSec support does not introduce any new commands. For more information regarding IPSec, refer to the “Configuring IPSec Network Security” chapter and the “IPSec Network Security Commands” chapter of the *Cisco IOS Security Command Reference*.

How to Configure IPSec

The following sections describe how to configure IPSec between the ITP and another IP address, and then run an SCTP link over IPSec.

- [Create an IPSEC Tunnel, page 266](#)
- [Configure a CS7 Peer Link over the Tunnel, page 269](#)

Create an IPSEC Tunnel

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp policy**
4. **encryption**
5. **hash**
6. **authentication**
7. **exit**
8. **crypto isakmp key**
9. **crypto ipsec transform-set**
10. **crypto map**
11. **set peer**
12. **set transform-set**
13. **match address**
14. **exit**
15. **interface**
16. **ip address**
17. **crypto map**
18. **exit**
19. **access-list**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto isakmp policy Example: Router(config)# crypto isakmp policy 1	Defines an Internet Key Exchange (IKE) policy and enables ISAKMP policy configuration mode.
Step 4	encryption Example: Router(config-isakmp)# encryption 3des	Specifies the encryption algorithm within an IKE policy.
Step 5	hash Example: Router(config-isakmp)# hash md5	Specifies the hash algorithm within an IKE policy.
Step 6	authentication Example: Router(config-isakmp)# authentication pre-share	Specifies the authentication method within an IKE policy.
Step 7	exit Example: Router(config-isakmp)# exit	Exits ISAKMP policy configuration mode and enables global configuration mode.
Step 8	crypto isakmp key Example: Router(config)# crypto isakmp key cisco_123 address 10.2.1.2	Configures a preshared authentication key.
Step 9	crypto ipsec transform-set Example: Router(config)# crypto ipsec transform-set to_vpn esp-3des esp-md5-hmac	Defines a transform set—an acceptable combination of security protocols and algorithms.
Step 10	crypto map Example: Router(config)# crypto map to_vpn 10 ipsec-isakmp	Configures IKE extended authentication (Xauth) on the router.

	Command or Action	Purpose
Step 11	set peer Example: Router(config-crypto-map)# set peer 10.2.1.2	Specifies an IP Security peer in a crypto map entry.
Step 12	set transform-set Example: Router(config-crypto-map)# set transform-set to_vpn	Specifies which transform sets can be used with the crypto map entry.
Step 13	match address Example: Router(config-crypto-map)# match address 101	Specifies an extended access list for a crypto map entry.
Step 14	exit Example: Router(config-crypto-map)# exit	Exits to Global configuration mode.
Step 15	interface Example: Router(config)# interface FastEthernet0/0	Configures the interface and enable Interface configuration mode.
Step 16	ip address Example: Router(config-if)# ip address 10.1.3.1 255.255.255.0	Specifies an IP address.
Step 17	crypto map Example: Router(config-if)# crypto map to_vpn	Assigns a crypto map set to the interface.
Step 18	exit	Exits to Global configuration mode.
Step 19	access-list Example: Router(config)# access-list 101 permit ip 10.1.3.0 0.0.0.255 10.2.1.0 0.0.0.255 Router(config)# access-list 101 permit ip 10.2.1.0 0.0.0.255 10.1.3.0 0.0.0.255	Configures an access list.

What to Do Next

Configure a CS7 peer link over the tunnel you created.

Configure a CS7 Peer Link over the Tunnel

SUMMARY STEPS

1. **cs7 local-peer**
2. **local-ip**
3. **exit**
4. **cs7 linkset**
5. **link**

DETAILED STEPS

	Command or Action	Purpose
Step 1	cs7 local-peer Example: Router(config)# cs7 local-peer 5000	Specifies the local peer and enables CS7 local peer mode.
Step 2	local-ip Example: Router(config-cs7-lp)# local-ip 10.1.3.1	Configures the IP address for this local peer instance.
Step 3	exit	Exits to global configuration mode.
Step 4	cs7 linkset Example: Router(config)# cs7 linkset dasher 3.3.3	Specifies a linkset to an adjacent node and enables linkset configuration mode.
Step 5	link Example: Router(config-cs7-ls)# link 0 sctp 10.2.1.2 5000 5000	Configures an SS7 link within a linkset and enables CS7 link configuration mode.

Configuration Examples for IPsec

The following example configures IPSEC between the ITP and another IP address, then runs an SCTP link over IPSEC.

First use the Cisco IPSEC commands to create an IPSEC tunnel from the router's IP address 10.1.3.1 to IP address 10.2.1.2:

```
crypto isakmp policy 1
  encr 3des
  hash md5
  authentication pre-share
crypto isakmp key cisco123 address 10.2.1.2

crypto ipsec transform-set to_vpn esp-3des esp-md5-hmac

crypto map to_vpn 10 ipsec-isakmp
```

```
set peer 10.2.1.2
set transform-set to_vpn
match address 101

interface FastEthernet0/0
ip address 10.1.3.1 255.255.255.0
duplex auto
speed auto
crypto map to_vpn

access-list 101 permit ip 10.1.3.0 0.0.0.255 10.2.1.0 0.0.0.255
access-list 101 permit ip 10.2.1.0 0.0.0.255 10.1.3.0 0.0.0.255
```

Next, configure a CS7 peer link over the tunnel:

```
cs7 local-peer 5000
local-ip 10.1.3.1

cs7 linkset dasher 3.3.3
link 0 sctp 10.2.1.2 5000 5000
```



MAP Proxy: GSM Authentication Service MMSC Gateway Service



Note

Configuration Mode Restrictions: Simultaneous changes to the configuration from multiple CLI sessions are not supported. Only one configuration session is allowed to enter in configuration mode at a time; other sessions should not enter in configuration mode. The **show line** or **show users EXEC** command may be used to determine the active user sessions on an ITP, and the **clear line EXEC** command may be used to ensure that only a single active session exists.

The MAP Proxy feature delivers Mobile Application Part (MAP) functionality.

Feature History for MAP Proxy

Release	Modification
12.4(11)SW	Feature introduced
12.4(15)SW	SIP MAP Gateway

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Information About MAP Proxy, page 272](#)
- [How to Configure MAP Proxy, page 274](#)

Information About MAP Proxy

The Mobile Application Part (MAP) layer of the SS7 protocol suite provides mobility procedures to SS7 network applications. The MAP layer includes protocol details that support mobility functions such as registration, authentication, and call completion while providing service transparency to roaming subscribers.

The Cisco ITP MAP Proxy feature delivers MAP functionality by exporting a MAP User API (MAPUA). The MAPUA provides an interface between IP-based servers and SS7-based cellular wireless network nodes such as HLRs, VLRs, etc.

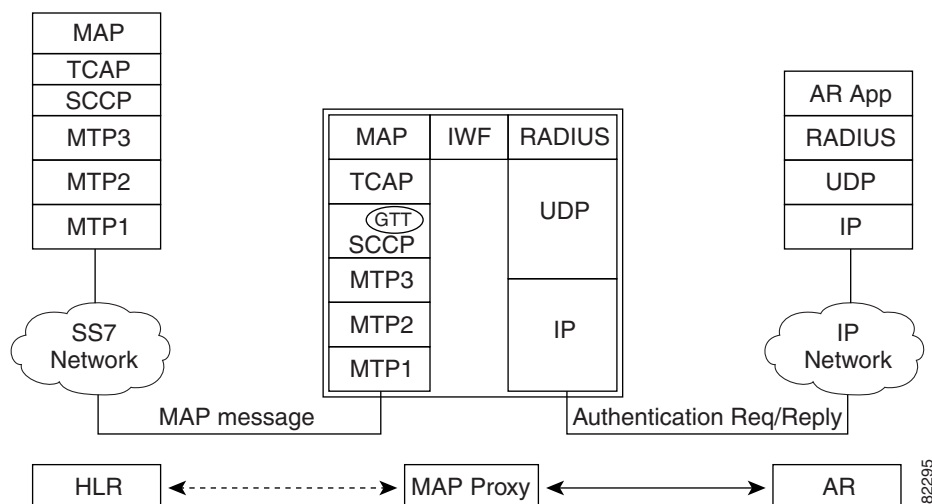
The MAP proxy feature enables the development of IP-based application servers (AS) without the need to develop SS7 layers on the AS platform. The AS platform needs only to implement the remote MAPUA appropriate for the application (the required MAP procedure.) The ITP terminates or translates all SS7 events and sends the translated event or the MAP reply data to the remote AS over the MAPUA.

GSM MAP Authentication

The initial release of MAPUA supports a non-standard interface using the RADIUS protocol for performing the GSM MAP authentication service on behalf of a Cisco Access Registrar (AR). As an option, authorization check can be turned on during the authentication procedure. To authorize a subscriber the ITP currently invokes the MAP_RESTORE_DATA service. The subscriber profile obtained from the HLR is examined for the presence of a predetermined bearer service or teleservice. If authorization fails then no authentication triplets are returned to the AR. [Figure 33](#) depicts the protocol layers in this implementation.

[Figure 33](#) represents a scenario in which an AS requests HLR information through the MAP Proxy. The AR uses the MAPUA to request authentication triplets for a particular IMSI. The interworking function (IWF) on the MAP Proxy receives the request and initiates the appropriate MAP procedure. If the request cannot be satisfied using cached information, then a request is sent to the HLR using MAP/TCAP. (An SS7 transport is depicted in this scenario, but the transport could also be through SS7 over IP protocols such as M2PA, M3UA, or SUA.)

Figure 33 Protocol Layers for GSM MAP Authentication Service



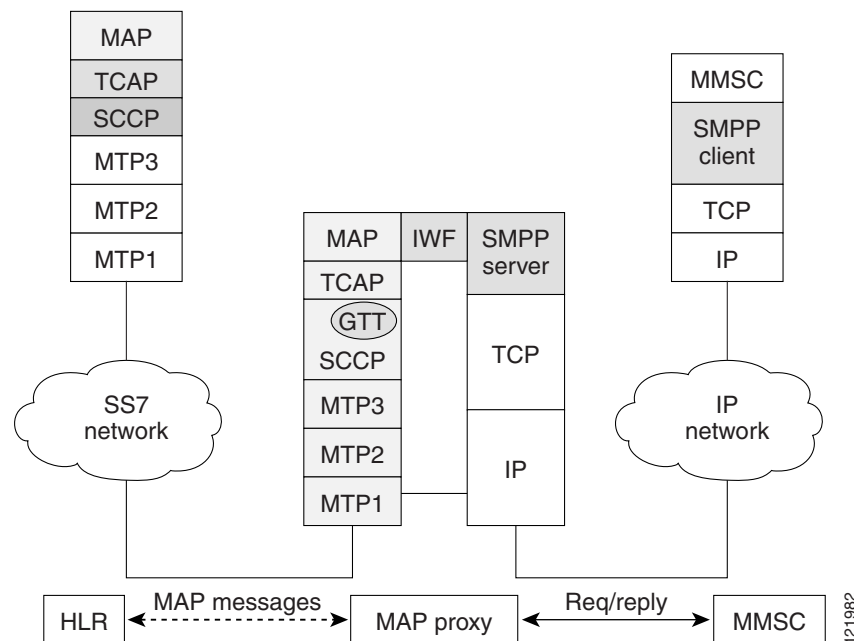
Multimedia Message Service Center Gateway

In IOS Software Release 12.2(25)SW, the MAP Proxy implementing a remote MAPUA provides a Short Message Peer to Peer (SMPP) interface for IP-based multimedia message service centers (MMSC) to exchange information with SS7-based cellular wireless network nodes. This implementation exports a MAPUA that also supports the GSM MAP-based SendIMSI, SendRoutingInfoForSM (SRISM), and SendRoutingInformation (SRI) procedures to support an MMSC Gateway service.

Figure 34 depicts the protocol layers used to support the MMSC Gateway service. The MMSC requests mobile station information from an HLR through the MAP Proxy. The MMSC uses the SMPP to send a request. The interworking function (IWF) on the MAP Proxy receives the request and initiates the appropriate MAP procedure. A SendIMSI, SendRoutingInfoForSM, or SendRoutingInfo request is sent to the HLR using MAP/TCAP. (An SS7 transport is depicted in this figure, but the transport to the HLR may also be through SS7 over IP protocols such as M2PA, M3UA or SUA.)

The MMSC Gateway feature allows FDA SMSC, M3UA, SUA, M2PA, MTP2, and HSL concurrent operation in any combination. Traffic may flow from one component to any of the other components. Components are unaware of the origin of the traffic. All MSUs appear to be from the SS7 network.

Figure 34 Protocol Layers for the MMSC Gateway



PGW SIP MAP Gateway

The PGW SIP MAP Gateway feature provides a Gateway MSC MAP proxy service that supports SUMMA PGW-SIP routing optimization. The Gateway MSC MAP proxy service occurs when a SIP INVITE message is received from PGW with a proprietary username, which is specified within the route header. A MAP User API (MAPUA) supports the GSM SendRoutingInfo procedures and then queries the requested information from the HLR subsystem and returns the MSRN routing information to PGW via the contact header in a SIP 302 response.

How to Configure MAP Proxy

This section describes the following tasks:

- [Performing Basic ITP Configuration, page 274](#)
- [Implementing a GSM MAP Authentication Service, page 274](#)
- [Implementing a PGW SIP MAP Gateway, page 277](#)
- [Implementing an MMSC Gateway Service, page 282](#)
- [Provisioning MAP Proxy Parameters for An MMSC Gateway Service, page 284](#)
- [Enabling and Disabling MAPUA, page 285](#)

Performing Basic ITP Configuration



Note

The following configuration task includes basic ITP configuration, which is described fully in the “[Configuring ITP Basic Functionality](#)” chapter. If you are unfamiliar with ITP basic configuration, you are advised to refer to that chapter for more details.

To perform the minimum basic ITP configuration, use the following commands in global configuration mode:

	Command	Purpose
Step 1	cs7 variant {ansi itu china ttc}	Specifies which SS7 variant the ITP is running.
	Example: ITP(config)# cs7 variant ansi	
Step 2	cs7 point-code point-code	Specifies the point code representation.
	Example: ITP(config)# cs7 point-code 5.3.5	

Implementing a GSM MAP Authentication Service

SUMMARY STEPS

1. **cs7 mapua** name protocol local-port
2. **local-ip** local-ip
3. **client** remote-ip [port remote-port] [encryption-off] secret {0 | 7 | LINE} shared-secret
4. **map-source-addr** [use {national | international}] digits digit-string [tt tt gti {2 | 4 np np nai nai}]
5. **map-dest-addr** [use {national | international}] tt tt gti {2 | 4 np np nai nai}

Detailed Steps

	Command	Purpose
Step 1	cs7 mapua <i>name protocol local-port</i> Example: <pre>ITP(config)# cs7 mapua rad2000 radius 2000</pre>	Specifies the name, local port number, and protocol, and enables the CS7 MAPUA configuration submode. The name must be a character string with a maximum of 12 characters and must be unique among all MAPUA instances. The protocol must be radius. The local port is the local port number that the MAP Proxy will listen to on the specified protocol. You can configure a local port number in the range 1024 through 65535.
Step 2	local-ip <i>local-ip</i> Example: <pre>Router(config-cs7-mapua)# local-ip 4.4.4.4</pre>	Specifies the local IP addresses that will receive MAPUA packets. You can repeat this command for a total of 4 local IP addresses.
Step 3	client <i>remote-ip</i> [port <i>remote-port</i>] [encryption-off] secret { 0 7 LINE } <i>shared-secret</i> Example: <pre>Router(config-cs7-mapua)# client 2.2.2.2 secret client2222</pre>	Specifies the clients that are allowed by the MAP Proxy. The source IP address within the MAPUA client request is used to match the client IP address you specify here. You may specify the remote port of the MAPUA client. If you do not specify the remote port, the client may connect using any valid port number. You must specify a shared secret string (as specified by the RADIUS protocol) to authenticate the MAPUA client. You must also specify whether the shared secret is unencrypted or encrypted (7). You may use the optional keyword encryption-off to specify that MAP Proxy RADIUS packets are not encrypted.

	Command	Purpose
Step 4	map-source-addr [use { national international }] digits <i>digit-string</i> [tt <i>tt</i> gti { 2 4 <i>np np nai nai</i> }] Example: Router(config-cs7-mapua)# map-source-addr digits 1234567890 tt 9 gti 2	Provision a global title address, such as an E.164 address, to be used as the calling party address for all MAP-generated messages. If no address is specified, then the calling party address will contain the MAP Proxy's point code and VLR subsystem number. You must specify a digit string of 1 - 15 hexadecimal digits to represent the MAP Proxy. You may specify the translation type of the address specified in the digits parameter. The type determines the translation-type used in the global title representing the MAP Proxy. Typical values would be 9 (for IMSI), 14 (for MSISDN), or 10 (for network element without number portability). The valid types are in the range 0 through 255. You may also provisions the attributes of the destination global title address that represents the subscriber's IMSI. If not specified, the variant-specific address attributes for an IMSI are used.
Step 5	map-dest-addr [use { national international }] tt <i>tt</i> gti { 2 4 <i>np np nai nai</i> } Example: Router(config-cs7-mapua)# map-dest-addr tt 10 gti 2	Specifies the destination address parameters.

Implementing a PGW SIP MAP Gateway

SUMMARY STEPS

1. **cs7 variant** {ansi | itu | china | ttc}
2. **cs7 point-code** *point-code*
3. **cs7 mapua** *name* {radius [port] | smpp [port] | sip}
4. **client** *remote_ip*
5. **map-source-addr** [use {national | international}] **digits** *str* [**tt** *tt* | **gti** *gti* [**np** *np* **nai** *nai*]]
6. **map-dest-addr** [use {national | international}] [**tt** *tt* | **gti** *gti* [**np** *np* **nai** *nai*]]
7. **gsm-send-routing-info** [version *n*]
8. **shutdown**

Detailed Steps

	Command	Purpose
Step 1	cs7 variant {ansi itu china ttc} Example: ITP(config)# cs7 variant ansi	Specifies which SS7 version the ITP is running.
Step 2	cs7 point-code <i>point-code</i> Example: ITP(config)# cs7 point-code 5.3.5	Specifies the point code representation for the router.

Step 3	cs7 mapua <i>name</i> { radius [port] smpp [port] sip }	Allows the user to specify the name, local port number and protocol for the MAP Gateway feature. Only one MAPUA local port may be configured for the ITP router. For SIP MAP GW, local port can't be configured but using fixed 5060, this port should be used by SIP MAP GW exclusively. The no form of this command will delete the cs7 mapua command, and disable the MAP Gateway feature. The <i>name</i> identifies a name to be associated with this MAP User API instance. The name must be unique among all MAP User API instances. Initially, only a single MAPUA instance will be allowed. The name is specified as a character string with a maximum of 12 characters. sip specifies that the user protocol for this interface is SIP. This protocol is added for SIP MAP gateway usage. The only supported value for the SIP MAP GW is 'sip'. The SIP MAP GW will use the default port 5060 as listening port, the local port can't be configured. Note This command also enables the mapua configuration submode.
Step 4	client <i>remote_ip</i>	client allows the user to configure the list of clients which are allowed by the MAP Proxy. If no clients are specified, then no MAPUA client requests are processed. <i>remote_ip</i> is the client's remote IP address. The source IP address within the MAPUA client request is used to match this specified client IP address. The NAS-IP-Address attribute is not used.

Step 5	map-source-addr [use { national international }] digits <i>str</i> [tt <i>tt</i> gti <i>gti</i> [np <i>np</i> nai <i>nai</i>]]	Allows the user to provision a global title address, such as an E.164 address, to be used as the calling party address for all MAP-generated messages. use specifies national or international use bit in address indicator. national specifies national use bit in address indicator. international specifies international use bit in address indicator. digits is the 1-15 digit string representing the MAP Proxy. For the Chinese and ITU variants, the digit string will represent an E.164 address type. <i>str</i> is the local address digit string coded in hexadecimal. The tt parameter specifies the Translation Type of the address specified in the digits parameter. This parameter is optional, and is required when the variant is ANSI. The type determines the translation-type used in the global title representing the MAP Proxy. Typical values would be 9 (for IMSI), 14 (for MSISDN) or 10 (for Network Element without number portability). <i>tt</i> is the valid translation types are specified in the range 0-255. gti with a <i>gti</i> value of 2 indicates that only Translation Type (<i>tt</i>) will be used in the source address. The value <i>gti</i> equals to 4 indicates that the Translation Type, Numbering Plan (<i>np</i>) and Nature of Address Indicator (<i>nai</i>) will all be used in the source address. <i>gti</i> is the variable for the valid Global Title Indicator values are 2 and 4. When the np <i>np</i> variable is 4, Numbering Plan (<i>np</i>) and Nature of Address Indicator (<i>nai</i>) are required. <i>np</i> is the numbering plan with value in the range 0 to 15. nai is the nature of the address indicator. <i>nai</i> is the nai value in the range 0 to 127.

Step 6	map-dest-addr [use { national international }] [tt <i>tt</i> gti <i>gti</i> [np <i>np</i> nai <i>nai</i>]]	Allows the user to provision a global title address, such as an E.164 address, to be used as the calling party address for all MAP-generated messages use specifies national or international use bit in address indicator. national specifies national use bit in address indicator. international specifies international use bit in address indicator. digits is the 1-15 digit string representing the MAP Proxy. For the Chinese and ITU variants, the digit string will represent an E.164 address type. <i>str</i> is the local address digit string coded in hexadecimal. The tt parameter specifies the Translation Type of the address specified in the digits parameter. This parameter is optional, and is required when the variant is ANSI. The type determines the translation-type used in the global title representing the MAP Proxy. Typical values would be 9 (for IMSI), 14 (for MSISDN) or 10 (for Network Element without number portability). <i>tt</i> is the valid translation types are specified in the range 0-255. gti with a <i>gti</i> value of 2 indicates that only Translation Type (<i>tt</i>) will be used in the source address. The value <i>gti</i> equals to 4 indicates that the Translation Type, Numbering Plan (<i>np</i>) and Nature of Address Indicator (<i>nai</i>) will all be used in the source address. <i>gti</i> is the variable for the valid Global Title Indicator values are 2 and 4. When the np <i>np</i> variable is 4, Numbering Plan (<i>np</i>) and Nature of Address Indicator (<i>nai</i>) are required. <i>np</i> is the numbering plan with value in the range 0 to 15. nai is the nature of the address indicator. <i>nai</i> is the nai value in the range 0 to 127.
Step 7	gsm-send-routing-info [version <i>n</i>]	Allow the user to provision parameters specific to the GSM MAP Send Routing Information procedure. If not specified, the default behavior described under each parameter is applied. The gsm-send-routing-info command opens a submode for specification of individual parameters. version allows the MAP version of the outbound SRI to be specified. If not specified, the default version will be set to 3. <i>n</i> is the integer value in the range of 1 to 3.
Step 8	shutdown	(Optional) Disables the MAPUA on this MAP Proxy ITP router. This command will terminate MAPUA from listening on the specified port and protocol.

Example

The following example specifies the implementation of a PGW SIP MAP Gateway.

```
cs7 variant ITU
cs7 point-code 5.5.1
cs7 mapua sip1 sip
client 10.0.133.181
client 10.0.133.201
map-source-addr digits 86139123456
gsm-send-routing-info version 3
```

Provisioning MAP Proxy Parameters for GSM MAP Authentication Service

To enter the submode to provision parameters specific to the GSM MAP Process_Obtain_Authentication_Sets_VLR service, use the following commands, beginning in CS7 MAPUA submode:

	Command	Purpose
Step 1	gsm-authent-vlr Example: Router(config-cs7-mapua)# gsm-authent-vlr	Enables the authent-vlr submode, in which you can provision parameters.
Step 2	authorize { bs <i>bs-number</i> ts <i>ts-number</i> } Example: Router(config-cs7-mapua-gsm-authent-vlr)# authorize bs 26	Specifies that authorization of the IMSI must be performed by accessing the subscriber's profile stored in the HLR.
Step 3	cache-size <i>cache-size</i> Example: Router(config-cs7-mapua-gsm-authent-vlr)# cache-size 1024	Specifies the total number of IMSIs for which authentication triplets will be cached. A maximum of 5 triplets are stored per IMSI, and the default cache size is 65535. If the value 0 is specified, caching is disabled. If the cache-size is not configured, the default value is 65535.
Step 4	max-return <i>return-size</i> Example: Router(config-cs7-mapua-gsm-authent-vlr)# max-return 2	Specifies the maximum number of authentication triplets that may be returned to a MAPUA client for a single request. This command allows you to override the number of requested triplets specified by the client (e.g, AR) in order to optimize caching in the system. If not specified, the return size default is 5, but fewer triplets may be returned based on the number requested by the client and the number returned by the HLR (or stored in the cache from a previous query).
Step 5	ttl <i>time-to-live</i> Example: Router(config-cs7-mapua-gsm-authent-vlr)# ttl 10080	Specifies the amount of time, in seconds, that a cached authentication triplet will be stored. If not specified, the default is set to 604800 seconds (7 days).

	Command	Purpose
Step 6	reuse-count <i>count</i> Example: Router(config-cs7-mapua-gsm-authent-vlr)# reuse-count 3	Specifies the number of times a triplet can be reused.
Step 7	invoke-timer <i>seconds</i> Example: Router(config-cs7-mapua-gsm-authent-vlr)# invoke-timer 20	Specifies the maximum amount of time, in seconds, that the MAP Proxy will wait for a response to a sent TCAP Invoke component. The default value is 10 seconds

Example

The following example specifies a MAP Proxy configuration for a GSM MAP Authentication Service.

```
cs7 variant ansi
cs7 point-code 5.3.5

interface ethernet 0/0
 ip address 4.4.4.4 255.255.255.128

cs7 mapua rad2000 radius 2000
 local-ip 4.4.4.4
 client 1.1.1.1 secret client1111
 client 2.2.2.2 secret client2222
 client 3.3.3.3 secret client3333
 map-source-addr digits 1234567890 tt 9
 gsm-authent-vlr
  cache-size 100
  max-return 2
```

Implementing an MMSC Gateway Service

SUMMARY STEPS

1. **cs7 mapua** *name protocol local-port*
2. **local-ip** *local-ip*
3. **client** {**dynamic** | *remote-ip*}
4. **map-source-addr** [use {**national** | **international**}] **digits** *digit-string* [**tt** *tt*]
5. **map-dest-addr** [use {**national** | **international**}] [**tt** *tt*] [**gti** {**2** | **4 np np nai nai**}]
6. **get-imsi** [**include-msc**]
- or -
get-msrn [**map-version** *version*]

Detailed Steps

	Command	Purpose
Step 1	<pre>Router(config)# cs7 mapua name protocol local-port</pre> Example: <pre>ITP(config)# cs7 mapua GetIMSI smpp 9000</pre>	Specifies the name, local port number, and protocol for the MAP Proxy feature, and enables the CS7 MAPUA configuration submode. The name must be a character string with a maximum of 12 characters and must be unique among all MAPUA instances. The protocol must be smpp. The local port is the local port number that the MAP Proxy will listen to on the specified protocol. A well-known port of 9000 is used for GetIMSI requests and a well-known port of 9001 is used for GetMSRN requests.
Step 2	<pre>local-ip local-ip</pre> Example: <pre>Router(config-cs7-mapua)# local-ip 4.4.4.4</pre>	Specifies the local IP addresses that will receive SMPP packets.
Step 3	<pre>client {dynamic remote-ip}</pre> Example: <pre>Router(config-cs7-mapua)# client 1.1.1.1</pre>	Specifies the clients that are allowed by the MAP Proxy. You can specify the client's remote IP address or you can allow any client to connect. The source IP address within the MAPUA client request is used to match the client IP address you specify here. The dynamic keyword allows any client to connect.
Step 4	<pre>map-source-addr [use {national international}] digits digit-string [tt tt]</pre> Example: <pre>Router(config-cs7-mapua)# map-source-addr digits 1234567890 tt 9</pre>	Provisions a global title address, such as an E.164 address, to be used as the calling party address for all MAP-generated messages. You must specify a digit string of 1 - 15 hexadecimal digits to represent the MAP Proxy. For variant ANSI only, you may specify the translation type of the address specified in the digits parameter. The type determines the translation-type used in the global title representing the MAP Proxy. Typical values would be 9 (for IMSI), 14 (for MSISDN), or 10 (for network element without number portability). The valid types are in the range 0 through 255.

	Command	Purpose
Step 5	map-dest-addr [use { national international }] [tt <i>tt</i>] [gti { 2 4 np <i>np</i> nai <i>nai</i> }] Example: Router(config-cs7-mapua)# map-dest-addr tt 10	Specifies the destination address parameters.
Step 6	get-imsi [include-msc] -or- get-msrn [map-version <i>version</i>] Example: Router(config-cs7-mapua)# get-imsi include-msc -or- Router(config-cs7-mapua)# get-msrn map-version 3	get-imsi specifies the GetIMSI procedure and optionally includes the MSC number returned by the HLR in the GetIMSI response. get-msrn specifies the GetMSRN procedure and optionally specifies the default GSM MAP version for SendRoutingInfo MAP messages. Valid versions are in the range 1 to 3. The default is 2. For a given SMPP MAPUA, either the get-imsi or get-msrn procedure must be specified. If no procedure is specified, the SMPP requests will not be accepted from the MMSC.

Provisioning MAP Proxy Parameters for An MMSC Gateway Service

This optional task allows you provision parameters specific to the SMPP connections. If not specified, the default behavior for each parameter is applied.

	Command	Purpose
Step 1	smpp send-window <i>operations</i> Example: Router(config-cs7-mapua)# smpp send-window 40	(Optional) Specifies the maximum number of outstanding SMPP operations between an MMSC and the ITP. Valid range is 1 to 100. The default is 10 operations.
Step 2	smpp session-init-timer <i>ms</i> Example: Router(config-cs7-mapua)# smpp session-init-timer 20000	(Optional) Specifies the time lapse in milliseconds allowed between the establishment of a network connection and the establishment of the SMPP connection. Valid range is 500 to 120,000 ms. The default is 120,000 ms.
Step 3	smpp keepalive-timer <i>ms</i> Example: Router(config-cs7-mapua)# smpp keepalive-timer 5000	(Optional) Specifies the time lapse in milliseconds allowed between SMPP operations over an SMPP connection. Valid range is 0 to 600,000 ms. the default is 600,000 ms. The value 0 indicates no keepalive timer.
Step 4	smpp inactivity-timer <i>ms</i> Example: Router(config-cs7-mapua)# smpp inactivity-timer 10000	(Optional) Specifies the maximum time lapse in milliseconds allowed between transactions. Valid range is 1,000 to 9,000,000 ms. The default is 1,8000,000.
Step 5	smpp response-timer <i>ms</i> Example: Router(config-cs7-mapua)# smpp response-timer 9000	(Optional) Specifies the time lapse in milliseconds allowed between an SMPP request and the corresponding SMPP response. Valid range is 500 to 30,000 ms. The default is 5,000 ms.

Example

The following example specifies a MAP Proxy configuration for an MMSC Gateway service.

```
cs7 variant ansi
cs7 point-code 5.3.5

interface ethernet 0/0
 ip address 4.4.4.4 255.255.255.128

cs7 mapua GetIMSI smpp 9000
 local-ip 4.4.4.4
 client 1.1.1.1
 client 2.2.2.2
 client dynamic
 map-source-addr digits 1234567890 tt 9
 get-imsi include-msc
 smpp response-timer 6000
 smpp session-init-timer 3000
!
cs7 mapua GetMSRN smpp 9001
 local-ip 4.4.4.4
 client 1.1.1.1
 client 2.2.2.2
 map-source-addr digits 1234567890 tt 9
 invoke-timer 15
 get-msrn map-version 2
 smpp response-timer 2000
```

Enabling and Disabling MAPUA

To disable the MAPUA after it has been configured, or to re-enable it after it has been disabled, use one of the following commands in CS7-MAPUA submode:

	Command	Purpose
Step 1	shutdown Example: Router(config-cs7-mapua)# shutdown	Disables the MAPUA on this MAP Proxy ITP router and terminates MAPUA from listening on the specified port and protocol.
Step 2	no shutdown Example: Router(config-cs7-mapua)# no shutdown	Re-enables the MAPUA.



ITP QoS

The ITP QoS feature provides the framework that allows end-to-end Quality of Service (QoS) for SS7 packet flow through SS7 over IP (SS7oIP) networks.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



Note

Configuration Mode Restrictions: Simultaneous changes to the configuration from multiple CLI sessions are not supported. Only one configuration session is allowed to enter in configuration mode at a time; other sessions should not enter in configuration mode. The **show line** or **show users EXEC** command may be used to determine the active user sessions on an ITP, and the **clear line EXEC** command may be used to ensure that only a single active session exists.

Contents

- [Information About ITP QoS, page 287](#)
- [How to Configure ITP QoS, page 289](#)
- [Verifying ITP QoS, page 297](#)
- [QOS Configuration Example, page 299](#)

Information About ITP QoS

Quality of Service (QoS) refers to the performance of packet flow through networks. The goal in a QoS-enabled environment is to enable predictable service delivery to certain traffic classes or types regardless of other traffic flowing through the network at any given time. ITP QoS provides the framework that allows end-to-end QoS for SS7 packet flow through SS7oIP networks. End-to-end QoS is the ability of the network to deliver service required by specific network traffic from one end of the network to another. In particular, QoS features ensure improved and more predictable network service by providing the following services:

- Dedicated bandwidth

- Improving loss characteristics
- Avoiding and managing network congestion
- Shaping network traffic
- Setting traffic priorities across the network

QoS enables networks to control and predictably service a variety of network applications and traffic types. SS7 networks generally achieve QoS capabilities by over-provisioning bandwidth. Conventional SS7 networks lack the ability to identify different traffic types and provide network prioritization based on these traffic types. For instance, SS7 networks cannot separate ISUP and SCCP traffic and route this traffic over specific output links.

ITP QoS Components

ITP QoS is based on 2 components: packet classification and packet scheduling and queuing.

Packet classification provides the capability to partition network traffic into multiple priority levels or classes of service. For instance, you can configure ITP QoS to classify incoming ISUP traffic as a member of class 1 and classify incoming SCCP traffic as a member of another class. Traffic classified by ITP QoS is directed over a specified link or a set of links. Using ITP QoS packet classification, the underlying IP network can ensure that the appropriate service level is provided to each traffic type.

Packet scheduling and queuing is concerned with implementing and policing the packet priorities through the IP network. After packets are classified as members of a QoS class and marked accordingly, the scheduling and queuing component is required to provide the appropriate network priority for the different classes of traffic. Scheduling and queuing also provides congestion management, congestion avoidance, policing, and shaping. The scheduling and queuing component of ITP QoS is provided by Cisco IOS QoS. ITP QoS depends on Cisco IOS QoS services for policing packet priority based on the IP header Type of Service (ToS) byte settings. Cisco IOS provides a rich set of QoS policies such as Weighted Fair Queuing, Class-Based Weighted Fair Queuing, Random Detection, and Traffic Shaping.

ITP QoS Functionality

ITP QoS supports the setting of the ToS byte in the IP header. The ToS byte can be set to either a 3 bit IP precedence or 6 bit Differential Services Code Point (DSCP). Identifying the QoS requirements using the ToS byte provides the core network with an efficient classification method. Each hop can then provide each packet with the required QoS. IOS QoS techniques can be applied to provide policing for packet queuing and priority.

The ITP QoS service model allows the network administrator to configure up to 8 QoS classes, numbered 0 through 7. The hierarchy within the classes is based on the network priority characteristics assigned to each QoS class. The network administrator is responsible for provisioning the network priority characteristics to each QoS class, thus establishing the QoS class hierarchy. The network priority characteristics are provisioned by assigning either an IP precedence or DSCP to a QoS class. Packets that are classified as belonging to a provisioned QoS class will have the TOS byte in the IP header set to the assigned IP precedence or DSCP.

ITP QoS designates QoS class 0 as the default class. QoS class 0 member peer links can forward two types of packets:

- Packets are not classified as members of any other provisioned QoS class
- Packets are classified as members of a provisioned QoS class, but the QoS class does not have any member peer links available.

When peer links for an unavailable QoS class becomes available, packets classified as members of that QoS class will resume forwarding using the QoS class member peer links.

Peer links within a linkset which are not assigned a QoS class are members of the default class. **ITP QoS requires at least one default class peer link member.** The default class is provisioned automatically when the first QoS class is assigned to a peer link within a linkset. The IP precedence or DSCP for QoS class 0 defaults to zero. The IP precedence or DSCP default for QoS class 0 can be modified through the command line interface configuration for QoS classes.

By configuring ITP QoS, the network administrator can assign different network priority characteristics to certain types of traffic. ITP QoS can direct selected traffic types over a specific set of QoS provisioned peer links. The network administrator identifies the peer links that are members of a QoS class. Packets that are classified as members of a given QoS class are transmitted over the QoS class peer link members. **A peer link can be a member of only one QoS class.** It is strongly recommended that a QoS class have multiple peer link members to provide alternate links in case of link failures. ITP QoS supports changeover and changeback between peer link members of the same QoS class. When a peer link member of a QoS class fails, ITP QoS attempts changeover to a peer link member of the same QoS class. If there are no peer link members of the same QoS class available, ITP QoS forwards the packets of the unavailable QoS class using the QoS class 0 peer link members. If there are no QoS class 0 peer link members available the packets are dropped. When peer links for the unavailable QoS class become available, ITP QoS performs a changeback to switch the QoS class packets from the QoS class 0 peer links back to the QoS class peer link members that became available. The changeover and changeback function is prohibited between peer link members of different QoS classes.

MTP3 management messages will use any available peer link within a linkset regardless of the QoS classes assigned to the peer links.

Upon link failure of all peer link members provisioned for a QoS class, Transfer Restricted (TFR) messages are sent to adjacent signaling points. For ITU, the ITP QoS feature enhances the ITU specification by supporting response method TFRs. When conditions are met that require the sending of ITU response method TFRs, two TFRs at 30 second intervals will be sent. The TFR transmission interval is not configurable.

Link Selection is the process of identifying the outbound link that satisfies the classification criteria and QoS class. ITP MTP3 routing incorporates packet classification and QoS capabilities in the link selection decision. When the ITP QoS feature is configured, the outbound link for classified traffic is selected based on the QoS class and slc value.

For more information about deploying Cisco IOS QoS policies, refer to the *Cisco IOS Quality of Service Solutions Configuration Guide* and the *Cisco IOS Quality of Service Solutions Command Reference*, included in the Cisco IOS Release 12.2 documentation at the following URL:
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm>

How to Configure ITP QoS

ITP allows packets to be classified (or colored) based on DPC, GTT selector, global title address, service indicator, inbound linkset and access list. MTP3 routing then incorporates the packet classification and link QoS capabilities into the link selection decision. Once an M2PA link is selected, the provisioned QoS class is assigned to an IP precedence value (TOS field) or a Differential Services Code Point (DSCP).

ITP also provides a mechanism such that traffic flows to M3UA or SUA may be assigned to different QoS classes. ITP enables the classification of packets received from M3UA or SUA to further enhance QoS routing over M2PA links.

Specifying Packet Classification

Fundamental to the ITP QoS feature is packet classification or “coloring.” Classification is the process of identifying the QoS class of a packet. Packet classification provides the capability to partition network traffic into multiple classes of service. ITP QoS provides the following methods for specifying packet classification:

- [Specifying Input Linkset Classification, page 290](#)
- [Specifying Access List Classification, page 291](#)
- [Specifying Service Indicator Classification, page 292](#)
- [Specifying SCCP Packet Classification, page 293](#)
- [Specifying Destination Point Code Classification, page 295](#)
- [Specifying a QoS classification for an ASP, page 296](#)
- [Specifying QoS Routing Over M2PA Links, page 297](#)

The input linkset, access list, and service indicator packet classification methods are mutually exclusive.

The sccp and destination point code packet classification methods can be used separately or in tandem.

The sccp and destination point code packet classification methods can be used in conjunction with the input linkset, access list, and service indicator classification methods.

When combinations of the classification methods are used, the following precedence order should be observed (highest to lowest):

1. Destination point code classification
2. SCCP packet classification (GTA)
3. SCCP packet classification (Selector Table)
4. Input linkset, access list and service indicator classification

Specifying Input Linkset Classification

ITP QoS provides the capability to classify packets based on an input linkset. The network operator can classify all packets that arrive on links within a linkset to a provisioned ITP QoS class. By this method of packet classification, all incoming packets to the linkset are classified as members of the QoS class assigned by the network operator. This method of classification provides the capability to group network traffic into a single ITP QoS class regardless of the packet destination. An example where input linkset classification would be most useful is for linksets coming from an SMSC. In this case, the network administrator can be sure all MSUs are related to the short message service and give them the appropriate priority.

To permit input linkset packet classification, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# cs7 qos class <i>class</i>	Defines a QoS class and enters QoS class configuration mode.
Step 2	Router(config-cs7-qos)# qos-ip-precedence <i>class</i>	Defines an IP precedence for the class.
Step 3	Router(config-cs7-qos)# exit	Exits CS7 QoS configuration submode, and enters global configuration mode.

	Command	Purpose
Step 4	Router(config)# cs7 linkset <i>ls-name adj-pc</i>	Specifies an input linkset and enters linkset configuration submenu.
Step 5	Router(config-cs7-ls)# match any qos-class <i>class</i>	Sets the match criteria.
Step 6	Router(config-cs7-ls)# exit	Exits CS7 linkset mode and enters global configuration mode.
Step 7	Router(config)# cs7 linkset <i>ls-name adj-pc</i>	Specifies an output linkset and enters linkset configuration submenu.
Step 8	Router(config-cs7-ls)# link <i>slc</i>	Specifies a link in the linkset and enters link configuration mode.
Step 9	Router(config-cs7-ls-link)# qos-class <i>class</i>	Assigns QoS class to link.
Step 10	Router(config-cs7-ls-link)# exit	Exits CS7 link configuration mode and enters linkset configuration mode.
Step 11	Router(config-cs7-ls)# link <i>slc</i>	Specifies a link in the linkset and enters link configuration mode. ITP QoS requires that at least one link is configured with no QoS class assigned. A link with no class is a member of the default class (class 0). QoS class 0 member links forward packets that are not classified as members of any other QoS class and packets that are classified as members of an unavailable QoS class.

Specifying Access List Classification

Access lists provide the capability to classify packets based on message characteristics. ITP access lists allow the specification of one or more match criteria to be applied to packets. Access-list numbers 2700-2999 can be used to define ITP access lists. Access-lists allow the logical AND or logical OR between specified match elements. For example, an access list can be defined to match destination point code (dpc) and originating point code (opc). Packets that meet the defined match criteria for an ITP access list are classified as members of the ITP QoS class assigned to the access list. Each QoS class that has been assigned an access list is considered for a match. The search begins with QoS class 0 and ends with QoS class 7. The first access list match terminates the search and assigns the corresponding QoS class to the outgoing packet. Complex access list definitions can be created but require more CPU resources to determine packet matches and can increase packet latency.

Access lists assigned to ITP QoS classes do not provide screening. Packets that match an ITP access list with the deny option eliminate that access list for consideration and progress to the next access list. When there are no more access lists to consider, the packet is routed over the default class peer link members.

To permit access list packet classification, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# access-list <i>access-list-number</i> { deny permit } [dpc <i>point-code wildcard-mask</i> opc <i>point-code wildcard-mask</i> si <i>si-value</i> pattern <i>offset hex-pattern</i> aftpc <i>point-code wildcard-mask</i> cdpa <i>point-code wildcard-mask</i> <i>selector</i> all]	Defines an access list.
Step 2	Router(config)# cs7 qos class <i>class</i>	Defines a QoS class and enters QoS class configuration mode.
Step 3	Router(config-cs7-qos)# qos-ip-precedence <i>class</i>	Defines the IP precedence for the class.
Step 4	Router(config-cs7-qos)# qos-access-group <i>access-list-number</i>	Assigns the access list to the QoS class.
Step 5	Router(config)# cs7 linkset <i>ls-name adj-pc</i>	Specifies an input linkset and enters linkset configuration mode.
Step 6	Router(config-cs7-ls)# match access-group	Sets the match criteria.
Step 7	Router(config)# exit	Exits linkset configuration mode and enters global configuration mode.
Step 8	Router(config)# cs7 linkset <i>ls-name adj-pc</i>	Specifies an output linkset and enters linkset configuration mode.
Step 9	Router(config-cs7-ls)# link <i>slc</i>	Specifies a link in the linkset and enters link configuration mode.
Step 10	Router(config-cs7-ls-link)# qos-class <i>class</i>	Assigns the QoS class to the link.
Step 11	Router(config-cs7-ls-link)# exit	Exits CS7 link configuration mode and enters linkset configuration mode.
Step 12	Router(config-cs7-ls)# link <i>slc</i>	Specifies a link in the linkset and enters link configuration mode. ITP QoS requires that at least one link is configured with no QoS class assigned. A link with no class is a member of the default class (class 0). QoS class 0 member links forward packets that are not classified as members of any other QoS class and packets that are classified as members of an unavailable QoS class.

Specifying Service Indicator Classification

ITP QoS provides the capability to classify packets based on the Service Indicator (SI) field. This method of classification can be used as an alternative to access-lists without the overhead associated with access-lists. This method allows a simple match criteria based on SI value. To create more complex match criteria, ITP access lists should be used. Multiple SI value match criteria can be specified per input linkset. Packets that match one of the SI match criteria are classified as a members of the corresponding QoS class. A table lookup provides fast mapping of SI values to QoS classes. An example of where QoS based on service indicator is most useful is in distinguishing ISUP from SCCP traffic. ISUP has SI value of 5 and SCCP has SI value of 3.

To permit service indicator classification, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# cs7 qos class <i>class</i>	Defines a QoS class and enters QoS class configuration mode.
Step 2	Router(config-cs7-qos)# qos-ip-precedence <i>class</i>	Defines an IP precedence for the class.
Step 3	Router(config-cs7-qos)# exit	Exits CS7 QoS configuration submode, and enters global configuration mode.
Step 4	Router(config)# cs7 qos class <i>class</i>	Defines a QoS class and enters QoS class configuration mode.
Step 5	Router(config-cs7-qos)# qos-ip-precedence <i>class</i>	Defines an IP precedence for the class.
Step 6	Router(config)# cs7 linkset <i>ls-name adj-pc</i>	Specifies an input linkset and enters linkset configuration submode.
Step 7	Router(config-cs7-ls)# match si si qos-class <i>class</i>	Sets the match criteria.
Step 8	Router(config-cs7-ls)# exit	Exits CS7 linkset mode and enters global configuration mode.
Step 9	Router(config)# cs7 linkset <i>ls-name adj-pc</i>	Specifies an output linkset and enters linkset configuration submode.
Step 10	Router(config-cs7-ls)# link <i>slc</i>	Specifies a link in the linkset and enters link configuration mode.
Step 11	Router(config-cs7-ls-link)# qos-class <i>class</i>	Assigns QoS class to link.
Step 12	Router(config-cs7-ls)# link <i>slc</i>	Specifies a link in the linkset and enters link configuration mode.
Step 13	Router(config-cs7-ls-link)# qos-class <i>class</i>	Assigns QoS class to link.
Step 14	Router(config-cs7-ls-link)# exit	Exits CS7 link configuration mode and enters linkset configuration mode.
Step 15	Router(config-cs7-ls)# link <i>slc</i>	Specifies a link in the linkset and enters link configuration mode. ITP QoS requires that at least one link is configured with no QoS class assigned. A link with no class is a member of the default class (class 0). QoS class 0 member links forward packets that are not classified as members of any other QoS class and packets that are classified as members of an unavailable QoS class.

Specifying SCCP Packet Classification

Packets that require a Global Title Translation (GTT) can be classified on a per Global Title Address (GTA) basis or on a GTT selector table. A network administrator can assign one of the 8 ITP QoS classes to each GTA/GTA mask or selector table. During GTT processing, the QoS class associated with the GTA/GTA mask or selector table will be stored in the packet header for further processing by the ITP QoS feature.

There is a precedence order when a QoS class is assigned to both a selector table and to a GTA within that selector table. If a QoS class is assigned to a selector table and a GTA entry, the QoS class assigned to the GTA entry has precedence over the QoS class assigned to the selector table.

If the QoS class assigned to a selector table or GTA entry is not configured, the SCCP packet is routed over the default class peer link members.

To permit SCCP packet classification for a GTT selector, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# cs7 qos class <i>class</i>	Defines a QoS class and enters QoS configuration submode.
Step 2	Router(config-cs7-qos)# qos-ip-precedence <i>class</i>	Defines an IP precedence for the class.
Step 3	Router(config-cs7-qos)# exit	Exits CS7 QoS configuration submode, and enters global configuration mode.
Step 4	Router(config)# cs7 qos class <i>class</i>	Defines a QoS class and enters QoS configuration submode.
Step 5	Router(config-cs7-qos)# qos-ip-precedence <i>class</i>	Defines an IP precedence for the class.
Step 6	Router(config-cs7-qos)# exit	Exits QoS configuration submode and enters global configuration mode.
Step 7	Router(config)# cs7 gtt selector <i>selector tt tt</i>	Defines the selector table and enters CS7 GTT selector mode.
Step 8	Router(config-cs7-gtt-selector)# qos-class <i>class</i>	Assigns a QoS class to the selector table.
Step 9	Router(config-cs7-gtt-selector)# gta gta qos-class <i>class pcssn pc gt ntt ntt</i>	Assigns a QoS class to the GTA entry
Step 10	Router(config-cs7-gtt-selector)# exit	Exits CS7 GTT selector mode and enters global configuration mode.
Step 11	Router(config)# cs7 linkset <i>ls-name adj-pc</i>	Specifies an output linkset and enters linkset configuration submode.
Step 12	Router(config-cs7-ls)# link <i>slc</i>	Specifies a link in the linkset and enters link configuration mode.
Step 13	Router(config-cs7-ls-link)# qos-class <i>class</i>	Assigns QoS class to link.
Step 14	Router(config-cs7-ls-link)# exit	Exits link configuration mode and enters linkset configuration mode.
Step 15	Router(config-cs7-ls)# link <i>slc</i>	Specifies a link in the linkset and enters link configuration mode.
Step 16	Router(config-cs7-ls-link)# qos-class <i>class</i>	Assigns the QoS class to the link.

	Command	Purpose
Step 17	Router(config-cs7-ls-link)# exit	Exits CS7 link configuration mode and enters linkset configuration mode.
Step 18	Router(config-cs7-ls)# link <i>slc</i>	Specifies a link in the linkset and enters link configuration mode. ITP QoS requires that at least one link is configured with no QoS class assigned. A link with no class is a member of the default class (class 0). QoS class 0 member links forward packets that are not classified as members of any other QoS class and packets that are classified as members of an unavailable QoS class.

Specifying Destination Point Code Classification

ITP QoS provides the capability to classify packets based on the destination point code (DPC). All packets destined for a given DPC will be classified as members of the QoS class that was configured with an ITP routing entry. The QoS class configured with an ITP routing entry is stored with the ITP routes in the routing table. Storing the QoS class with the routing entry provides efficient packet classification based on DPC. An example of where QoS based on point code may be used is on links coming from an MSC. Packets to SMSC and HLR will both be SCCP MSUs with service indicator 3. The DPC may be checked to determine if the MSU is for an SMSC or an HLR (after GTT if desired) and then classified accordingly.

If the QoS class assigned to a DPC is not configured, packets are routed over the default class peer link members.

To permit destination point code packet classification, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# cs7 qos class <i>class</i>	Defines a QoS class and enters QoS class configuration mode.
Step 2	Router(config-cs7-qos)# qos-ip-precedence <i>class</i>	Defines an IP precedence for the class.
Step 3	Router(config-cs7-qos)# exit	Exits CS7 QoS configuration submode, and enters global configuration mode.
Step 4	Router(config)# cs7 route-table system	Specifies the route table and enters CS7 route table configuration submode.
Step 5	Router(config-cs7-rt)# update route point-code [<i>mask</i> <i>length</i>] linkset <i>ls-name</i> [priority <i>priority-value</i> ¹] [qos-class { <i>class</i> default }] [load_balance]	Adds QoS class to the destination point code.
Step 6	Router(config-cs7-rt)# exit	Exits CS7 route table configuration submode and enters global configuration mode.
Step 7	Router(config)# cs7 linkset <i>ls-name adj-pc</i>	Specifies an output linkset and enters linkset configuration submode.
Step 8	Router(config-cs7-ls)# link <i>slc</i>	Specifies a link in the linkset and enters link configuration mode.
Step 9	Router(config-cs7-ls-link)# qos-class <i>class</i>	Assigns QoS class to link.

	Command	Purpose
Step 10	<code>Router(config-cs7-ls-link)# exit</code>	Exits CS7 link configuration mode and enters linkset configuration mode.
Step 11	<code>Router(config-cs7-ls)# link <i>slc</i></code>	Specifies a link in the linkset and enters link configuration mode. ITP QoS requires that at least one link is configured with no QoS class assigned. A link with no class is a member of the default class (class 0). QoS class 0 member links forward packets that are not classified as members of any other QoS class and packets that are classified as members of an unavailable QoS class.

1. The smaller the number, the higher the priority. See the **update route** ITP Command Set entry for an example.

Specifying a QoS classification for an ASP

QoS packet classification occurs based on both the AS/routing-key and ASP, with ASP taking precedence.

When packets are to be delivered to the AS, the ASP selection process will remain unchanged (i.e., it will not use the QoS classification as a routing key parameter).

If QoS is provisioned for the AS, the classification will be used to set the appropriate TOS using precedence or DSCP values within the IP network. However, if an ASP is selected that is currently active in more than one AS, then the highest priority QoS classification among the active ASs will be used. Setting the QoS class to the highest class ensures that the traffic is processed at the most appropriate priority compared to other IP traffic streams.

If it is desirable for QoS classification to vary based on the type of SS7 traffic, then a unique association is required between the ITP SG and ASP host for each classification type. Thus, from the ITP SG perspective, the ASP “host” will have a unique SCTP association (ASP) per AS that it implements. Each AS is then provisioned with its appropriate QoS class on the ITP SG. For example, an ASP host supporting both ISUP and SCCP traffic would set up two associations to the ITP SG. This would appear to be two different ASPs to the SG, each supporting a unique AS with a different QoS classification value.

QoS can also be provisioned for the ASP. The QoS specified under the ASP takes precedence over the QoS specified for the AS. Consider the following example:

ASP1 has QoS class 5 and this ASP belongs to AS AS1 which has QoS class 3. Since QoS for the ASP overrides the QoS for the AS, the ASP1 will have QoS class 5.

The following rules affect QoS routing over M3UA or SUA links:

- When packets are being routed to an M3UA or SUA AS and eventually delivered to an ASP, the packet might already have been classified by existing packet classification options. The AS or ASP QoS classification overrides the previously set value.
- When a QoS classification is configured for an ASP or an AS, it takes effect only on the subsequent ASP connection. The QoS can only be changed when ASP is NOT active. Use the **shutdown** and **no shutdown** commands in CS7 ASP configuration mode to shut down and then activate the ASP with the QoS change.
- When qos-class is not specified for an ASP (and any of the ASs that the ASP serves), the Type of Service (TOS) for the SCTP association of the ASP is obtained from **cs7 qos class 0**, if it's defined. Otherwise, it is set to zero (0).

To configure a QoS classification for an ASP, use the following commands, beginning in global configuration mode:

Command	Purpose
Router(config)# cs7 asp <i>asp-name remote-port local-port</i> [m3ua sua]	Configures a CS7 ASP definition and enters CS7 ASP submode.
Router(config-cs7-asp)# remote-ip <i>remote-ip</i>	Specifies the remote IP address of the ASP.
Router(config-cs7-asp)# qos-class <i>class</i>	Defines the QoS class for the ASP
Router(config-cs7-asp)# match any qos-class <i>class</i>	Sets the match criteria.
Router(config-cs7-asp)# match si <i>si qos-class class</i>	Sets the serviced indicator match criteria.

Specifying QoS Routing Over M2PA Links

Packets received from M3UA or SUA must be classified with a default QoS class as a minimum requirement, to ensure that packets are not dropped by MTP3. Additionally, you may specify a QoS classification for packets received from a specific ASP.

Packets flowing from M3UA or SUA to M2PA will be subject to Topsail R2 coloring for DPC, GTT selector and GTT address, but not inbound linkset or access list. There is no single equivalent in M3UA or SUA for the inbound linkset. The ASP from which the data was received is the closest approximation to an inbound linkset. The source AS is unknown, and may not be used for this purpose.

Verifying ITP QoS

After the ITP is configured for QoS and the links come in service, you can verify that the ITP QoS was configured properly and that the ITP QoS functionality is available.

The **show cs7 qos** commands can be used to display a summary of the QoS configuration and QoS statistics for an input linkset.

To display a summary of the QoS configuration and verify that the QoS class and packet classifications are assigned correctly, use the following command in privileged EXEC mode:

Command	Purpose
Router# show cs7 qos class	Displays a summary of the QoS configuration.

The following is sample output from the **show cs7 qos class** command:

```
Router# show cs7 qos class
QoS   Prec  DSCP  Acc-Grp  MatchType  Input Linkset
---   ---   ---   ---      ---
1     3      10    2700     any        to_newyork
2     5      10    2701     si 3       to_chicago
3     5      10    2701     si 5       to_chicago
4     4      26    2700     access-group  to_atlanta
5     3      26    2701     none
6     3      26    2701     access-group  to_atlanta
```

The output indicates the following packet classifications for the configured QoS classes:

QoS class 1 is configured for input linkset packet classification.

QoS class 2 and QoS class 3 are configured for service indicator packet classification.

QoS class 4 and QoS Class 6 is configured for access list packet classification.

QoS class 5 is not configured for packet classification.

To verify that traffic is being routed over the correct QoS peer link member(s), use the following command in privileged EXEC mode:

Command	Purpose
Router# show cs7 qos statistics	Displays QoS link use statistics.

The following is sample output from the **show cs7 qos statistics** command:

```
Router# show cs7 qos statistics ls-name
lsn=to_itpa      apc=3.3.3      state=avail      available/links=2/3
  SLC  QoS      MSU In    MSU Out  Drops    ByteCnt In    ByteCnt Out
  00   0        494       492      0        8965         8864
  01   2        501       493      0        9006         8947
```

The sample output shows the number of MSUs sent and received for each QoS class (which is assigned to a peer link member or members) for a specific input linkset.

When classified packets are received from an input linkset and there are no available peer link members that support the QoS class assigned to the classified packets, the packet is dropped. The ITP displays an error message and logs an access violation in the ITP access violations database. A sample of the error message displayed is shown below:

```
no QoS class 2 link available for packets, see show cs7 accounting access-violations
```

The ITP accounting access-violations database indicates the dropped packets origin and destination point codes. To display CS7 accounting details, use the following command in privileged EXEC mode:

Command	Purpose
Router# show cs7 accounting access-violations	Displays the CS7 access-violations database.

The following is a sample output from the **show cs7 accounting access-violations** command:

```
Router# show cs7 qos statistics
Checkpoint Interval = 5 min

Linkset = 'to_newyork'
Destination   Originating   Service      Input          Output
Point Code    Point Code    Indicator    Packets        Bytes    Packets        Bytes
-----
  3.3.3        4.4.4        8           96           3824      0             0
```

The sample output shows that access violations occurred for packets destined for 3.3.3 from origin point code 4.4.4. Packets are received on the input, but zero packets are being routed to the destination point code.

QoS Configuration Example

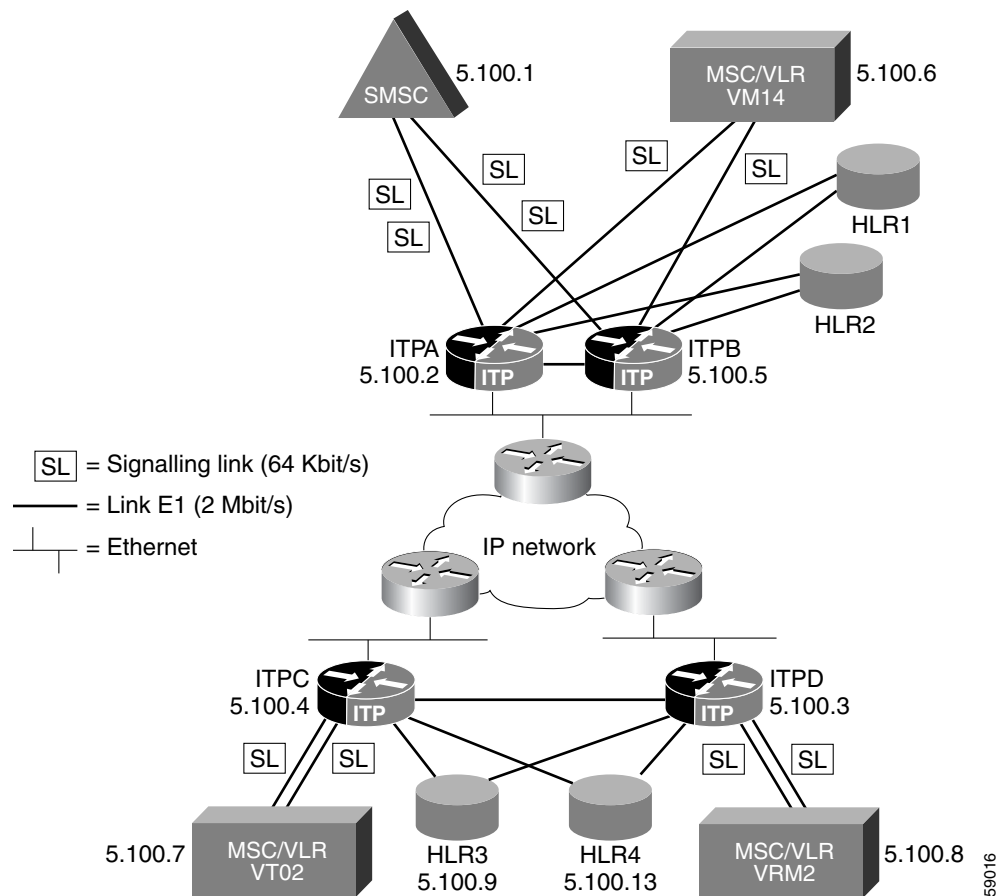
This section includes the following examples of ITP QoS packet classification and Cisco IOS QoS packet scheduling and queuing:

- [Service Indicator Packet Classification and Access List Classification, page 300](#)
- [SCCP Packet Classification, page 303](#)
- [Input Linkset Classification, page 305](#)
- [Destination Point Code Classification, page 307](#)
- [Cisco IOS QoS Packet Scheduling and Queuing, page 309](#)
- [ITP SG QoS Configuration Examples, page 312](#)

The network configuration is illustrated in [Figure 35](#).

→ The arrow symbol indicates the specific configuration statements that implement QoS on each ITP.

Figure 35 ITPs as STPs in an SS7oIP Topology



Assumptions:

All routers have redundant ethernet connectivity and therefore all SCTP associations use two IP addresses (multi-homing).

Point codes and IP addresses for ITP routers:

```
ITPA  5.100.2  172.18.44.242 117.117.117.2
ITPB  5.100.5  172.18.44.243 117.117.117.3
ITPC  5.100.4  172.18.45.1  117.117.119.4
ITPD  5.100.3  172.18.46.1  117.117.118.4
```

Point codes for SS7 SSPs:

```
SMSC  5.100.1
VMI4  5.100.6
VT02  5.100.7
VRM2  5.100.8
```

Service Indicator Packet Classification and Access List Classification

In the following configuration example, ITPA is configured to perform ITP QoS Service Indicator packet classification and access list classification.

All packets arriving on linkset **smsc** are classified according to service indicator. Packets with si 3 are classified class 2 and are sent out on link 1 of the linkset ITPd. Packets with si 5 are classified class 1 and are sent out on link 0 of the linkset ITPd.

All ISUP packets arriving on linkset vmi4 are matched with access list 2701, classified as QoS class3 and are sent out on link 1 of linkset ITPc. All other packets arriving from linkset vmi4 are sent out on link 0 of linkset ITPc.

```
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ITPA
!
enable secret 5 $1$iBmo$AF1H6u2CVGDRM5BMeuGmx/
enable password lab
!
!
no ip cef
no ip finger
no ip domain-lookup
!
cs7 variant itu
cs7 point-code 5.100.2
!
controller E1 1/0/0
  channel-group 0 timeslots 1
!
controller E1 1/0/1
  channel-group 0 timeslots 1
!
controller E1 2/0/0
  channel-group 0 timeslots 1
!
```

```

!
interface FastEthernet0/0/0
 ip address 172.18.44.242 255.255.255.128
 no ip route-cache distributed
 no ip route-cache
 no ip mroute-cache
!
interface FastEthernet0/0/1
 ip address 117.117.117.2 255.255.255.0
 no ip route-cache distributed
 no ip route-cache
 no ip mroute-cache
!
interface Serial1/0/0:0
 no ip address
 encapsulation mtp2
 no ip route-cache distributed
 no ip route-cache
 load-interval 30
!
interface Serial1/0/1:0
 no ip address
 encapsulation mtp2
 no ip route-cache distributed
 no ip route-cache
 load-interval 30
!
interface Serial2/0/0:0
 no ip address
 encapsulation mtp2
 no ip route-cache distributed
 no ip route-cache
 load-interval 30
!
cs7 local-peer 7000
 local-ip 172.18.44.242
 local-ip 117.117.117.2

cs7 local-peer 8000
 local-ip 172.18.44.242
 local-ip 117.117.117.2

cs7 local-peer 9000
 local-ip 172.18.44.242
 local-ip 117.117.117.2

→ cs7 qos class 1
→ ip precedence 4
!
→ cs7 qos class 2
→ ip precedence 3
!
→ cs7 qos class 3
→ qos-access-group 2701
→ qos-ip-precedence 2
!
! Routes using linksets to ITPC and ITPD have a default
! priority of 5. Routes to adjacent node SMS-C and VMI4
! are inserted by the systems with priority 5 and when
! the linkset is configured. They don't have to be defined
! here. Backup-routes to SMS-C and VMI4 are inserted with
! priority 9 using the "C-Link".
!
cs7 route-table system

```

```

update route 5.100.7 7.255.7 linkset ITPc
update route 5.100.8 7.255.7 linkset ITPd
update route 5.100.1 7.255.7 linkset ITPb priority 9
update route 5.100.6 7.255.7 linkset ITPb priority 9
!
cs7 linkset ITPc 5.100.4
accounting
link 0 sctp 172.18.45.1 117.117.119.4 7000 7000
link 1 sctp 172.18.45.1 117.117.119.4 8000 8000
→ qos-class 3
link 2 sctp 172.18.45.1 117.117.119.4 9000 9000
route all table system
!
cs7 linkset ITPd 5.100.3
accounting
link 0 sctp 172.18.46.1 117.117.118.4 7000 7000
→ qos class 1
link 1 sctp 172.18.46.1 117.117.118.4 8000 8000
→ qos class 2
link 2 sctp 172.18.46.1 117.117.118.4 9000 9000
route all table system
!
cs7 linkset smsc 5.100.1
→ match si 3 qos class 2
→ match si 5 qos-class 1
accounting
link 0 Serial1/0/0:0
link 1 Serial2/0/0:0
route all table system
!
cs7 linkset vmi4 5.100.6
→ match access-group
accounting
link 0 Serial1/0/1:0
route all table system
!
cs7 linkset ITPb 5.100.5
accounting
link 0 sctp 172.18.44.243 117.117.117.3 7000 7000
route all table system
!
ip classless
no ip http server
!
!
→ access-list 2701 permit si 5
!
line con 0
transport input none
line aux 0
line vty 0 4
password lab
login
!
end

```

SCCP Packet Classification

In the following configuration example, ITPB is configured to perform ITP QoS SCCP packet classification. QoS class 1 is assigned to the GTT selector table named **c7gsp**. QoS class 2 is assigned to GTA 339. According to QoS rules of precedence, if a QoS class is assigned to a selector table and to a GTA within that selector table, the QoS class assigned to the GTA entry has precedence over the QoS class assigned to the selector table.

```

version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ITPB
!
enable secret 5 $1$iBmo$AF1H6u2CVGDRM5BMeuGmx/
enable password lab
!
!
!
!
no ip cef
no ip finger
no ip domain-lookup
!
cs7 variant itu
cs7 point-code 5.100.3
cs7 capability-pc 5.100.12
!
controller E1 1/0/0
    channel-group 0 timeslots 1
!
controller E1 1/0/1
    channel-group 0 timeslots 1
!
controller E1 2/0/0
    channel-group 0 timeslots 1
!
!
interface FastEthernet0/0/0
    ip address 172.18.44.243 255.255.255.128
    no ip route-cache distributed
    no ip route-cache
    no ip mroute-cache
!
interface FastEthernet0/0/1
    ip address 117.117.117.3 255.255.255.0
    no ip route-cache distributed
    no ip route-cache
    no ip mroute-cache
!
interface Serial1/0/0:0
    no ip address
    encapsulation mtp2
    no ip route-cache distributed
    no ip route-cache
    load-interval 30
!
interface Serial1/0/1:0
    no ip address
    encapsulation mtp2
    no ip route-cache distributed

```

```

no ip route-cache
load-interval 30
!
interface Serial2/0/0:0
no ip address
encapsulation mtp2
no ip route-cache distributed
no ip route-cache
load-interval 30
!
cs7 local-peer 7000
local-ip 172.18.44.243
local-ip 117.117.117.3
!
cs7 local-peer 8000
local-ip 172.18.44.243
local-ip 117.117.117.3
!
cs7 local-peer 9000
local-ip 172.18.44.243
local-ip 117.117.117.3
!
→ cs7 qos class 1
→ qos-ip-precedence 4
!
→ cs7 qos class 2
→ qos-ip-precedence 3

! Routes using linksets to ITPC and ITPD have a default
! priority of 5. Routes to adjacent node SMS-C and VMI4
! are inserted by the systems with priority 5 and when
! the linkset is configured. They don't have to be defined
! here. Backup-routes to SMS-C and VMI4 are inserted with
! priority 9 using the "C-Link".
!
cs7 route-table system
update route 5.100.7 7.255.7 linkset ITPc
update route 5.100.8 7.255.7 linkset ITPd
update route 5.100.1 7.255.7 linkset ITPa priority 9
update route 5.100.6 7.255.7 linkset ITPa priority 9
!
cs7 gtt selector c7gsp tt 0
→ qos-class 1
→ gta 339 qos-class 2 pcssn 5.100.14 gt ntt 0

cs7 linkset ITPc 5.100.4
accounting
link 0 sctp 172.18.45.1 117.117.119.4 7000 7000
→ qos-class 1
link 1 sctp 172.18.45.1 117.117.119.4 8000 8000
→ qos-class 2
link 2 sctp 172.18.45.1 117.117.119.4 9000 9000
route all table system
!
cs7 linkset ITPd 5.100.3
accounting
link 0 sctp 172.18.46.1 117.117.118.4 7000 7000
route all table system
!
cs7 linkset smsc 5.100.1
accounting
link 0 Serial1/0/0:0
link 1 Serial2/0/0:0
route all table system

```

```

!
cs7 linkset vmi4 5.100.6
  accounting
  link 0 Serial1/0/1:0
  route all table system
!
cs7 linkset ITPa 5.100.2
  accounting
  link 0 sctp 172.18.44.242 117.117.117.2 7000 7000
  route all table system
!
ip classless
no ip http server
!
!
!
line con 0
  transport input none
line aux 0
line vty 0 4
  password lab
  login
!
end
!

```

Input Linkset Classification

In the following configuration example, ITPC is configured to perform ITP QoS Input Linkset packet classification. All packets arriving on linkset **vt02** are classified as class 1 and are sent out on link 0 of the linkset ITPa.

```

version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ITPC
!
enable secret 5 $1$iBmo$AF1H6u2CVGDRM5BMeuGmx/
enable password lab
!
!
!
!
!
no ip cef
no ip finger
no ip domain-lookup
!
cs7 variant itu
cs7 point-code 5.100.4
!
!
controller E1 1/0/0
  channel-group 0 timeslots 1
!
controller E1 2/0/0
  channel-group 0 timeslots 1
!
!
interface FastEthernet0/0/0
  ip address 172.18.45.1 255.255.255.128

```

```

no ip route-cache distributed
no ip route-cache
no ip mroute-cache
!
interface FastEthernet0/0/1
ip address 117.117.119.4 255.255.255.0
no ip route-cache distributed
no ip route-cache
no ip mroute-cache
!
interface Serial1/0/0:0
no ip address
encapsulation mtp2
no ip route-cache distributed
no ip route-cache
load-interval 30
!
interface Serial2/0/0:0
no ip address
encapsulation mtp2
no ip route-cache distributed
no ip route-cache
load-interval 30
!
cs7 local-peer 7000
local-ip 172.18.45.1
local-ip 117.117.119.4
!
cs7 local-peer 8000
local-ip 172.18.45.1
local-ip 117.117.119.4
!
cs7 local-peer 9000
local-ip 172.18.45.1
local-ip 117.117.119.4
!
→ cs7 qos class 1
→ ip precedence 2

! Routes to SMS-C and VMI4 use a combined linkset.
! This is defined by inserting two routes with
! identical priority (5 is default).
!
cs7 route-table system
update route 5.100.1 7.255.7 linkset ITPa
update route 5.100.1 7.255.7 linkset ITPb
update route 5.100.6 7.255.7 linkset ITPa
update route 5.100.6 7.255.7 linkset ITPb
update route 5.100.8 7.255.7 linkset ITPd
!
cs7 linkset ITPa 5.100.2
accounting
→ link 0 sctp 172.18.44.242 117.117.117.2 7000 7000
   qos class 1
link 1 sctp 172.18.44.242 117.117.117.2 8000 8000
link 2 sctp 172.18.44.242 117.117.117.2 9000 9000
route all table system
!
cs7 linkset ITPb 5.100.5
accounting
link 0 sctp 172.18.44.243 117.117.117.3 7000 7000
link 1 sctp 172.18.44.243 117.117.117.3 8000 8000
link 2 sctp 172.18.44.243 117.117.117.3 9000 9000
route all table system

```



```

!
cs7 linkset ITPd 5.100.3
  accounting
  link 0 sctp 172.18.46.1 117.117.118.4 7000 7000
  route all table system
!
cs7 linkset vt02 5.100.7
  accounting
→ match any qos class 1
  link 0 Serial1/0/0:0
  link 1 Serial2/0/0:0
  route all table system
!
ip classless
no ip http server
!
!
!
line con 0
  transport input none
line aux 0
line vty 0 4
  password lab
  login
!
end

```

Destination Point Code Classification

In the following configuration example, ITPD is configured to perform ITP QoS Destination Point Code packet classification. All packets with a DPC of 5.100.1 are classified as class 1 and are sent out on link 0 of the linkset ITPa.

```

version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ITPD
!
enable secret 5 $1$iBmo$AF1H6u2CVGDRM5BMeuGmx/
enable password lab
!
!
!
!
!
no ip cef
no ip finger
no ip domain-lookup
!
cs7 variant itu
cs7 point-code 5.100.3
!
!
controller E1 1/0/0
  channel-group 0 timeslots 1
!
controller E1 2/0/0
  channel-group 0 timeslots 1
!
!
interface FastEthernet0/0/0

```

```

ip address 172.18.46.1 255.255.255.128
no ip route-cache distributed
no ip route-cache
no ip mroute-cache
!
interface FastEthernet0/0/1
ip address 117.117.118.4 255.255.255.0
no ip route-cache distributed
no ip route-cache
no ip mroute-cache
!
interface Serial1/0/0:0
no ip address
encapsulation mtp2
no ip route-cache distributed
no ip route-cache
load-interval 30
!
interface Serial2/0/0:0
no ip address
encapsulation mtp2
no ip route-cache distributed
no ip route-cache
load-interval 30
!
cs7 local-peer 7000
local-ip 172.18.46.1
local-ip 117.117.118.4
!
cs7 local-peer 8000
local-ip 172.18.46.1
local-ip 117.117.118.4
!
cs7 local-peer 9000
local-ip 172.18.46.1
local-ip 117.117.118.4
!
→ cs7 qos class 1
→ ip precedence 4
! Routes to SMS-C and VMI4 use a combined linkset.
! This is defined by inserting two routes with
! identical priority (5 is default).
!
cs7 route-table system
→ update route 5.100.1 7.255.7 linkset ITPa qos class 1
update route 5.100.1 7.255.7 linkset ITPb
update route 5.100.6 7.255.7 linkset ITPa
update route 5.100.6 7.255.7 linkset ITPb
update route 5.100.7 7.255.7 linkset ITPc
!
cs7 linkset ITPa 5.100.2
accounting
link 0 sctp 172.18.44.242 117.117.117.2 7000 7000
→ qos class 1
link 1 sctp 172.18.44.242 117.117.117.2 8000 8000
link 2 sctp 172.18.44.242 117.117.117.2 9000 9000
route all table system
!
cs7 linkset ITPb 5.100.5
accounting
link 0 sctp 172.18.44.243 117.117.117.3 7000 7000
route all table system
!
cs7 linkset ITPd 5.100.4

```

```

accounting
link 0 sctp 172.18.45.1 117.117.119.4 7000 7000
route all table system
!
cs7 linkset vrm2 5.100.8
accounting
link 0 Serial11/0/0:0
link 1 Serial12/0/0:0
route all table system
!
ip classless
no ip http server
!
!
!
line con 0
transport input none
line aux 0
line vty 0 4
password lab
login
!
end

```

Cisco IOS QoS Packet Scheduling and Queuing

The following configuration example illustrates ITP QoS used in conjunction with Cisco IOS QoS at the edge of the IP network.

ITPA is configured to perform ITP QoS Service Indicator packet classification. All packets arriving on linkset vmi4 are classified according to service indicator. Packets with si 3 (SCCP) are classified class 2 and are sent out on link 1 of the linkset ITPd. Packets with si 5 (ISUP) are classified class 1 and are sent out on link 0 of the linkset ITPd. The ITP QoS configuration statements are highlighted in bold text. Cisco ITP QoS configuration statements are highlighted in bold italic text.

Cisco IOS Modular QoS Command-Line Interface will be used to create traffic policies and attach these policies to interfaces. A traffic policy contains a traffic class and one or more IOS QoS features. A traffic class is used to classify traffic, while the QoS features in the traffic policy determine how to treat the classified traffic. The traffic policy in this configuration allocates 50% of the available bandwidth to ISUP packets and 25% of the available bandwidth to SCCP packets during periods of congestion.

Packets classified by ITP QoS will have the ToS byte in the IP header set to the appropriate IP precedence value. Before the classified packets are transmitted, the Cisco IOS QoS traffic policy assigned to the output interface is applied to each packet. In this example, any packets with an IP precedence value of 3, will be subject to the characteristics defined for class sccp. Packets with an IP precedence value of 4 will be subject to class isup characteristics

For more information about deploying Cisco IOS QoS policies, refer to the *Cisco IOS Quality of Service Solutions Configuration Guide* and the *Cisco IOS Quality of Service Solutions Command Reference*, included in the Cisco IOS Release 12.2 documentation at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm>

```

no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ITPA
!
enable secret 5 $1$iBmo$AF1H6u2CVGDRM5BMeuGmx/
enable password lab

```

```

!
!
no ip cef
no ip finger
no ip domain-lookup
!
cs7 variant itu
cs7 point-code 5.100.2
!
!
→ class-map match-all sccp
→   match ip precedence 3
→ class-map match-all isup
→   match ip precedence 4
!
!
→ policy-map itpQoS
→   class sccp
→     bandwidth 25
→   class isup
→     bandwidth 50
!
controller E1 1/0/0
  channel-group 0 timeslots 1
!
controller E1 1/0/1
  channel-group 0 timeslots 1
!
controller E1 2/0/0
  channel-group 0 timeslots 1
!
!
interface FastEthernet0/0/0
  ip address 172.18.44.242 255.255.255.128
  no ip route-cache distributed
  no ip route-cache
  no ip mroute-cache
→ service-policy output itpQoS
!
interface FastEthernet0/0/1
  ip address 117.117.117.2 255.255.255.0
  no ip route-cache distributed
  no ip route-cache
  no ip mroute-cache
!
interface Serial1/0/0:0
  no ip address
  encapsulation mtp2
  no ip route-cache distributed
  no ip route-cache
  load-interval 30
!
interface Serial1/0/1:0
  no ip address
  encapsulation mtp2
  no ip route-cache distributed
  no ip route-cache
  load-interval 30
!
interface Serial2/0/0:0
  no ip address
  encapsulation mtp2
  no ip route-cache distributed
  no ip route-cache

```

```

load-interval 30
!
cs7 local-peer 7000
local-ip 172.18.44.242
local-ip 117.117.117.2

cs7 local-peer 8000
local-ip 172.18.44.242
local-ip 117.117.117.2

cs7 local-peer 9000
local-ip 172.18.44.242
local-ip 117.117.117.2

→ cs7 qos class 1
→ qos-ip-precedence 4
!
→ cs7 qos class 2
→ qos-ip-precedence 3
!
!
! Routes using linksets to ITPC and ITPD have a default
! priority of 5. Routes to adjacent node SMS-C and VMI4
! are inserted by the systems with priority 5 and when
! the linkset is configured. They don't have to be defined
! here. Backup-routes to SMS-C and VMI4 are inserted with
! priority 9 using the "C-Link".
!
cs7 route-table system
update route 5.100.7 7.255.7 linkset ITPc
update route 5.100.8 7.255.7 linkset ITPd
update route 5.100.1 7.255.7 linkset ITPb priority 9
update route 5.100.6 7.255.7 linkset ITPb priority 9
!
cs7 linkset ITPc 5.100.4
accounting
link 0 sctp 172.18.45.1 117.117.119.4 7000 7000
link 1 sctp 172.18.45.1 117.117.119.4 8000 8000
link 2 sctp 172.18.45.1 117.117.119.4 9000 9000
route all table system
!
cs7 linkset ITPd 5.100.3
accounting
link 0 sctp 172.18.46.1 117.117.118.4 7000 7000
→ qos class 1
link 1 sctp 172.18.46.1 117.117.118.4 8000 8000
→ qos class 2
link 2 sctp 172.18.46.1 117.117.118.4 9000 9000
route all table system
!
cs7 linkset smsc 5.100.1
accounting
link 0 Serial1/0/0:0
link 1 Serial2/0/0:0
route all table system
!
cs7 linkset vmi4 5.100.6
→ match si 3 qos-class 2
→ match si 5 qos-class 1
accounting
link 0 Serial1/0/1:0
route all table system
!
cs7 linkset ITPb 5.100.5

```

```

accounting
link 0 sctp 172.18.44.243 117.117.117.3 7000 7000
route all table system
!
ip classless
no ip http server
!
!
line con 0
  transport input none
line aux 0
line vty 0 4
  password lab
  login
!
end

```

ITP SG QoS Configuration Examples

Example 1

In Example 1 all the traffic flowing to asp1 will be classified based on the QoS class 3 since asp1 belongs to AS as1.

```

cs7 qos class 3
  qos-ip-precedence 3
!
cs7 m3ua 2905
  local-ip 7.7.7.7
!
cs7 asp asp1 2905 2905 m3ua
  remote-ip 5.5.5.5
!
cs7 as as1 m3ua
  routing 05050505 4.4.4
  asp asp1
  qos-class 3
!

```

Example 2

In Example 2, since asp2 has been provisioned with qos-class 4, all the traffic flowing to asp2 will be classified with QoS class 4.

```

cs7 qos class 4
  qos-ip-dscp 40
!
cs7 m3ua 2905
  local-ip 7.7.7.7
!
cs7 asp asp2 2905 2905 m3ua
  remote-ip 5.5.5.6
  qos-class 4
!
cs7 as as2 m3ua
  routing 05050506 4.4.4
  asp asp1
!

```

Example 3

In Example 3, the ISUP and SCCP ASPs are located on the same host (same IP address, but different SCTP ports). They are defined as two different ASPs. Since isup-asp belongs to isup-as and isup-as-bk ASs, the QoS with highest IP Type Of Service (TOS), i.e. qos-class 5, will be used for the traffic flowing to isup-asp. Also the traffic flowing to sccp-asp will be classified based on QoS class 3 since this ASP belongs to AS sccp-as.

```

cs7 qos class 3
  qos-ip-precedence 3
cs7 qos class 5
  qos-ip-precedence 5
!
cs7 m3ua 2905
  local-ip 7.7.7.7
!
cs7 asp isup-asp 5500 2905 m3ua
  remote-ip 6.6.6.6
cs7 asp sccp-asp 6000 2905 m3ua
  remote-ip 6.6.6.6
!
cs7 as isup-as m3ua
  routing-key 06060606 5.5.5
  asp isup-asp
  qos-class 5
!
cs7 as isup-as-bk m3ua
  routing-key 07070707 6.6.6
  asp isup-asp
  qos-class 3
!
cs7 as sccp-as m3ua
  routing-key 08080808 7.7.7
  asp sccp-asp
  qos-class 3
!

```

Example 4

In Example 4 any traffic coming in from asp3 will be classified as having QoS class 3. Also any ISUP (si=5) traffic coming in from asp4 will be classified as having QoS class 5. The packet is classified this way so that, if needed, it would properly get routed over M2PA links, as explained in the [“Specifying QoS Routing Over M2PA Links”](#) section on page 297.

```

cs7 qos class 3
  qos-ip-precedence 3
cs7 qos class 5
  qos-ip-dscp 40
!
cs7 m3ua 2905
  local-ip 7.7.7.7
!
cs7 asp asp3 2905 2905 m3ua
  remote-ip 6.6.6.10
  match any qos-class 3
cs7 asp asp4 2905 2905 m3ua
  remote-ip 6.6.6.11
  match si 5 qos-class 5

```




Load Sharing

Feature History for Load Sharing

Release	Modification
12.2(33)IRA	Feature introduced.
12.2(33)IRC	Added the sccp-class1-loadshare command.
12.2(33)IRD	- Enhanced GTT application group load balancing. - Added GTT over-flow load sharing.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



Note

Configuration Mode Restrictions: Simultaneous changes to the configuration from multiple CLI sessions are not supported. Only one configuration session is allowed to enter in configuration mode at a time; other sessions should not enter in configuration mode. The **show line** or **show users EXEC** command may be used to determine the active user sessions on an ITP, and the **clear line EXEC** command may be used to ensure that only a single active session exists.

Contents

- [Information About SCCP Load Sharing, page 316](#)
- [Scenarios for SCCP Load Sharing, page 316](#)
- [Configuring SCCP Load Sharing, page 318](#)
- [Configuring MTP3 Enhanced Load Sharing For ITU, page 331](#)
- [Verifying and Monitoring MTP3 Load Sharing, page 333](#)

Information About SCCP Load Sharing

Signaling Connection Control Part (SCCP) supports routing and translation and management functions and data transfer without logical signaling connections. ITP supports SCCP Load Balancing which includes support for SCCP class 0 and class 1 traffic.

SCCP load sharing utilizing mated applications or application groups includes the following functionality:

- Load-sharing / multiplicity is configurable on a Mated-Application (MAP) or application group basis.
- Class 0 traffic can be load-shared among a maximum of two destinations based on a round-robin algorithm using a GTT MAP (multiplicity = share).
- Class 0 traffic can be load-shared among a maximum of 2 destinations based on a dominant algorithm using a GTT MAP (multiplicity = dominant).
- Class 0 traffic can be load-shared among a maximum of 64 destinations based on a round-robin algorithm using a GTT Application Group. (multiplicity = share).
- Class 0 traffic can be load-shared among a maximum of 64 destinations based on a least cost available algorithm using a GTT Application Group. (multiplicity = cost).
- Class 0 traffic can be load-shared among a maximum of 64 destinations based on a weighted round robin (WRR) algorithm using a GTT Application Group. (multiplicity = wrr).
- Class 1 traffic can be load-shared among a maximum of 2 destinations based on 1 SLS bit using a GTT MAP (multiplicity = share).
- Class 1 traffic can be load-shared among a maximum of 2 destinations on a dominant algorithm using a GTT MAP (multiplicity = dominant).
- Class 1 traffic can be load-shared among a maximum of 64 destinations based on the class 1 traffic loadshare option using a GTT Application Group. (multiplicity = share).
- Class 1 traffic can be load-shared among a maximum of 64 destinations based on a least cost available algorithm using a GTT Application Group in conjunction with the class 1 traffic loadshare option. (multiplicity = cost).
- Class 1 traffic can be load-shared among a maximum of 64 destinations based on a weighted round robin (WRR) algorithm using a GTT Application Group. (multiplicity = wrr).

Scenarios for SCCP Load Sharing

This section describes the possible configuration options for SCCP load sharing as well as address guidelines for when to use the different methods provided. Load-sharing/multiplicity is configurable on a Mated-Application or Application group basis.

The following SS7 network elements are typical in most SS7 architectures utilizing GTT.

1. Solitary intermediate destination – The final destination of the global title is not known and only one intermediate destination is available for the next hop.
2. Solitary final destination - The final destination of the global title is known and only one choice is available.
3. Redundant intermediate destination - The final destination of the global title is not known and two or more intermediate destinations are available for the next hop.

4. Redundant final destination - The final destination of the global title is known and two or more choices are available.
5. More than one backup final or intermediate: The result may be final or intermediate depending on the availability of external nodes or the ability to load-share across up to 64 different destinations.

Scenario 1 and 2 above do not involve any load sharing and are mentioned only for completeness. In each of these cases all resultant GTT traffic is directed to the solitary destination. In case 1, only the MTP3 status determines if the destination is available. In case 2, the MTP3 point-code status as well as the SCCP subsystem status is analyzed. In either case, if the solitary destination is not available, there is no alternate, and the message is discarded.

Scenario 3: In order to configure this situation an application group must be used. There are 2 different possibilities concerning how load sharing may be configured for this group:

- a. Share mode: When this mode is configured Class 0 traffic will be shared between the two destinations if available based on a round-robin algorithm. Class 1 traffic will be shared based on the class 1 traffic loadshare option, which has an SLS default. This situation may be configured to share between up to 64 destinations for class 0 and class 1 traffic.
- b. Cost Mode: When cost mode is configured the least cost item or items (if more than one at that cost) will be used. When more than 1 item at the least cost is available, round-robin is used for class 0 traffic and the class 1 traffic loadshare option is used for class 1 traffic.

Cost Mode Example 1: Suppose an application group is defined with two items, each with its own unique cost. In this situation all traffic would use the least cost item (A) if it were available otherwise it would use item B. This is equivalent to the dominant mode described later for GTT MAPs.

Table 21 **Reference for Cost Mode Example 1**

Item	Cost
A	1
B	2

Cost Mode Example 2: Suppose an application group is defined with two items, each with the same cost. In this situation all traffic would share equally between A and B using round robin or the class 1 traffic loadshare option depending on the protocol class. This is equivalent to the share mode described earlier.

Table 22 **Reference for Cost Mode Example 2**

Item	Cost
A	1
B	1

Cost Mode Example 3: In this example, items A and B shall always be used in a share like fashion (either by round-robin or the class 1 traffic loadshare option). If both A and B, become unavailable, then items C and D are used in the same fashion. If all items A through D become unavailable, then item E must handle all the traffic.

Table 23 *Reference for Cost Mode Example 3*

Item	Cost
A	1
B	1
C	2
D	2
E	3

Scenario 4: There is no difference between scenario 4 and 3 other than the resultant routing-indicator is final for this scenario instead of intermediate. The same cost and share modes may be applied if using an application group. One option not available for scenario 3, that is available for this, is the ability to use GTT MAP (Mated Application) instead of an application group. GTT Mated Applications only allow a maximum of two replicated PC/SSN combinations as the choice for the resultant GTT. These can operate in the share or dominant modes. The advantage of using a GTT MAP instead of an application group is memory savings. An application group uses more memory than utilizing a GTT MAP.

Scenario 5: There is no difference between this scenario and scenario 3 except the items in the group may have mixed values for the resultant routing indicator. The same cost and share modes may be applied. Suppose GTT is performed from the ITP to locate HLRs (item A and B). The data on A and B is replicated and traffic is shared between them, thus the equal cost 1. If a failure occurred at A or B it may be desired to direct the traffic to another pair of ITPs which will have to perform GTT again to find a different final destination since the primary final destination could not be reached. This is one reason network operators may wish to have a mixture of final and intermediate destinations in one application group utilizing cost mode sharing.

Table 24 *Reference for Scenario 5*

Item	Cost
A - Final	1
B - Final	1
C - Intermediate	2
D - Intermediate	2

Configuring SCCP Load Sharing

Cisco ITP supports several methods for distributing SCCP traffic.

This section contains the following information and procedure:

- [Configuring GTT Application Group Overflow Load Sharing for SCCP Class 0, page 319](#)
- [Configuring the MTP Overflow Load Sharing, page 323](#)
- [Configuring GTT Application Group Load Balancing for SCCP Traffic at the Global Level, page 327](#)
- [Configuring GTT Application Groups with the WRR Algorithm for Processing SCCP Class 1 Traffic, page 329](#)
- [Configuring SCCP Class 0 Load Sharing to Ignore Class and Sequencing, page 330](#)

- [Configuring SCCP Class 1 Load Sharing to Ignore Class and Sequencing, page 330](#)

Configuring GTT Application Group Overflow Load Sharing for SCCP Class 0

This configuration allows the ITP to send a user defined amount of traffic to a primary destination. Excess traffic is then sent to a secondary destination. This distribution is more specific than those based on congestion. Overflow load sharing is especially useful for enforcing customer limitations.

Restrictions and Considerations

- Only one rate limit entry is allowed for a GTT application group.
- You configure the rate limit entry for a specific destination in the GTT application group.
- You must configure both a primary and secondary (backup).
- You can define the primary and secondary by configuring ASs, DPCs, or any combination of an AS and DPC.
- The primary AS or DPC is defined as the one with the lowest configured cost.

CONFIGURATION STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	cs7 gtt application-group <i>group-name</i> Example: Router(config)# cs7 gtt application-group abc	Defines the GTT application group and enables application-group submode.

Command or Action	Purpose
Step 4 multiplicity {cost share cgpa wrr} Example: Router(config-cs7-gtt-app-grp)# multiplicity cost	Specifies a method for selecting a destination for the application group. • cost—Uses the destination with the least cost if that destination is available. • share—Shares equally among all destinations. • cgpa—Uses the SCCP calling party address (CGPA) field, which results in a weighted factor selection number for choosing the next destination from the available items in the application group. • wrr—Applies weighted round robin load balancing (WRR) to SCCP class 0 and SCCP class 1 traffic.  Note The cost keyword is used for overflow load sharing configurations.
Step 5 instance <i>instance-number</i> asname <i>as-name</i> {cost [ssn <i>ssn</i>] {gt [ntt <i>ntt</i>] pcssn} [limit <i>rate</i>] wf [ssn <i>ssn</i>] {gt [ntt <i>ntt</i>] pcssn}} Example: The primary AS use the limit keyword and <i>rate</i> argument to define the rate limit. Router(config-cs7-gtt-app-grp)# asname weekday 1 gt limit 2000 The backup AS does not define a rate limit. Router(config-cs7-gtt-app-grp)# asname weekday overflow 2 gt	(Optional) Assigns an M3UA or SUA AS directly to a global title. You must configure both a primary and backup AS to take advantage of the GTT loadshare overflow feature. You must assign a cost to the AS to take advantage of the GTT overflow loadsharing feature. The primary destination is defined by the lower cost. • cost— Index value (1-64). Specifies the priority of the AS within the application group. Use the limit keyword to limit traffic rate to a specific AS in a GTT application group. The rate limit is configured only on the primary destination. • limit—Specifies the traffic-rate limitation. • rate—defines the rate as an integer value from 1 to 4294967296 MSU/sec.

	Command or Action	Purpose
Step 6	instance <i>instance-number</i> pc <i>pc</i> [ssn <i>ssn</i>] {<i>cost</i> {gt [<i>ntt</i> <i>ntt</i>] pcssn} [limit <i>rate</i>] <i>wf</i> {gt [<i>ntt</i> <i>ntt</i>] pcssn}} Example: The primary DPC use the limit keyword and <i>rate</i> argument to define the rate limit. <pre>Router(config-cs7-gtt-app-grp)# pc 1.1.1 ssn 11 1 pcssn limit 2000</pre> The backup DPC does not define a rate limit. <pre>Router(config-cs7-gtt-app-grp)# pc 1.1.2 ssn 11 2 pcssn</pre>	(Optional) Adds or changes a point code and optional subsystem number in the application group. You must configure both a primary and backup DPC to take advantage of the GTT loadshare overflow feature. You must assign a cost to the DPC to take advantage of the GTT overflow load sharing feature. The primary destination is defined by the lower cost. The rate limit is configured only on the primary destination. <i>cost</i>— Index value (1-64). Specifies the priority of the DPC within the application group. Use the limit keyword to specify the traffic limitations for a specific AS in a GTT application group. The limit keyword is configured only on the primary destination. limit—specifies the traffic limitation. <i>rate</i>—defines the rate as an integer value from 1 to 4294967296 MSU/sec.
Step 7	exit Example: <pre>Router(config-cs7-gtt-app-grp)# exit</pre>	Exits CS7 GTT application-group submode.

Example

In the following example, the application group SMS-peak-on-weekdays has a primary DPC with a point code of 1.1.1 is limited to a rate of 2000 MSU per second. Any overflow traffic is sent to the backup DPC with a point code of 1.1.2. The primary DPC is defined by the lower cost of 1. The backup is defined by the higher cost of 2.

```
cs7 gtt application-group SMS-peak-on-weekdays
multiplicity cost
pc 1.1.1 ssn 11 1 pcssn limit 2000
pc 1.1.2 ssn 11 2 pcssn
```

In the following example, the application group SMS-peak-on-weekdays has a primary AS named weekday is limited to a rate of 2000 MSU per second. Any overflow traffic is sent to the backup AS named weekend. The primary AS is defined by the lower cost of 1. The AS is defined by the higher cost of 2.

```
cs7 gtt application-group SMS-peak-on-weekdays
multiplicity cost
asname weekday 1 gt limit 2000
asname weekend 2 gt
```

Verifying and Monitoring

To verify the GTT SCCP overflow loadshare feature, use the following command in EXEC mode:

Command	Purpose
Router# show cs7 { instance <i>instance</i> } id rate-limit { pc <i>pc</i> asname <i>as-name</i> }	Displays the rate limit status of MTP overflow loadshare through the GTT application group .
Router# show cs7 instance id gtt application-group name <i>application-group-name</i> rate-limit	Displays the rate limit status of each line card for GTT SCCP loadshare overflow.

Configuring the MTP Overflow Load Sharing

This configuration allows the ITP to send a user defined amount of traffic to an application group using MTP. The feature is instance wide and takes into account that there may be more than application group containing the same AS or DPC. It is similar to the GTT SCCP overflow loadshare feature.

CONFIGURATION STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	cs7 gtt application-group <i>group-name</i> Example: Router(config)# cs7 gtt application-group abc	Defines the GTT application group and enables application-group submenu.
Step 4	multiplicity {cost share cgpa wrr} Example: Router(config-cs7-gtt-app-grp)# multiplicity cost	Specifies a method for selecting a destination for the application group. cost—Uses the destination with the least cost if that destination is available. share—Shares equally among all destinations. cgpa—Uses the SCCP calling party address (CGPA) field, which results in a weighted factor selection number for choosing the next destination from the available items in the application group. wrr—Applies weighted round robin load balancing (WRR) to SCCP class 0 and SCCP class 1 traffic.  Note The cost keyword is used for overflow load sharing configurations.

	Command or Action	Purpose
Step 5	instance <i>instance-number</i> pc <i>pc</i> [ssn <i>ssn</i>] {cost [gt [ntt <i>ntt</i>] pcssn] [limit <i>rate</i>] wf {gt [ntt <i>ntt</i>] pcssn}} Example: The primary DPC use the limit keyword and <i>rate</i> argument to define the rate limit. <pre>Router(config-cs7-gtt-app-grp)# pc 1.1.1 ssn 11 1 pcssn limit 2000</pre> The backup DPC does not define a rate limit. <pre>Router(config-cs7-gtt-app-grp)# pc 1.1.2 ssn 11 2 pcssn</pre>	(Optional) Adds or changes a point code and optional subsystem number in the application group. You must configure both a primary and backup DPC to take advantage of the GTT loadshare overflow feature. You must assign a cost to the DPC to take advantage of the GTT overflow load sharing feature. The primary destination is defined by the lower cost. The rate limit is configured only on the primary destination. <i>cost</i>— Index value (1-64). Specifies the priority of the DPC within the application group. Use the limit keyword to specify the traffic limitations for a specific AS in a GTT application group. The limit keyword is configured only on the primary destination. limit—specifies the traffic limitation. <i>rate</i>—defines the rate as an integer value from 1 to 4294967296 MSU/sec.
Step 6	instance <i>instance-number</i> asname <i>as-name</i> {cost [ssn <i>ssn</i>] {gt [ntt <i>ntt</i>] pcssn} [limit <i>rate</i>] wf [ssn <i>ssn</i>] {gt [ntt <i>ntt</i>] pcssn}} Example: You configure the limit keyword and <i>rate</i> argument to define the traffic limitations only on the primary AS. <pre>Router(config-cs7-gtt-app-grp)# asname weekday 1 gt limit 2000</pre> The backup AS does not the limit keyword and <i>rate</i> argument. <pre>Router(config-cs7-gtt-app-grp)# asname weekday overflow 2 gt</pre>	(Optional) Assigns an M3UA or SUA AS directly to a global title. You must configure both a primary and backup AS. You must assign a cost to the AS. The primary destination is defined by the lower cost. <i>cost</i>— Index value (1-64). Specifies the priority of the AS within the application group. Use the limit keyword to specify the traffic limitations for a specific AS in a GTT application group. The limit keyword is configured only on the primary destination. <i>rate</i>—defines the rate as an integer value from 1 to 4294967296 MSU/sec.
Step 7	exit Example: <pre>Router(config-cs7-gtt-app-grp)# exit</pre>	Exits GTT configuration mode.

	Command or Action	Purpose
Step 8	cs7 instance [<i>instance id</i>] rate-limit <i>rate</i> { pc [<i>ss7 pc</i>] asname [<i>as-name</i>] } [type sccp] Example: Router(config)# cs7 instance 7 rate-limit 1000 as Alpha type sccp	Limits traffic rate to a specified DPC or AS in MTP overflow loadshare through a GTT application group. • rate-limit—specifies there is a traffic-rate limitation. It limits the total traffic rate from gtt application group to this DPC or AS. The over-flow traffic will be routed to higher cost DPC or AS in the coming gtt application group. If not specified, the DPC or AS does not have a rate-limit. • rate—An integrate value from 1 to 4294967296 MSU/sec. • type—indicates which type the rate-limit would apply to. Default is sccp. • sccp— specifies that the rate limit is only applied to MAP entry instance-wide. This means the gtt application group can be limited.  Note The SCCP option is the only type currently supported.
Step 9	exit Example: Router(config)# exit	Exits global configuration mode.

Configuring GTT Application Group Load Balancing for SCCP Traffic

GTT application group load balancing allows both SCCP class 0 and SCCP class 1 traffic to be shared among multiple active destinations. You can choose one of several method for routing the traffic.

CONFIGURATION STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	cs7 gtt application-group <i>group-name</i> Example: Router(config)# cs7 gtt application-group abc	Defines the GTT application group and enables CS7 GTT application-group submenu.
Step 4	multiplicity { <i>cost</i> <i>share</i> <i>cgpa</i> <i>wrr</i> } Example: Router(config-cs7-gtt-app-grp)# multiplicity cost	Specifies a method for selecting a destination for the application group. cost—Uses the destination with the least cost if that destination is available. share—Shares equally among all destinations. cgpa—Uses the SCCP calling party address (CGPA) field, which results in a weighted factor selection number for choosing the next destination from the available items in the application group. wrr—Applies weighted round robin load balancing (WRR) to SCCP class 0 and SCCP class 1 traffic.  Note The destination in a GTT application group uses the wf argument when the multiplicity command is configured with the cgpa or wrr keyword.
Step 5	instance <i>instance-number</i> asname <i>as-name</i> [<i>cost</i> [<i>ssn</i> <i>ssn</i>] { <i>gt</i> [<i>ntt</i> <i>ntt</i>] <i>pcssn</i> } [<i>rate-limit</i> <i>rate</i>] <i>wf</i> [<i>ssn</i> <i>ssn</i>] { <i>gt</i> [<i>ntt</i> <i>ntt</i>] <i>pcssn</i> }} Example: Router(config-cs7-gtt-app-grp)# asname as1 4 gt	(Optional) Assigns an M3UA or SUA AS directly to a global title.

	Command or Action	Purpose
Step 6	instance <i>instance-number</i> pc <i>pc</i> [ssn <i>ssn</i>] { <i>cost</i> { gt [<i>ntt</i> <i>ntt</i>] pcssn } [rate-limit <i>rate</i>] wf { gt [<i>ntt</i> <i>ntt</i>] pcssn }}	(Optional) Adds or changes a point code and optional subsystem number in the application group.
	Example: Router(config-cs7-gtt-app-grp)# pc 7.7.1 3 gt	
Step 7	exit	Exits CS7 GTT application-group submode.
	Example: Router(config)# exit	

Example

The following example shows how to configure a GTT application group named alpha that uses the CGPA method for selecting a destination for the application group. The CGPA method uses the SCCP calling party address (CGPA) field to determine the destination.

It also configures an application group of three items. The first item is used approximately twice as many times as the other two items. These items handle equal amounts of traffic.

```
cs7 gtt application-group alpha
multiplicity cgpa
pc 1.1.1 ssn 8 50 pcssn
pc 1.1.2 ssn 8 25 pcssn
pc 1.1.3 ssn 8 25 pcssn
```

The following example shows how to configure a GTT application group named abc that uses the destination with the least cost to select a destination for the application group.

It also configures two AS names. AS1 has a cost value of four and RI set to route on GT. AS2 has a cost value of five and the RI set to route on point code and subsystem number.

```
cs7 gtt application-group abc
multiplicity cost
pc 7.7.1 3 gt
asname as1 4 gt
asname as2 5 pcssn
```

Configuring GTT Application Group Load Balancing for SCCP Traffic at the Global Level

You can configure the loadsharing option for GTT application groups at the global level. This applies only to Class 1 traffic.

CONFIGURATION STEPS

	Command	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	cs7 [instance <i>instance-number</i>] sccp-class1-loadshare { opc-sls [opc-shift [<i>opc-shift-number</i>] cgpa sls } Example: ITP(config)# cs7 instance 1 sccp-class1-loadshare cgpa	Configures the global loadsharing option for GTT application groups. instance —(Optional) Configures the secondary point code on an instance. instance-number—Defines the specific instance. Valid values are from 0 to 7. opc-sls—Extends SLS based ASP binding to OPC-SLS combination based binding. This command applies only to the ITU standard not the ANSI standard. cgpa—Specifies the SCCP calling party address option. sls—Specifies the signaling link selection (sls) based load sharing option. opc-shift—(Optional) opc-shift applies only to opc-sls option. The default shift is 0. This command applies only to the ITU standard not the ANSI standard. opc-shift-number— (Optional) Defines the specific instance.

Example

The following command configure the loadsharing option for GTT application groups in loadshare/cost mode with the SCCP calling party address option:

```
cs7 instance 1 sccp-class1-loadshare cgpa
```

Configuring GTT Application Groups with the WRR Algorithm for Processing SCCP Class 1 Traffic

You can configure the loadsharing option for GTT application groups in WRR mode with the SCCP calling party address option. It applies for Class 1 traffic for all GTT application groups with the wrr mode in that instance.

CONFIGURATION STEPS

	Command	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	cs7 [instance instance-number] sccp-class1-wrr {opc-sls [opc-shift [opc-shift-number] cgpa-sls sls opc]} Example: ITP(config)# cs7 instance 1 sccp-class1-wrr cgpa-sls	Indicates the seed for the WRR algorithm when processing SCCP class 1 traffic. instance —(Optional) Configures the secondary point code on an instance. instance-number—Defines the specific instance. Valid values are from 0 to 7. opc-sls—Extends SLS based ASP binding to OPC-SLS combination based binding. This command applies only to the ITU standard not the ANSI standard. cgpa-sls—Load sharing with the combination of cgpa and sls. sls—Specifies the signaling link selection (sls) based load sharing option. opc—Uses OPC to calculate wrr loadsharing. opc-shift—(Optional) opc-shift applies only to opc-sls option. The default shift is 0. This command applies only to the ITU standard not the ANSI standard. opc-shift-number— (Optional) Defines the specific instance.

Example

```
cs7 instance 1 sccp-class1-wrr cgpa-sls
```

Configuring SCCP Class 0 Load Sharing to Ignore Class and Sequencing

Although some high level SS7 protocols require in-sequence delivery of packets, other high level SS7 protocols, such as SCCP and TCAP, do not. When **cs7 distribute-sccp-unsequenced** is enabled, the Cisco ITP examines the packet header and determines whether or not that protocol requires in-sequence delivery. If in-sequence delivery is not required, the SLS field value is ignored and the Cisco ITP makes a round-robin selection of the link or ASP on which to forward the packet.

PROCEDURE STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	cs7 [instance instance-number] distribute-sccp-unsequenced Example: Router(config)# cs7 instance 1 distribute-sccp-unsequenced	Disable SCCP load sharing recognition of class and sequencing. instance—Specifies an instance if multiple instances exist. If you have configured the ITP with the multi-instance command, you must use the instance keyword to specify the particular instance. A single instance does not require this keyword. instance-number—Specifies the particular instance with a valid range of 0 through 7. The default is 0.

Example

```
cs7 distribute-sccp-unsequenced

or

cs7 instance 1 distribute-sccp-unsequenced
```

Configuring SCCP Class 1 Load Sharing to Ignore Class and Sequencing

Having SCCP recognize the class or round-robin sequencing of traffic may not benefit some networks. For example, if the majority of traffic is SCCP class 1, but there is no advantage in keeping the traffic in sequence. The **cs7 distribute-sccp-sequenced** command configures SCCP load sharing to ignore class and sequencing. Enabling this command allows an even distribution of class 1 traffic.



Note

SCCP class 1 sequencing is not guaranteed and could impact application behavior.

PROCEDURE STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	cs7 [instance instance-number] distribute-sccp-sequenced Example: Router(config)# cs7 instance 1 distribute-sccp-sequenced	Disable SCCP load sharing recognition of class and sequencing. instance—Specifies an instance if multiple instances exist. If you have configured the ITP with the multi-instance command, you must use the instance keyword to specify the particular instance. A single instance does not require this keyword. instance-number—Specifies the particular instance with a valid range of 0 through 7. The default is 0.

Example

```
cs7 distribute-sccp-sequenced
or
cs7 instance 1 distribute-sccp-sequenced
```

Configuring MTP3 Enhanced Load Sharing For ITU

The ITU standard specifies a 4-bit SLS in the MSU for link selection (SLC). This is insufficient for combined linksets made up of 17 or more links. To enable a better load distribution for the combined linksets, the user can configure the enhanced load sharing feature. The enhanced load sharing feature concatenates a 3-bit value, derived from the opc and dpc, with the 4-bit SLS and yields a 7-bit value used to select a link from a 128 entry SLS->SLC mapping table.

The user can also shift the SLS bits used for linkset and link configuration with the **sls-shift** command.

To configure the enhanced load sharing feature or to shift the SLS bits, perform the following steps:

**Note**

These configurations are only available with the ITU variant.

CONFIGURATION STEPS

	Command	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	cs7 [instance instance-number] sls-opc-dpc [opc-shift <opc-shift-number>] [dpc-shift <dpc-shift-number>] Example: ITP(config)# cs7 instance 4 sls-opc-dpc opc-shift 7 dpc-shift 4	(Optional) Creates a 3-bit value from 6-bit subsets of the OPC and DPC. opc-shift <i>opc-shift-number</i>—(Optional) Sets parameters for the subset of bits from the OPC. The range is from 0 to 8 with a default of 0. Beginning with the least significant bit position as <i>opc-shift-number</i> 0. The <i>opc-shift-number</i> specifies the number of bit positions from which the 6-bits are selected. dpc-shift <i>dpc-shift-number</i>—(Optional) Sets parameters for the subset of bits from the DPC. The range is from 0 to 8 with a default of 0. Beginning with the least significant bit position as <i>dpc-shift-number</i> 0. The <i>dpc-shift-number</i> specifies the bit position from which the 6-bits are selected.
Step 4	cs7 [instance instance-number] sls-shift { <i>sls-shift-value</i> } Example: ITP(config)# cs7 instance 0 sls-shift 3 or ITP(config-cs7-ls)# sls-shift 3	(Optional) Shifts the SLS bits to change which SLS bits are used for link and linkset selection. The range is from 0 to 3. The default is 0. - When sls-opc-dpc is configured, simultaneous configuration of sls-shift at the global and/or linkset level is allowed. Also the valid range of sls-shift-value increases to 0 to 6 with sls-opc-dpc configured. - When sls-opc-dpc is configured, the shift operation is performed on the computed 7-bit sls. - If the sls-shift values are set in the 4 to 6 range and sls-opc-dpc is unconfigured, then any configured value in the 4 to 6 range is reset to zero.

Verifying and Monitoring MTP3 Load Sharing

The SLS field in MSUs is used for load sharing. Proper load sharing in SS7 networks relies on end nodes generating all SLS values equally. In order to trouble shoot load sharing problems in the network, this command samples the SLS values for incoming or outgoing MSUs on a link or linkset, and the related show command reports the number of MSUs received for each SLS.

SUMMARY STEPS

1. **enable**
2. **cs7 sample linkset** [*linkset-name*] [*slc*] {**in** | **out**} [**sample-time** [*sample-time-seconds*]]
3. **show cs7 sample sls**

	Command	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	cs7 sample linkset [<i>linkset-name</i>] [<i>slc</i>] { in out } [sample-time [<i>sample-time-seconds</i>]] Example: Router# cs7 sample linkset LS-A in	Samples all traffic coming in or out on a link or linkset and then reports the number of MSUs for each SLS value to monitor MTP3 load sharing.
Step 3	show cs7 sample sls Example: router# show cs7 sample sls SLS Received Report for linkset LS-A from Nov 27 2007 13:44:32 SLS number SLS number SLS number SLS number rcvd rcvd rcvd rcvd 000 0002 004 0002 008 0000 012 0000 001 0002 005 0002 009 0000 013 0000 002 0002 006 0002 010 0000 014 0000 003 0002 007 0002 011 0000 015 0000	Displays the results from the latest SLS sample.



Inter-Carrier Accounting

Inter-Carrier Accounting enables Cisco ITP to accumulate ingress and egress traffic statistics into accounts. Each configured account can represent an operator or carrier. Inter-Carrier Accounting allows the use of ITP accounting data for Signaling Data Records (SDR) and Inter-Carrier billing.

Feature History for Load Sharing

Release	Modification
12.2(33)IRD	This feature was introduced.
12.2(33)IRF	SMS accounting was added.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



Note

Configuration Mode Restrictions: Simultaneous changes to the configuration from multiple CLI sessions are not supported. One configuration session is allowed to enter configuration mode; other sessions cannot enter in configuration mode. The **show line** or **show users EXEC** command may be used to determine the number of active user sessions on an ITP, and the **clear line EXEC** command may be used to ensure that only a single active session exists.

Contents

- [Information About Inter-Carrier Accounting, page 335](#)
- [Configuring Inter-Carrier Accounting, page 338](#)
- [Verifying and Monitoring, page 346](#)

Information About Inter-Carrier Accounting

Cisco ITP generates a large amount of statistical and accounting information from its signaling network. Inter-Carrier Accounting allows the user to tailor this information for use in billing and settlement.

The process starts with manually configuring a set of accounts. An account represents a carrier, customer or operator. Select the appropriate criteria for the traffic accumulating against these accounts. For example, you might configure Inter-Carrier Accounting for the traffic on a linkset to a specific operator.

Inter-Carrier Accounting is based on MTP3, SCCP, or SMS messages. It also has data collection and backup options to help preserve the integrity of the data.

MTP3 Accounting

MTP3 Accounting counts the bytes and message signal units (MSUs) of the signaling traffic received from, or sent to an active linkset. For each linkset in an account, there are sets of counters that increment based on the destination of the traffic.

For MTP3 Accounting, an account consists of:

- The ITP and the instance number.
- The customer number, ID, or name that indicates the identity of the adjacent network operator.
- A set of names for the linksets that connect to this specific operator.
- A direction for the accounting inspection. The direction is set as either In, Out, or Both. Specifying In or Out prevents the ITP from having to inspect the traffic in both directions.
- (Optional) A set of either destination point codes (DPCs) or originating point codes (OPCs) for this account to accumulate. Each accounting direction (In, Out, Both) could accumulate on either OPC or DPC. This allows an operator to accumulate Outgoing traffic based on OPC, or incoming based on DPC.
- (Optional) A set of service indicators to accumulate in this account.

SCCP Accounting

SCCP Accounting counts the bytes, message signal units (MSUs) and Global Title Translation (GTT) operations performed on the received SCCP traffic, which requires onward forwarding. This process only accounts for final or intermediate traffic requiring GTT at the ITP, when the ITP functions as an SCCP relay node instead of an MTP3 relay node. SCCP messages, in which the destination point code (DPC) is not the local point code of the ITP, should use MTP3 Accounting.

For SCCP accounting, an account would consist of:

- The ITP and the instance number.
- The customer number, ID, or name that indicates the identity of the adjacent network operator.
- A set of names for the linksets that connect to this specific operator. The use of a linkset as an account variable allows the operator to turn SCCP accounting off and on.
- A direction for the accounting. The direction is set as either In, Out, or Both. In specifies ingress traffic. Out specifies egress traffic.
- A set of either:
 - OPC (In traffic) of the operator which performed GTT previously.
 - DPC (Out traffic) of the operator which has to perform GTT next.
- (Optional) A set of one of the following:
 - CgPA GTA (originating operator for In traffic)
 - CdPA GTA (destination operator for Out traffic)

- CgPA SSN (originating service for In traffic)
- CdPA SSN (destination service for Out traffic)

SMS Traffic Accounting

Inter-Carrier Accounting also supports accounting for incoming SMS traffic. SMS accounting is based on defining an account at the SCCP level. You define and use SMS accounting in the same manner as MTP3/SCCP accounting. The account can be defined only on the inbound interface, not on the outbound interface. Account IDs configured with the type SMS help segregate the SMS traffic. No counters increment at the MTP3 or SCCP level for SMS accounts. The defined parameters operate at the MAP/IS41 layer to isolate SMS messages for this particular account and increment the SMS specific counters.

MLR routing is required for SMS traffic accounting. SMS traffic accounting is not valid when the Cisco ITP is routing SMS traffic at the SCCP or MTP3 level.

Service Data Records

The accounting information is stored in the form of signaling data records (SDRs) formatted as plain text. These SDRs are saved onto a storage server. You can use these accumulated SDRs to generate billing information.

The SDR contains these fields:

- Date/Time of the start and end of each time interval
- SDR Version ID
- Instance ID
- Account ID / Name
- Linkset name and direction
- OPC
- SMS MSU sent/received
- SMS Bytes/Octets transmitted or received

This is an example of an SDR:

```
Start Timestamp : 2009/09/22/09:15:03.191
End Timestamp   : 2009/09/22/09:16:33.183
SDR Version ID: Ver-1.0
Total Records   : 10
-----
Instance : 0
Instance : 0
Account   : sms-acc
Linkset   : m2pa_194_0_0
SCCP OPC IN : 1.1.2
SSN       : others
SMS MSU/SMS OCTETS : 10/1380
```

Data Collection and Backup Options

Accounting records used for billing and Inter-Carrier settlement activities need a robust mechanism to limit the loss and maintain the integrity of the accounting data. They should also generate and retain information about the collection and distribution of the data. Inter-Carrier Accounting includes these features:

- Traceable accounting records with sequence number
- Visibility to the operator of any lost data or time gaps in the accounting data
- Uploading for backup purposes and for subsequent post-processing, and distribution or collection
- Temporary backup to a flash drive
- Minimal or no accumulator data loss after a supervisor module switchover, hardware removal, or other recoverable events

Configuring Inter-Carrier Accounting

This section contains information and procedures:

- [Configuring an MTP3 Inter-Carrier Accounting Billing Account, page 338](#)
- [Configuring an SCCP Inter-Carrier Accounting Billing Account, page 341](#)
- [Configuring Inter-Carrier Accounting Data Collection, page 345](#)
- [Saving and Loading Inter-Carrier Accounting Configurations, page 346](#)
- [Verifying and Monitoring, page 346](#)

Configuring an MTP3 Inter-Carrier Accounting Billing Account

You can set up an Inter-Carrier Accounting billing account based on MTP3, SCCP, or a combination of both. Either account type can also be configured for SMS Traffic Accounting. The procedure shown below configures an MTP3 account.

CONFIGURATION STEPS

	Command or Action	Purpose
Step 1	enable Example: ITP> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: ITP# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	cs7 [instance <i>instance-number</i>] linkset <i>ls-name</i> <i>adj-pc</i> [local-pc <i>pc</i>] Example: ITP(config)# cs7 instance 0 linkset LINKSET_01 2.179.0	Specifies a linkset and enter cs7 linkset submode: <i>instance-number</i>—The range is from 0 to 7. The default instance is 0. <i>ls-name</i>—Name of the linkset. (Linkset names are case-specific.) <i>adj-pc</i>—Point code of the adjacent signaling point. local-pc—(Optional) Specifies a secondary point code, which functions as a second linkset between the ITP and the adjacent node. <i>pc</i>—Either the ITP's primary or secondary point code. By default, it is the primary point code.
Step 4	link <i>slc</i> [<i>name</i>] sctp <i>remote-ip-addr</i> [<i>remote-ip-addr</i> ...] <i>remote-port-num</i> <i>local-port-num</i> Example: ITP(config-cs7-ls)# link 0 sctp LINKSET_02 24879 24879	Configures an SS7 link: <i>slc</i>—Signal Link Code. Range is from 0 to 15. The <i>slc</i> value uniquely identifies this link within the linkset. The <i>slc</i> value must match the value configured on the partner node for this link. <i>name</i>—Name of the group peer on which the link physically resides. The <i>name</i> parameter is valid (and required) only if the ITP Group feature has been configured. sctp—Specifies Stream Control Transmission Protocol. <i>remote-ip-addr</i>—Remote IP address that is one of the four IP addresses configured as local IP addresses on the remote peer. At least one, and up to four, remote IP addresses can be specified. <i>remote-port-num</i>—Remote port number (the local port number configured on the remote ITP). <i>local-port-num</i>—Local port number.
Step 5	exit Example: ITP(config-cs7-ls)# exit	Exits submode.
Step 6	cs7 [instance <i>instance-number</i>] billing pc-table <i>pctbl_name</i> {mtp3 sccp sms_sccp} Example: ITP(config)# cs7 instance 0 billing pc-table PCTBL_01 mtp3	Configures a one point code table used in billing criteria: <i>pctbl_name</i>—Name of the PC table. mtp3—Specifies that the PC table is defined as the MTP3 type. sccp—Specifies that the PC table is defined as the SCCP type. sms_sccp—Specifies that the PC table is defined as the SMS type.

	Command or Action	Purpose
Step 7	point-code <i>point-code</i> si <i>si-number</i> Example: ITP(cfg-billing-pctbl-mtp3)# point-code 1.1.1 si 11	Configures the billing PC table entry when the PC table type is MTP3: <i>point-code</i>—Point code of table entry. si—Specifies Service indicator. <i>si-number</i>—Service indicator number.
Step 8	point-code <i>point-code</i> si <i>si-number</i> Example: ITP(cfg-billing-pctbl-mtp3)# point-code 1.1.2 si 12	Configures a second billing PC table entry when the PC table type is MTP3: <i>point-code</i>—Point code of table entry. si—Specifies the Service indicator. <i>si-number</i>—Service indicator number.
Step 9	exit Example: ITP(config-cs7-bt)# exit	Exits submode.
Step 10	cs7 [instance <i>instance</i>] billing account <i>billing-account-name</i> Example: ITP(config)# cs7 instance 0 billing account BILL_ACCNT	Configures and identifies a billing account and enters the cs7 billing account configuration submode.
Step 11	linkset <i>linkset_name</i> {inbound outbound} [type {mtp3 sccp sms_sccp}] {opc-table dpc-table} <i>pctbl_name</i> Example: ITP(cfg-billing-accnt)# linkset LINKSET_01 inbound type mtp3 opc-table PCTBL_01	Configures a criteria entry of a billing account: <i>linkset_name</i>—Name of the criteria entry. inbound—Inbound messages used for accounting criteria. outbound—Outbound messages used for accounting criteria. mtp3—Defines the potocol type for the accounting criteria as MTP3. sccp—Defines the potocol type for the accounting criteria as SCCP. sms_sccp—Defines the potocol type for the accounting criteria as SMS. opc-table—Originating point-code specified for the PC table. Ingress point code (OPC). dpc-table—Originating point-code specified for the PC table. Egress point code (DPC). <i>pctbl_name</i>—Name of PC table that will be associated with this entry.
Step 12	exit Example: ITP(config)# exit	Exits submode.

Inter-Carrier Accounting Billing Account Configured for MTP3 Example

In the following example, an Inter-Carrier Accounting billing account is configured for MTP3:

```
cs7 instance 0 linkset LINKSET_01 2.179.0
  link 0 sctp LINKSET_02 24879 24879

cs7 instance 0 billing pc-table PCTBL_01 mtp3
  point-code 1.1.1 si 11
  point-code 1.1.2 si 12

cs7 instance 0 billing account BILL_ACCNT
  linkset LINKSET_01 inbound type mtp3 opc-table PCTBL_01
```

Inter-Carrier Accounting Billing Account Configured for Both MTP3 and SCCP Example

In the following example, an Inter-Carrier Accounting billing account is configured for MTP3 and SCCP:

```
cs7 instance 0 linkset LINKSET_01 2.179.0
  link 0 sctp LINKSET_02 24879 24879

cs7 instance 0 linkset to_2800-10 2.149.0
  link 0 sctp 10.74.50.149 24849 24849

cs7 instance 0 billing pc-table PCTBL_01 mtp3
  point-code 1.1.1 si 11
  point-code 1.1.2 si 12

cs7 instance 0 billing pc-table PCTBL_02 sccp
  point-code 2.2.1 ssn 8 gta 12345 tt 0 gti 2
  point-code 2.2.2 ssn 8 gta 67890 tt 0 gti 4 np 4 nai 2

cs7 instance 0 billing account BILL_ACCNT
  linkset LINKSET_01 inbound type mtp3 opc-table PCTBL_01
  linkset LINKSET_02 outbound type sccp dpc-table PCTBL_02
```

Configuring an SCCP Inter-Carrier Accounting Billing Account

This procedure configures an Inter-Carrier Accounting Billing Account using SCCP.

CONFIGURATION STEPS

	Command or Action	Purpose
Step 1	enable Example: ITP> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: ITP# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	cs7 [instance <i>instance-number</i>] linkset <i>ls-name</i> <i>adj-pc</i> [local-pc <i>pc</i>] Example: ITP(config)# cs7 instance 0 linkset to_2800-10 2.149.0	Specifies a linkset and enter cs7 linkset submode: <i>instance-number</i>—The range is from 0 to 7. The default is 0. <i>ls-name</i>—Name of the linkset. (Linkset names are case-specific.) <i>adj-pc</i>—Point code of the adjacent signaling point. local-pc—(Optional) Specifies the secondary point code, which functions as a second linkset between the ITP and the adjacent node. <i>pc</i>—Either the ITP's primary or secondary point code. By default, it is the primary point code.
Step 4	link <i>slc</i> [<i>name</i>] sctp <i>remote-ip-addr</i> [<i>remote-ip-addr</i> ...] <i>remote-port-num</i> <i>local-port-num</i> Example: ITP(config-cs7-ls)# link 0 sctp 10.74.50.149 24849 24849	Configures an SS7 link: <i>slc</i>—Signal Link Code. The range is from 0 to 15. The <i>slc</i> value uniquely identifies this link within the linkset. The <i>slc</i> value must match the value configured on the partner node for this link. <i>name</i>—Name of the group peer on which the link physically resides. The <i>name</i> parameter is valid (and required) only if the ITP Group feature has been configured. sctp—Specifies Stream Control Transmission Protocol. <i>remote-ip-addr</i>—Remote IP address that is one of the four IP addresses configured as local IP addresses on the remote peer. At least one, and up to four, remote IP addresses can be specified. <i>remote-port-num</i>—Remote port number (the local port number configured on the remote ITP). <i>local-port-num</i>—Local port number.
Step 5	exit Example: ITP(config-cs7-ls)# exit	Exits submode.
Step 6	cs7 [instance <i>instance-number</i>] billing pc-table <i>pctbl_name</i> {mtp3 sccp sms_sccp} Example: ITP(config)# cs7 instance 0 billing pc-table PCTBL_02 sccp	Configures a one point code table used in billing criteria: <i>pctbl_name</i>—Name of the PC table. mtp3—Specifies that the PC table is defined as the MTP3 type. sccp—Specifies that the PC table is defined as the SCCP type. sms_sccp—Specifies that the PC table is defined as the SMS type.

	Command or Action	Purpose
Step 7	point-code <i>point-code</i> [ssn <i>ssn-number</i>] [gta <i>gta-number</i> tt <i>tt-number</i> gti <i>gti-number</i>] Example: ITP(cfg-billing-pctbl-sccp)# point-code 2.2.1 ssn 8 gta 12345 tt 0 gti 2	Configures the billing PC table entry when the PC table type is SCCP: <i>point-code</i>—Point code of table entry. <i>ssn-number</i>—Sub-System Number (0-255) <i>gta-number</i>—Global Title Address number (1 to 15 hex digits) <i>tt-number</i>—Translation Type number (0-255) <i>gti-number</i>—Global Title Indicator number (2 or 4) <i>np-number</i>—National Plan number (0-15) <i>nai-number</i>—Nature of Address Indicator number (0-127)
Step 8	point-code <i>point-code</i> [ssn <i>ssn-number</i>] [gta <i>gta-number</i> tt <i>tt-number</i> gti <i>gti-number</i>] [np <i>np-number</i>] [nai <i>nai-number</i>] Example: ITP(cfg-billing-pctbl-sccp)# point-code 2.2.2 ssn 8 gta 67890 tt 0 gti 4 np 4 nai 2	Configures a second billing PC table entry when the PC table type is SCCP: <i>point-code</i>—Point code of table entry. <i>ssn-number</i>—Sub-System Number (0-255) <i>gta-number</i>—Global Title Address number (1 to 15 hex digits) <i>tt-number</i>—Translation Type number (0-255) <i>gti-number</i>—Global Title Indicator number (2 or 4) <i>np-number</i>—National Plan number (0-15) <i>nai-number</i>—Nature of Address Indicator number (0-127)
Step 9	exit Example: ITP(config-cs7-bt)# exit	Exits submode.
Step 10	cs7 [instance <i>instance</i>] billing account <i>billing-account-name</i> Example: ITP(config)# cs7 instance 0 billing account BILL_ACCNT	Configures and identifies a billing account and enters the cs7 billing account configuration submode.

Command or Action	Purpose
Step 11 <pre>linkset linkset_name {inbound outbound} [type {mtp3 sccp sms_sccp}] {opc-table dpc-table} pctl_name</pre> Example: ITP(cfg-billing-accnt)# linkset LINKSET_02 outbound type sccp dpc-table PCTBL_02  Note If you are configuring the cs7 billing account for the SMS protocol, the criteria can only be defined on the inbound interface.	Configures a criteria entry of a billing account: <i>linkset_name</i>—Name of the criteria entry. inbound—Inbound messages used for accounting criteria. outbound—Outbound messages used for accounting criteria. mtp3—Defines MTP3 as the potocol type for the accounting criteria. sccp—Defines SCCP as the potocol type for the accounting criteria. sms_sccp—Defines SMS as the potocol type for the accounting criteria. opc-table—Originating point-code specified for the PC table. Ingress point code is OPC. dpc-table—Destination point-code specified for the PC table. Egress point code is DPC. <i>pctl_name</i>—Name of PC table that will be associated with this entry.
Step 12 <pre>exit</pre> Example: ITP(config)# exit	Exits submode.

Example

In this example an Inter-Carrier Accounting billing account is configured for SCCP:

```
cs7 instance 0 linkset to_2800-10 2.149.0
  link 0 sctp 10.74.50.149 24849 24849

cs7 instance 0 billing pc-table PCTBL_02 sccp
  point-code 2.2.1 ssn 8 gta 12345 tt 0 gti 2
  point-code 2.2.2 ssn 8 gta 67890 tt 0 gti 4 np 4 nai 2

cs7 instance 0 billing account BILL_ACCNT
  linkset LINKSET_02 outbound type sccp dpc-table PCTBL_02
```

In this example, an Inter-Carrier billing account is configured for SMS:

```
cs7 instance 0 billing pc-table PCTBL_01 sms_sccp
  point-code 1.11.0 ssn 3
  point-code 1.11.5 ssn 11

cs7 instance 0 billing pc-table PCTBL_02 sms_sccp
  point-code 1.13.0 ssn 5
  point-code 1.13.1 sss 5

cs7 instance 0 billing account BILL_ACCNT-AT-1
  linkset hsl_tg13_FW1 inbound type sms_sccp opc-table PCTBL_01
  linkset m2pa_tg11_9_3 inbound type sms_sccp opc-table PCTBL_02
```

Configuring Inter-Carrier Accounting Data Collection

You can configure several accounting data options for Inter-Carrier Accounting. This procedure details this configuration:

CONFIGURATION STEPS

	Command or Action	Purpose
Step 1	enable Example: ITP> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: ITP# configure terminal	Enters global configuration mode.
Step 3	cs7 billing options Example: ITP(config)# cs7 billing options	Enables the user to configure options for the billing account and enters the billing option configuration submode.
Step 4	rx-per-tx times Example: ITP(config-options-entry)# rx-per-tx 12	(Optional) Time of data collection in a data storage interval: <i>times</i> —Times of data collection (3-1024).
Step 5	rx-interval seconds Example: ITP(config-options-entry)# rx-interval 300	(Optional) Sets interval for a time of data collection: <i>seconds</i> —Seconds of interval (30-86400)
Step 6	backstore [order][url] Example: ITP(config-options-entry)# backstore 0 ftp://admin:admin@192.168.1.2/itp_billing.dat	(Optional) Sets the location and order of the back storage files: <i>order</i> —Order of trying current back storage among all back storages (0-1). <i>url</i> —The URL location of the back storage file.
Step 7	bak-file-num num Example: ITP(config-options-entry)# bak-file-num 2	(Optional) Sets the backup file number. <i>num</i> —backup file number in data saving destination (1-1024)
Step 8	exit Example: ITP(config-options-entry)# exit	Exits submode.

Example

In this example, Inter-Carrier Accounting options are configured:

```
(config)#cs7 billing options
(config-optns-entry)# rx-per-tx 12
(config-optns-entry)# rx-interval 300
(config-optns-entry)# backstore 0 ftp://admin:admin@192.168.1.2/itp_billing.dat
(config-optns-entry)# backstore 1 disk0:itp_billing.bak
(config-optns-entry)# bak-file-num 2
```

Saving and Loading Inter-Carrier Accounting Configurations

You can configure the saving and loading of Inter-Carrier Accounting billing configurations. This procedure details these operations:

CONFIGURATION STEPS

	Command or Action	Purpose
Step 1	enable Example: ITP> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: ITP# configure terminal	Enters global configuration mode.
Step 3	cs7 save billing-cfg url Example: ITP(config)# cs7 save billing config disk0:itp-billing.cfg	Saves the current billing configuration to a specified URL: <i>url</i> —The location of the saved billing configuration.
Step 4	cs7 billing load url [execute] Example: ITP(config)# cs7 billing load disk0:itp_billing.cfg	Loads the stored billing configuration: <i>url</i> —The location of the saved billing configuration. execute —Specifies that the stored billing configuration is immediately applied. The default is to apply the configuration after the next system reboot.

Example

In this example, the saving and loading of an Inter-Carrier Accounting billing configuration file is shown:

```
enable
cs7 save billing-cfg disk0:itp-billing.cfg
config terminal
cs7 billing load disk0:itp_billing.cfg
```

Verifying and Monitoring

To verify Inter-Carrier Accounting billing configurations, use the following commands in EXEC mode:

Command	Purpose
ITP# show cs7 billing configuration [account <i>account-name</i> pc-table options load]	Displays the cs7 billing configuration.
ITP# show cs7 billing statistics	Displays the latest collected billing statistics.



Summary Routing and ANSI Cluster Routing

The Summary Routing feature allows routing of MSUs to groups of DPCs by specifying one or more routes to a summary destination in the route table rather than individual route table entries for each destination.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



Note

Configuration Mode Restrictions: Simultaneous changes to the configuration from multiple CLI sessions are not supported. Only one configuration session is allowed to enter in configuration mode at a time; other sessions should not enter in configuration mode. The **show line** or **show users EXEC** command may be used to determine the active user sessions on an ITP, and the **clear line EXEC** command may be used to ensure that only a single active session exists.

Contents

- [Information About Summary Routing and ANSI Cluster Routing, page 350](#)
- [How to Configure Summary Routes, page 353](#)
- [How to Configure ANSI Cluster Routing, page 355](#)

Information About Summary Routing and ANSI Cluster Routing

The Summary Routing feature allows routing of MSUs to groups of DPCs by specifying one or more routes to a summary destination in the route table rather than individual route table entries for each destination.

Typically a route table has primary (or normal) routes and alternate routes of lower priority to fully qualified (or full PC) destinations. A fully qualified destination has all significant bits in the point code explicitly specified. Summary Routing is the capability of using partly qualified destinations in the route table, where one or more trailing bits in the point code are left unspecified, to refer collectively to all the fully qualified destinations that have any combination of bits within the unspecified portion.

This overview begins with a fictional scenario that explains how fully-qualified point codes are assigned and how partly-qualified point codes are derived. The remainder of the overview covers in greater detail the function of summary routing and the routing table.

How Point Codes Are Used in Summary Routing

To examine how point codes are used in Summary Routing, consider the following example for a company in France we will call Voila. This example uses the ITU standard for point codes, which uses 3 bits to indicate the zone, 8 bits to indicate the region, and 3 bits to indicate the signaling point (SP).

Assigning Point Codes

When Voila acquired its block of point codes, the zone segment was preassigned to be 5, or 101 binary. The network administrator at Voila wanted to take advantage of Summary Routing and so devised the following numbering strategy for assigning the region and SP segments of the point codes:

- In the Ile-De-France region the region segment of the point code would begin with 00 binary.
- In the Normandy region the region segment would begin with 01 binary.
- In the Brittany region, the region segment would begin with 10 binary. The SP segments would be numbered sequentially.

Focusing on Ile-De-France, we can see that numbering the region segment 00xxxxxx binary provides the range of numbers 0 through 63 decimal. Within this numbering system, the network administrator further decided to provision point codes in the city of Paris to have a region segment of 42 or 00101010 binary. SPs would be numbered sequentially.

The following table shows a partial list of point codes in the Voila network:

Table 0-25 Sample Point Code Numbering Plan

Location	Device	Point Code
Paris	ITP-P1	5.42.1
Paris	ITP-P2	5.42.2
Paris	MSC-P1	5.42.3
Paris	MSC-P2	5.42.4
Paris	SMSC-P1	5.42.5
Meudon	HLR-P1	5.50.1
Normandy	ITP-N1	5.91.1
Normandy	ITP-N2	5.91.2

Table 0-25 Sample Point Code Numbering Plan (continued)

Location	Device	Point Code
Normandy	MSC-N1	5.91.3
Normandy	SMSC-N2	5.91.4
Brittany	ITP-B1	5.149.1
Brittany	ITP-B2	5.149.2

Specifying Summary Destinations

In our example, the Voila network administrator assigned point codes in a way that can take advantage of the Summary Routing feature. Consider the point codes assigned to the three regions in France. All point codes belonging to each of these groups have in common the first 5 bits of the point code. For example, ITP-P1 in Paris and HLR-P1 in Meudon are both assigned point codes that belong to the same region, as defined by the network administrator.

The point code for MSC-P1 in Paris is 5.42.3, shown in binary format below:

1	0	1	0	0	1	0	1	0	1	0	0	1	1

The point code for HLR-P1 in the Paris suburb of Meudon is 5.50.1, shown in binary format below:

1	0	1	0	0	1	1	0	0	1	0	0	0	1

The first 5 characters of the point codes are the same for both destinations and for all of the fully qualified destinations in the region. This commonality can be expressed as a partly-qualified destination with the point code and mask 5.0.0 7.192.0 (or the equivalent expression 5.0.0/5). This partly qualified destination means “consider the first 5 bits in the point code (the mask 7.192.0 and /5 both mean the first 5 bits) and include all point codes with the zone segment equal to 5 and the region segment in the range 0 (all 8 bits off = 0) through (first 2 region bits off and the remaining 6 bits on = 63).”

Examine the point codes for Normandy and Brittany, and notice that all of these point codes can be identified by the partly-qualified destinations 5.64.0/5 (Normandy) and 5.128.0/5 (Brittany). The first two bits in the region segment for Normandy are 01, so the range of numbers in the Normandy region segment will be 64 through 127. The first two bits in the region segment for Brittany are 11, so the range of numbers in the Brittany region segment will be 128 through 255.

Summary Routes and the Routing Table

Summary routes are used primarily to reduce the number of route table entries. Summary Routing allows an easy translation of the hierarchy in the network topology into the logical organization of the route table. For example, a remote set of nodes with DPCs 1.*.* (where * is a number in the appropriate range for ITU or ANSI) can be reached by creating a set of routes to 1.0.0/3 (ITU), or 1.0.0/8 (ANSI), only. There is no need to create individual routes to all the dozens of destinations 1.*.* that may be present in the network, particularly if all those destinations can be reached by the same set of linksets in the same order of priority. If there happens to be a member within 1.*.*, say 1.6.7, routes to which do not share some or all the linksets with the routes to the summary destination, then it is possible to configure routes to 1.6.7 using these different linkset(s) along with the summary routes that covers all the other point codes within 1.*.*. Such a configuration would be displayed as follows:

```
Router# show cs7 route detailed
Routing table = system
C=Cong Q=QoS P=Prio
Destination      C  Q  P Linkset Name      Linkset Non-adj Route
-----
1.6.7/14         acces  2  sirius             avail    allowed avail
                  3  castor             avail    allowed avail
                  4  pollux             avail    allowed avail
1.0.0/3          acces  2  polaris            avail    avail
                  3  pollux             avail    avail
```

Summary routes can coexist with fully qualified routes. In the presence of a configured full PC member, summary routes behave as alternate routes that have priority lower than that of fully qualified alternate routes.

When a route has to be selected for an outbound MSU, the route table is searched for a full point code entry matching the DPC in order of route priority. If any route to the full PC is configured and available, it is chosen for routing, otherwise the route table is searched for the next best partial match with a shorter mask length. If a summary route is configured and it is available, then this route is chosen for routing, otherwise the search continues. The search ends after mask length zero yields no route.

If a message is received for routing to an unconfigured destination Y that is a member of a summary destination and that summary destination is inaccessible, then the Response Method will be used to send a TFP concerning Y. Likewise, if the summary destination is restricted a TFR will be sent. If a route-set test message (Route Processor/RST or RSR) is received concerning a destination Y that is a member of a summary route, then a response will be sent concerning Y depending on the status of that summary route.

Routes to 0.0.0/0 are system wide default routes that behave as alternate routes to all the fully or partly qualified routes configured in the system. The linkset that goes between a mated pair of ITPs is such a default route from the perspective of each of those ITPs. There is no special external route management messages for the support of summary routes (the ANSI cluster routing case is an exception, see below).

There are no route management messages exchanged between network elements to maintain summary route status except the usual TFP, TFR, TFA, Route Processor/RST and RSR. When a TFP is received on a certain route (i.e. a certain linkset leading to an adjacent point code) concerning a point-code, say 1.6.1 in the above example, and that point-code is not configured, and there is a summary route configured and available on that linkset, route table entries are created dynamically for the concerned point-code by copying the summary routes. The concerned route is marked prohibited. Future traffic is blocked for 1.6.1 but allowed for all other members of the summary route 1.6.0/11. Route set test is started. When a TFA is received on the same route, and all the other dynamic routes to the concerned point-code have non-adjacent status available, then all the dynamic routes are removed. Dynamic routes are also created when a TFR is received, and traffic for that route is affected as for any other restricted route. Route set restricted test is started.

In the previous example if routes to the concerned point code were configured, none being the route to which the TFP/TFR pertains, and these routes are all unavailable, then a single dynamic route is created with priority value one more than the highest configured. If a route with priority 9 were to already exist then the dynamic route cannot be added. It is therefore necessary to keep the priority value of the lowest priority configured route at, say, 6 or below when a configured full point-code route is using summary routes.

Dynamic routes are also created when TFC concerning a destination is received and summary routes to that destination exist in the route table. When the Route set congestion test procedure eventually brings the destination congestion status to zero, these dynamic routes are removed.

Dynamic routes cannot be removed using the **no update route** command. There is a periodic audit of the route table that runs once a day at 3:00 a.m. to remove dynamic entries older than 12 hours. This mechanism allows dynamic routes to remain in the system between 12 and 36 hours (24 hours average). For this audit to work properly, the system time-of-day clock and time zone must be set. When the route table is saved to file, dynamic routes are not included.

How to Configure Summary Routes

You can create a summary route by entering the **update route** command and specifying a mask length value that is less than that for a full point code. The mask length is in the range 0 through 13 for ITU, and 0 through 15, and 17 through 23 for ANSI. For ANSI, mask length 16 is for cluster routes.

To create a summary route, enter the following command, starting in global configuration mode:

Command	Purpose
Router(config)# cs7 route-table system	Specifies the name of the route table and enters route table configuration mode.
Router(config-cs7-rt)# update route point-code [mask length] linkset ls-name [priority priority-value¹] [qos-class {class default}] [load_balance]	Adds a summary route to the table.

1. The smaller the number, the higher the priority. See the **update route** ITP Command Set entry for an example.

For example, the following two configurations show equivalent ways to specify a summary route when the variant is **ITU**:

```
Router(config)# cs7 route-table system
Router(config-cs7-rt)# update route 1.6.0/11 linkset polaris prio 2
Router(config-cs7-rt)# update route 1.6.0/11 linkset pollux prio 3
Router(config-cs7-rt)# end
```

OR

```
Router(config)# cs7 route-table system
Router(config-cs7-rt)# update route 1.6.0 7.255.0 linkset polaris prio 2
Router(config-cs7-rt)# update route 1.6.0 7.255.0 linkset pollux prio 3
Router(config-cs7-rt)# end
```

The following two configurations show equivalent ways to specify a summary route when the variant is **ANSI**:

```
Router(config)# cs7 route-table system
Router(config-cs7-rt)# update route 1.6.0/17 linkset polaris prio 2
Router(config-cs7-rt)# update route 1.6.0/17 linkset pollux prio 3
Router(config-cs7-rt)# end
```

OR,

```
Router(config)# cs7 route-table system
Router(config-cs7-rt)# update route 1.6.0 255.255.128 linkset polaris prio 2
Router(config-cs7-rt)# update route 1.6.0 255.255.128 linkset pollux prio 3
Router(config-cs7-rt)# end
```

ITU users should set the point code format to suit their national numbering structure and hierarchy using the **cs7 point-code format** command. This will allow them to create summary destinations with mask lengths that conveniently terminate on the point-code delimiters.

A sample route table display for an ITU case with summary routes is shown below for the default format (3 bit - 8 bit - 3 bit):

```
Router# show cs7 route detailed
Routing table = system
C=Cong Q=QoS P=Prio
Destination      C  Q  P Linkset Name      Linkset Non-adj Route
-----
1.4.0/11         RESTR      2  polaris          UNAVAIL          UNAVAIL
                  3  pollux          avail            avail
1.5.1/14         INACC      1  polaris          UNAVAIL allowed UNAVAIL
1.5.3/14         acces     1  pollux          avail allowed avail
1.6.1/14         RESTR      2  polaris          UNAVAIL allowed UNAVAIL dyn
                  3  pollux          avail PROHIB UNAVAIL dyn
1.6.3/14         RESTR      2  polaris          UNAVAIL allowed UNAVAIL dyn
                  3  pollux          avail PROHIB UNAVAIL dyn
1.6.0/11         RESTR      2  polaris          UNAVAIL          UNAVAIL
                  3  pollux          avail            avail
```

The non-adjacent status field is blank for summary routes. Since there are no route management messages exchanged for such routes, there is no non-adjacent status. The availability of a summary route is determined solely by the linkset status. Dynamic route table entries are flagged by **dyn** at the end of the line. Although all routes to 1.6.1 and 1.6.3 are unavailable, the destination status is restricted (instead of inaccessible) because these destinations are members of the summary route 1.6.0/11, one route to which is available. Routes to 1.6.0/11 are considered to be alternate routes to 1.6.1 and 1.6.3.

Use the **show cs7 route** command with the keyword **summary-routes** to display all summary routes of which the given point code is a member:

```
Router# show cs7 route 1.6.1 summary-routes detailed
Routing table = system
C=Cong Q=QoS P=Prio
Destination      C  Q  P Linkset Name      Linkset Non-adj Route
-----
1.6.1/14         RESTR      2  polaris          UNAVAIL allowed UNAVAIL dyn
                  3  pollux          avail PROHIB UNAVAIL dyn
1.6.0/11         RESTR      2  polaris          UNAVAIL allowed UNAVAIL
                  3  pollux          avail allowed avail
```

To turn off usage of the summary routes for routing MSUs, when configured full point-code routes exist and are unavailable, use the following command in global configuration mode:

Command	Purpose
Router(config)# cs7 summary-routing-exception	Turns off usage of the summary routes.

The summary routes will be used as a default. To restore the default use the **no cs7 summary-routing-exception** global configuration command.

To configure the maximum number of dynamic routes that can be created by the system, use the following command in global configuration mode:

Command	Purpose
Router(config)# cs7 max-dynamic-routes <i>number</i>	Specifies the maximum number of dynamic routes that can be created by the system. The valid range is 100 through 1000. The default is 500.

To restore the default use the **no cs7 max-dynamic-routes** global configuration command.

How to Configure ANSI Cluster Routing

ANSI Cluster Routing is a special case of Summary Routing, and has associated with it a dedicated set of route management messages and procedures as specified in T1.111 and GR-82. If the variant is ANSI, a cluster route would be created by specifying a mask length of 16 or a mask of 255.255.0 using the default point-code format 8 bit - 8 bit - 8 bit. Cluster Routing and Management Diversity (CRMD) as specified in GR-82 is supported. When a route is configured to a member of a remote cluster using a direct E-link, the route is automatically assigned a priority of 1, contrary to an example in GR-82.

Cluster routes are created by specifying a mask length of 16, or mask 255.255.0:

Command	Purpose
Router(config)# cs7 route-table <i>system</i>	Specifies the name of the route table and enters route table configuration mode.
Router(config-cs7-rt)# update route <i>point-code</i> {[255.255.0 /16 linkset <i>ls-name</i> prio <i>priority-value</i>	Specifies a cluster route.

The following is an example of a cluster route configured using the **/16** form to specify the mask:

```
Router(config)# cs7 route-table system
Router(config-cs7-rt)# update route 1.6.0/16 linkset polaris prio 2
Router(config-cs7-rt)# update route 1.6.0/16 linkset pollux prio 3
Router(config-cs7-rt)# end
```

Cluster routes have a non-adjacent status as dictated by the last received TCP, TCR or TCA message on that route. In the output of the **show cs7 route detailed** command, this status is displayed just as for full pc routes. Exclusion list (x-list) members are flagged by **dyn** at the end of the line for the concerned route. A route table display for an ANSI case with two clusters (1.4.0 and 1.6.0) and two x-list members (1.6.1 and 1.6.3) is shown below:

Router# **show cs7 route detailed**

Routing table = system

C=Cong Q=QoS P=Prio

Destination	C	Q	P	Linkset Name	Linkset	Non-adj	Route
1.4.0/16	RESTR		2	polaris	UNAVAIL	allowed	UNAVAIL
			3	pollux	avail	allowed	avail
1.5.1/24	INACC		1	polaris	UNAVAIL	allowed	UNAVAIL
1.5.3/24	acces		1	pollux	avail	allowed	avail
1.6.1/24	RESTR		2	polaris	UNAVAIL	allowed	UNAVAIL dyn
			3	pollux	avail	PROHIB	UNAVAIL dyn
1.6.3/24	RESTR		2	polaris	UNAVAIL	allowed	UNAVAIL dyn
			3	pollux	avail	PROHIB	UNAVAIL dyn
1.6.0/16	RESTR		2	polaris	UNAVAIL	allowed	UNAVAIL
			3	pollux	avail	allowed	avail

If a cluster route is configured then another summary route with mask length in the range 17 - 23 should not be created. In the example above, the presence of a summary route 1.6.128/17 would cause faulty operation.



Verifying, Monitoring, and Tuning the ITP

This chapter describes how to verify proper configuration of the ITP, monitor status and traffic, and tune the ITP. This chapter includes the following optional tasks:

- [Verifying ITP, page 357](#)
- [Monitoring ITP, page 369](#)
- [Tuning ITP, page 394](#)

Feature History for Verifying, Monitoring, and Tuning the ITP

Release	Modification



Note

Configuration Mode Restrictions: Simultaneous changes to the configuration from multiple CLI sessions are not supported. Only one configuration session is allowed to enter in configuration mode at a time; other sessions should not enter in configuration mode. The **show line** or **show users EXEC** command may be used to determine the active user sessions on an ITP, and the **clear line EXEC** command may be used to ensure that only a single active session exists.

Verifying ITP

After you have configured Cisco ITP, you can perform several tasks that will verify that the Cisco ITP was installed and configured properly, and that Cisco ITP functionality is available. Perform the tasks in this section to verify the Cisco ITP.

Verify that Cisco ITP is configured on the router with the correct variant and local point code.

To confirm that the correct variant and point code are configured, use the following command in EXEC mode:

Command	Purpose
Router# write term	Displays the configuration.

The output of the above command should include lines such as the following that show the correct variant and point code:

```
cs7 variant ITU
cs7 point-code 1.1.1
```

Verify that required linksets to adjacent nodes are available.

To verify that required linksets to adjacent nodes are available, use the following command in EXEC mode:

Command	Purpose
Router# show cs7 linkset brief	Displays ITP linkset information.

The possible states of a linkset are:

- **UNAVAIL** Indicates the linkset does not have any “available” links and cannot transport traffic.
- **shutdown** Indicates the linkset has been shutdown in the configuration.
- **avail** Indicates the linkset has at least one available link and can carry traffic.

The output of the above command should include lines such as the following. The state of each linkset should be “avail.”

```
Router# show cs7 linkset brief
lsn=mscl      apc=5.5.5      state=avail
lsn=mica      apc=4.4.4      state=avail
lsn=malo      apc=2.2.2      state=avail
lsn=momo      apc=3.3.3      state=avail
```

If the state of a linkset is not available it might be shutdown or UNAVAIL:

```
lsn=momo      apc=3.3.3      state=shutdown
lsn=momo      apc=3.3.3      state=UNAVAIL
```

If the linkset state is shutdown, it should be administratively restarted. If a linkset is unavailable, verify the links within the linkset (See step 4).

Verify that all required destinations are accessible.

To verify that all required destinations are accessible, use the following command in EXEC mode:

Command	Purpose
Router# show cs7 route	Displays the ITP routing table.

The above command should include output such as the following. Each destination should be “access” and the route status should be “avail.”

```
Router# show cs7 route
Routing table = system
Destination          Prio Linkset Name      Route Status
-----
2.2.2/14             acces  1  malo              avail
                      9  mica              avail
3.3.3/14             acces  1  momo              avail
                      9  mica              avail
4.4.4/14             acces  1  mica              avail
                      9  momo              avail
5.5.1/14             acces  1  msc1              avail
                      9  momo              avail
5.5.5/14             acces  1  msc1              avail
                      9  momo              avail
6.6.1/14             acces  1  mica              avail
                      9  malo              avail
6.6.6/14             acces  1  malo              avail
                      9  mica              avail
```

Routes to a destination are listed in priority order. The first route to be selected is the route with the lowest cost (listed in the Prio field). If the route with the lowest cost is available the destination is available. If the route with the lowest cost is UNAVAIL or RESTRIC and there is another available route with a higher cost, then the destination will be RESTR.

```
3.3.3/14             RESTR  1  momo              UNAVAIL
                      9  mica              avail
```

If there are no available routes, the destination will be INACC.

```
5.5.1/14             INACC  1  msc1              UNAVAIL
                      9  momo              UNAVAIL
```

If a destination is inaccessible or restricted, investigate why by verifying the affected cs7 route.

If a required destination is not shown, the route should be administratively added to the route table.

If steps 1 - 3 yield the expected results, you have verified connectivity to all the adjacent nodes and *potentially* available routes to all destinations. (*Potentially* because Cisco ITP assumes that routes are available until the node is notified that a destination is not available.)

To verify connectivity to a particular node, use the following command in EXEC mode:

Command	Purpose
Router# ping cs7 [instance-number] [-opc origination-point-code] [-duration seconds] [-ni network-indicator] [-rate MSU-per-second] [-size bytes] [-sls value round-robin] {destination-point-code host}	Verify that you can reach ITP nodes.

The following is typical output of the **cs7 ping** command:

```
Router# ping cs7 2.2.2
3d19h:%CS7PING-6-RTT:Test Q.755 2.2.2:MTP Traffic test rtt 16/16/16
3d19h:%CS7PING-6-STAT:Test Q.755 2.2.2:MTP Traffic test 100% successful (1/1)
3d19h:%CS7PING-6-TERM:Test Q.755 2.2.2:MTP Traffic test terminated.
```

Verify the links within a linkset.

To verify that all the links in a linkset are available, use the following command in EXEC mode:

Command	Purpose
Router# show cs7 linkset	Displays the ITP linkset information.

The possible states of a linkset are:

- **UNAVAIL** Indicates the linkset does not have any “available” links and cannot transport traffic.
- **shutdown** Indicates the linkset has been shutdown in the configuration.
- **avail** Indicates the linkset has at least one available link and can carry traffic.

The possible states of a link are:

- **UNAVAIL** Indicates the link is not available to carry traffic. This can occur if the link is remotely or locally inhibited by a user. It can also be unavailable if MTP2/M2PA has not been able to successfully activate the link connection or the link test messages sent by MTP3 are not being acknowledged.
- **shutdown** Indicates the link has been shutdown in the configuration. A link is **shutdown** when it is shutdown at the MTP3 layer.
- **avail** Indicates the link is active and able to transport traffic.
- **FAILED** A link is **FAILED** when the link is not shutdown but is unavailable at layer2 for some reason. It is **FAILED** when the link is unavailable because the link has been inhibited or it is blocked.
- **sys-shutdown** Indicates the link has been shutdown by the system. A link may be in this state when:
 - MTP3 offload is configured and the system is performing error recovery on the FlexWAN
 - MTP3 offload has been permanently disabled on a FlexWAN by the system due to excessive errors. When MTP3 offload has been permanently disabled on a FlexWAN (by the system) all links on that FlexWAN will be in the sys-shutdown state.
 - The Service field should indicate that links are “avail.”

```

Router# show cs7 linkset
lsn=mscl          apc=5.5.5          state=avail
  SLC  Interface          Service  PeerState  Inhib
  00   199.1.1.5 4096 4096    avail    InService  -----

lsn=mica          apc=4.4.4          state=avail
  SLC  Interface          Service  PeerState  Inhib
  00   199.1.1.4 4096 4096    avail    InService  -----
  01   199.1.1.4 4097 4097    avail    InService  -----
  02   199.1.1.4 4098 4098    avail    InService  -----
  03   199.1.1.4 4099 4099    avail    InService  -----

lsn=malo          apc=2.2.2          state=avail
  SLC  Interface          Service  PeerState  Inhib
  00   199.1.1.2 4096 4096    avail    InService  -----

```

```
lsn=momo          apc=3.3.3          state=avail
SLC  Interface    Service  PeerState    Inhib
*00  Serial0/0     avail    -----     -----
*01  Serial0/1     avail    -----     -----
*02  Serial0/2     avail    -----     -----
03   Serial0/3     avail    -----     -----
```

If a link is not available it might be shutdown, FAILED or UNAVAIL....

```
*01  Serial0/1     shutdown -----     -----
*02  Serial0/2     FAILED    -----     -----
*03  Serial0/3     UNAVAIL   -----     rem
```

If the link is shutdown, it should be administratively restarted.

If a link is failed, then the link has failed at MTP2 (or M2PA in the case of SCTP links). The cause must be investigated by verifying MTP2 (or M2PA) links.

If the link is unavailable, the link is okay at the MTP2 (or M2PA) layer.

The link might be remotely inhibited or locally inhibited, or there may be a remote processor outage.

```
*03  Serial0/3     UNAVAIL   -----     loc
```

The above link was locally inhibited. The link should be administratively uninhibited.

```
*03  Serial0/3     UNAVAIL   -----     rem
```

The above link was remotely inhibited. The link should be administratively uninhibited by the SS7 node at the remote end of the link.

```
*03  Serial0/3     UNAVAIL   -----     -----
```

The above link is unavailable and is not inhibited. It is probably blocked due to remote processor outage. (i.e. The problem is at the SS7 node at the remote end of the link)

Verify routes.

To verify routes, use the following command in EXEC mode:

Command	Purpose
Router# show cs7 route detail	Displays details of the ITP routing table.

The **show cs7 route detail** command should include output such as the following:

```
Router# show cs7 route detail
Routing table = system
C=Cong Q=QoS P=Prio
Destination      C  Q  P  Linkset Name      Linkset  Non-adj  Route
-----
2.2.2/14         acces      1  malo              avail    allowed  avail
                  9  mica              avail    allowed  avail
3.3.3/14         acces      1  momo              avail    allowed  avail
                  9  mica              avail    PROHIB   UNAVAIL
4.4.4/14         acces      1  mica              avail    allowed  avail
                  9  momo              avail    RESTRIC  RESTRIC
5.5.1/14         INACC      1  msc1              avail    PROHIB   UNAVAIL
                  9  momo              avail    PROHIB   UNAVAIL
5.5.5/14         acces      1  msc1              avail    allowed  avail
                  9  momo              avail    allowed  avail
6.6.1/14         INACC      1  mica              avail    PROHIB   UNAVAIL
```

```

6.6.6/14      acces      9  malo      avail  PROHIB  UNAVAIL
                  1  malo      avail  allowed avail
                  9  mica      avail  allowed avail

```

Routes are listed in priority order. The route with the lowest cost (listed under the Prio heading) will be the first route selected to a particular destination. A route should be “avail,” the non-adj status should be “allowed” and the linkset should be “avail.”

If a route is not available, it may be restricted or unavailable. If a route is not available and the linkset is available, then the route is restricted or unavailable because it received a TFR or TFP from the adjacent SS7 node. In this case you need to verify the route in the adjacent SS7 node.

If a route is not available and the linkset is not available, verify the links within the linkset.

Verify MTP2 links

To Verify that the link state control is “In service,” use the following command in EXEC mode:

Command	Purpose
Router# show cs7 mtp2 state	Displays MTP2 state machine status.

The following is typical output of the **show cs7 mtp2 state** command:

```

Router# show cs7 mtp2 state ser 1/0/0:0
CS7 MTP2 states for interface Serial1/0/0:0
Protocol version for interface Serial1/0/0:0 is ITU-T Q.703 (1996) (White Book)

Link State Control (LSC)                = In Service
                                         ^^^^^^^^^^
Initial Alignment Control (IAC)          = Idle
Transmission Control (TXC)              = In Service
Reception Control (RC)                  = In Service
Signal Unit Error Rate Monitor (SUERM)   = Monitoring
Alignment Unit Error Rate Monitor (AERM) = Idle
Congestion (CONG)                       = Idle

Layer3 link status                      = Started
Layer3 congestion status                 = Abate

```

Other possibilities for LSC might be as follows:

```

Link State Control (LSC)                = Out of Service
or
Link State Control (LSC)                = Initial Alignment

```

If the LSC state is “Out of Service” or transitions in and out of “Initial alignment,” check the physical interface for correct cabling, clocking, etc.

To verify that the physical link is up, use the following command in EXEC mode:

Command	Purpose
Router# show interface	Displays MTP2 state machine status.

The following is typical output of the **show interface** command:

```
router# show int ser 0/0
Serial0/0 is up, line protocol is up
Hardware is PowerQUICC Serial
  MTU 290 bytes, BW 1544 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation SS7 MTP2, loopback not set
  Keepalive set (10 sec)
  Last input never, output 00:00:16, output hang never
  Last clearing of "show interface" counters 3d17h
  Queueing strategy:fifo
  Output queue 0/40, 0 drops; input queue 0/75, 20654 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    20673 packets input, 62068 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    10339 packets output, 113605 bytes, 0 underruns
    0 output errors, 0 collisions, 2 interface resets
    0 output buffer failures, 0 output buffers swapped out
    4 carrier transitions
  DCD=up DSR=up DTR=up RTS=up CTS=up
```

The output might indicate that the interface is administratively down:

```
Serial0/0 is administratively down, line protocol is down
```

If the interface is “administratively down,” the interface must be started administratively.

The output might indicate that the interface is down:

```
Serial0/0 is down, line protocol is down
```

If the interface is “down” check the physical cabling.

To verify that the line protocol is up and the encapsulation is MTP2, use the following command in EXEC mode:

Command	Purpose
Router# show interface	Displays MTP2 state machine status.

If the encapsulation is not MTP2, it must be changed administratively.

The following is typical output of the show interface command:

```
Router# show int ser 0/0
Serial0/0 is up, line protocol is up
      ^^
Hardware is PowerQUICC Serial
MTU 290 bytes, BW 1544 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation SS7 MTP2, loopback not set
^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
Keepalive set (10 sec)
Last input never, output 00:00:16, output hang never
Last clearing of "show interface" counters 3d17h
Queueing strategy:fifo
Output queue 0/40, 0 drops; input queue 0/75, 20654 drops
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  20673 packets input, 62068 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  10339 packets output, 113605 bytes, 0 underruns
    0 output errors, 0 collisions, 2 interface resets
    0 output buffer failures, 0 output buffers swapped out
    4 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=up
```

The output might indicate that the line protocol is down:

```
Serial0/0 is up, line protocol is down
```

If the line protocol is down verify that the physical cabling and clocking rates are correct.

Verify M2PA Links

To verify M2PA links, use the following command in EXEC mode:

Command	Purpose
Router# show cs7 linkset <i>ls-name</i>	Displays ITP linkset information.



Note

When an interface is already configured, do not change its IP address. Doing so can result in the crash and mismatch in the configuration of a linkset on the standby card. Memory corruption can also occur. Since the linkset already has a port configured, it will search for the old IP address and run into this issue. If you must change the IP address on a configured interface, first remove the linkset before changing the IP address.

The following is typical output of the **show cs7 linkset** command:

```
Router# show cs7 linkset mica
lsn=Router apc=4.4.4      state=UNAVAIL
  SLC  Interface          Service  PeerState  Inhib
  00   199.1.1.4 4096 4096    avail    InService  ----
      ^^^^^^^^^
  01   199.1.1.4 4097 4097    avail    InService  ----
  02   199.1.1.4 4098 4098    avail    InService  ----
  03   199.1.1.4 4099 4099    avail    InService  ----
```

If the PeerState field shows “InitialAlignment,” check that the remote peer IP address and port number are correct and that the link at the remote end is not administratively shutdown. The remote peer IP address and port number should correspond with a local peer and port number on a remote router.

```
01 199.1.1.4 4097 4098          FAILED InitialAlignment  -----
```

In the above example,

- 199.1.1.4 is the remote IP address
- 4097 is the remote port
- 4098 is the local port

Also check that the local peer IP address and port number correspond to the remote peer IP address and port number in the remote router.

To obtain the local peer IP address, use the following command in EXEC mode:

Command	Purpose
Router# show cs7 m2pa local-peer <i>port-num</i>	Displays ITP M2PA statistics.

The following is typical output of the **show cs7 m2pa local-peer** command:

```
Router# show cs7 m2pa local-peer 4097
CS7 M2PA Local Peer Info for local port = 4097
Local Port          = 4097
Local IP            = 199.1.1.1
                   ^^^^^^^^^^
SCTP Instance Handle = 1
Num Peers On Instance = 1
Instance Local Recv Window = 64000
Instance maxInitRetrans = 8
Instance maxInitTimeout = 1000 ms
Instance Unordered Priority = EQUAL
```

If the remote and local peers are not correct, they need to be corrected administratively.

If they are correct and the remote link is not shutdown, then verify IP connectivity.

If the peerstate is OutofService, then the link should be administratively activated.

```
lsn=mica          apc=4.4.4          state=UNAVAIL
  SLC  Interface          Service  PeerState      Inhib
*02   199.1.1.1 4098 4098          shutdown OutOfService      -----
```

Verify GTT

Refer to the [“Verifying Global Title Translations”](#) section on page 123 in the [“Global Title Translation”](#) chapter.

Verify IP connectivity

To verify IP connectivity ping the remote IP address, using the following command in EXEC mode:

Command	Purpose
Router# ping <i>ip-address</i>	Pings an IP address.

The following is typical output of the **ping** command:

```
Router# ping 199.1.1.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 199.1.1.4, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

The ping should succeed with 100% success rate and the min/avg/max round trip delays should not be excessive.

If the success rate is zero, as in the sample output that follows, there is no IP connectivity between the cs7 peers.

```
Router# ping 199.1.1.4

!Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 199.1.1.4, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Router#
```

For each peer, verify that the local IP peer address is associated with an active interface. Verify this using the **show ip interface brief** command. (In this case the local IP address is 199.1.1.1.)

```
Router# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	172.18.44.176	YES	NVRAM	up	up
Serial0/0	unassigned	YES	NVRAM	up	down
FastEthernet0/1	199.1.1.1	YES	NVRAM	up	up
				^^ ^^	
Serial0/1	unassigned	YES	NVRAM	down	down
Serial0/2	unassigned	YES	NVRAM	up	up
Serial0/3	unassigned	YES	NVRAM	up	up

```
Router#
```

If the interface status and protocol are not “up,” take the appropriate measures to activate the interface.

If the required interface status and protocol are up, verify that there is an IP route to the remote IP address. (In this case the remote IP address is 199.1.1.4)

```
Router# show ip route
Codes:C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    172.18.0.0/25 is subnetted, 1 subnets
C       172.18.44.128 is directly connected, FastEthernet0/0
C       199.1.1.0/24 is directly connected, FastEthernet0/1
    161.44.0.0/32 is subnetted, 1 subnets
S       161.44.2.30 [1/0] via 172.18.44.129
```

The above display shows that there is an IP route to the network 199.1.1.0 via the directly connected fastethernet0/0 interface.

Verify the State of M3UA and SUA Application Servers and Application Server Processes

The command includes keywords to filter and format the output.

- The filter options are **active**, **all** ASes (the default), **m3ua**, **name asname**, **operational**, and **sua**.
- The GTT subfilters are **include-gtt**, **exclude-gtt**, or **only-gtt**
- The format options are **brief** (the default format), **details**, **event-history**, and **statistics**.

The following is output from the **show cs7 as** command entered with no format or filter keywords. The command uses the default filter (**all**) and the default format (**brief**):

```
Router# show cs7 as
```

AS Name	State	Routing Context
asp1	down	1
asp2	down	2

AS Name	State	Routing Context	Routing Key Dpc	Si	Opc	Cic Ssn	Cic Min	Cic Max
as1	down	111	2.1.1					

The following is output from the **show cs7 as** command with the **binding-table** keyword. The Mate state is the status of the remote ASP. The options are: inactive/active.

```
ITP# show cs7 as binding-table
```

AS: mas2 (Total ASP Weight: 8)

ASP	State	Mate State	Weight	CIC
dasp2	down	active	1	0, 4
dasp3	active	inactive	0	
dasp4	down	inactive	0	
dasp5	active	inactive	3	1, 2, 3, 5, 6, 7d
asp1	down	inactive	4	
m3ua_s_176_0	active	inactive		

The following is output from the **show cs7 as** command entered with the **name asname** filter keyword and the **detail** format keyword:

```
Router#show cs7 as name owl5 detail
```

AS name: m3ua_s_176_0 State: active Type: M3UA
RoutContext: 6700 Class2 binding: enabled
Traf mode: loadshare bindings SLS
Mate AS state: unknown Rerouting queue depth: 0
Recovery tmout: 2000 ms Recovery queue depth: 0
QOS Class: 0 Burst recovery tmout: 4000 ms
PMP Status: N Inbound/outbound DCS group: n/a / n/a
Routing Key:
Dest PC: 2.1.1 Origin PC: n/a Origin PC mask: n/a
SI: n/a CIC min: n/a CIC max: n/a
SSN: n/a GTT: n/a

ASP Name	AS Name	State	Type	Rmt Port	Remote IP Addr	SCTP Assoc
asp2	owl5	down	SUA	9022	172.18.57.136	
asp1	owl5	down	SUA	9012	172.18.57.136	
cuba	owl5	down	SUA	14101	172.18.57.90	

Traffic-mode states are: override, loadshare bindings, loadshare roundrobin, broadcast, or undefined.

AS and Mate-AS states are: shutdown, down, down-rerouting, inactive, inactive-rerouting, active, or pending.

The following is output from the **show cs7 asp sua** command in the default brief format:

ASP Name	AS Name	State	Type	Rmt Port	Remote IP Addr	SCTP
-----	-----	-----	----	-----	-----	----
asp1	asp1	down	SUA	9012	172.18.57.136	
asp1	as1	down	SUA	9012	172.18.57.136	
asp2	asp2	down	SUA	9022	172.18.57.136	
asp2	as1	down	SUA	9022	172.18.57.136	
cuba	as1	down	SUA	14101	172.18.57.90	

ASP States are: shutdown, blocked, down, inactive, active, or active/congested.

If the ASP is down or shutdown, then the remote port and remote IP address display the configured values instead of the actual values.

The following example includes output from the **show cs7 asp** command in the **detail** format and filtering on the ASP name **asp1**. This ASP (type SUA) is down and the association state is closed. It is offloaded to the line card in slot 6.

AspVipId is an internal number used to identify the ASP.

Options for ASP state include: down/inactive/active/standby

The Mate state is the status of the remote ASP. The options are: inactive/active.

If the ASP is down or shut down, then the remote port and remote IP address display the configured values instead of the actual values.

```
ITP# show cs7 asp name asp1 detail
ASP name: asp1                               Type: SUA
Availability: enabled                         ASP id: n/a
SCTP association state: closed                 Association id: n/a
AS name: as1      ASP state: down             Mate state: inactive
Traffic mode: ldshr rr                       Active Time: Not Active
Configured remote port: 6000                  Actual remote port: 6000
Configured remote ip addresses: 10.10.20.2
Actual remote ip addresses:      n/a
Local port: 6000
Offload to FlexWAN:      Yes  Slot: 6  AspVipId: 101
ASP protocol class capability: class 0, class 1
ASP interworking with SS7 networks capability: ASP
Local receive window      64000                Cumulative sack timeout: 200 ms
Assoc retrans:            10                    Path retrans:         4
Max init retrans:         8                     Max init RTO:         1000 ms
Minimum RTO:              1000 ms               Maximum RTO:          1000 ms
Bundle status:            on                    Bundle timeout:        5 ms
Keep alive status:        true                  Keep alive timeout:    30000 ms

Unordered priority:       equal                  Cleanup timeout:       0 ms

Link status T1 timeout: 0 ms                    Remote congest T6 timeout: 0 ms
SCTP congestion level: 0                        SCON congestion level: 0
Transmit queue depth:    1000
Thresholds for congestion on transmit queue
  Level 1 onset:         500                    Level 1 abate:         300
  Level 2 onset:         700                    Level 2 abate:         500
  Level 3 onset:         900                    Level 3 abate:         700
  Level 4 onset:        1000                    Level 4 abate:         900
QOS Class:              4 (instance:4)          IP TOS:                0x60
Match Type:             Any                     Class:4 (instance:4)
```

Monitoring ITP

You can perform the tasks in the following sections to monitor and maintain the Cisco ITP:

- [Configuring ITP for Event Logging to an External Server, page 369](#)
- [Enabling Simple Network Management Protocol, page 370](#)
- [Monitoring the Cisco ITP, page 372](#)

Configuring ITP for Event Logging to an External Server

Routers send system messages to an internal logging process. The logging process controls the distribution of system messages to the various destinations, such as the console (default), terminal lines, router logging buffer, or external UNIX syslog server.

To set the severity level of the system messages to control the type of messages displayed at each of the destinations, use the following commands in global configuration mode:

Command	Purpose
Router(config)# logging console level	Limits the logging of messages displayed on the console terminal to a specified level.
Router(config)# logging monitor level	Limits the logging messages displayed on terminal lines other than the console line to messages at or above the specified level.
Router(config)# logging trap level	Limits the logging of error messages sent to syslog servers to only those messages at the specified level.

By default, system messages are delivered to the console. To enable messages on a terminal line, Use the following command in EXEC mode:

Command	Purpose
Router# terminal monitor	Display debug command output and system error messages for the current terminal and session.

To enable logging to a non-volatile ITP buffer and adjust the size of the buffer, use the following command in EXEC mode:

Command	Purpose
Router(config)# logging buffered size	Log messages to an internal buffer. The logging is circular, so newer messages overwrite older messages.

To enable logging messages to a UNIX syslog server host, use the following command in EXEC mode:

Command	Purpose
Router(config)# logging <i>host</i>	Log messages to a UNIX syslog server host. The host parameter is the name or Internet address of the server. By repeating the command, you can have messages sent to multiple syslog servers. the syslog format is compatible with 4.3 BSD UNIX.

By default, a syslog message contains the IP address of the interface it uses to leave the router. To specify that all syslog messages contain the same IP address, regardless of which interface they take to reach the syslog server, use the following command in global configuration mode:

Command	Purpose
Router(config)# logging source-interface	Specify the source IP address of syslog packets.

Enabling Simple Network Management Protocol

The Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a message format for communication between SNMP managers and agents. The SNMP system consists of the following three parts:

- An SNMP manager
- An SNMP agent
- A Management Information Base (MIB)

The SNMP manager can be part of a Network Management System (NMS) such as CiscoWorks. The agent and MIB reside on the router. To configure SNMP on the router, you define the relationship between the manager and the agent. For more information about SNMP, refer to “Configuring SNMP Support” in the Cisco IOS Release 12.1 *Configuration Fundamentals Configuration Guide*, Part 3, Cisco IOS System Management, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/fun_c/fcprt3/fcd301.htm

To enable SNMP traps for Cisco ITP to be sent, use the **snmp-server enable traps cs7** global configuration command.

Command	Purpose
Router(config)# snmp-server enable traps cs7 [gw-map-state] [gw-link-congestion] [gw-link-state] [gw-link-utilization] [gw-linkset-state] [gw-route-mgmt-state] [xua-state]	Enables SNMP traps for Cisco ITP.

When you enable CS7 traps, the default value for trap queue length (10 events) might cause traps to be lost. To avoid this situation set the trap queue length to 100 using the **snmp-server queue-length** global configuration command:

Commands	Purpose
Router(config)# snmp-server queue-length 100	Sets the default for trap queue length to 100.

You can control the rate of notifications for destination state changes and route state changes.

To specify the maximum number of destination state changes allowed per window, use the **cs7 snmp dest-max-window** global configuration command:

Command	Purpose
Router(config)# cs7 snmp dest-max-window	Sets the maximum number of destination state changes allowed per window. Valid range is 10 to 9000 changes. Default is 60. (Large values can impact the performance of the device and all notifications might not be sent to the management station.)

The **cs7 snmp dest-max-window** command corresponds to the `cgrtDestNotifMaxPerWindow` object in the Cisco-ITP-GRT-MIB.my MIB. Destination state changes are sent in the `ciscoGrtdDestStateChange` notification.

To specify the maximum number of route management state changes allowed per window, use the **cs7 snmp mgmt-max-window** global configuration command:

Command	Purpose
Router(config)# cs7 snmp mgmt-max-window	Sets the maximum number of route management state changes allowed per window. Valid range is 10 to 9000 changes. Default is 60. (Large values can impact the performance of the device and all notifications might not be sent to the management station.)

The **cs7 snmp mgmt-max-window** command corresponds to the `cgrtMgmtNotifMaxPerWindow` object in the Cisco-ITP-GRT-MIB.my MIB. Route management state changes are sent in the `ciscoGrtdMgmtStateChange` notification.

You can control the rate of notifications for rev1 destination state changes and rev1 route state changes.

To specify the maximum number of destination state changes allowed per window, use the **cs7 snmp dest-max-r1-window** global configuration command:

Command	Purpose
Router(config)# cs7 snmp dest-max-r1-window	Sets the maximum number of rev1 destination state changes allowed per window. Valid range is 10 to 9000 changes. Default is 60. (Large values can impact the performance of the device and all notifications might not be sent to the management station.)

The **cs7 snmp dest-max-r1-window** command corresponds to the `cgrtDestNotifMaxPerWindow` object in the Cisco-ITP-GRT-MIB.my MIB. Destination state changes are sent in the `ciscoGrtDestStateChange` notification.

To specify the maximum number of rev1 route management state changes allowed per window, use the **cs7 snmp mgmt-max-r1-window** global configuration command:

Command	Purpose
Router(config)# cs7 snmp mgmt-max-r1-window	Sets the maximum number of rev1 route management state changes allowed per window. Valid range is 10 to 9000 changes. Default is 60. (Large values can impact the performance of the device and all notifications might not be sent to the management station.)

The **cs7 snmp mgmt-max-r1-window** command corresponds to the `cgrtMgmtNotifMaxPerWindow` object in the Cisco-ITP-GRT-MIB.my MIB. Route management state changes are sent in the `ciscoGrtMgmtStateChange` notification.

Monitoring the Cisco ITP

This section includes information about the following tasks:

- [Monitoring CPU/Memory, page 372](#)
- [Monitoring Linksets and Links, page 373](#)
- [Monitoring MTP2 Links/Interfaces, page 375](#)
- [Monitoring M2PA Links/Interfaces, page 380](#)
- [Monitoring GTT Measurements, page 383](#)
- [Monitoring M3UA or SUA, page 384](#)
- [Monitoring AS, ASP, Mated-SG, page 385](#)
- [Monitoring Routes, page 391](#)
- [Monitoring Gateway Screening Violations, page 392](#)
- [Monitoring System Messages, page 392](#)
- [Monitoring Accounting, page 393](#)

Monitoring CPU/Memory

Why is this task important?

A healthy SS7oIP router needs to be running at less than 50% CPU during non fail-over conditions and must have 50% available memory to handle route table changes due to network conditions. If an SS7oIP router has a CPU and/or memory shortage, network availability is at risk. CPU and memory should be monitored via system error messages or SNMP traps alerts

Under what circumstances should this task be performed?

System health monitoring is an ongoing process and should be automated. CiscoWorks network management application can be used to automate this task.

What incidents or system messages should prompt the user to monitor the CPU/memory?

When Cisco ITP attempts to allocate memory for an event for which no memory is available, the following IOS message is displayed:

```
%SYS-2-MALLOCFAIL:Memory allocation of [dec] bytes failed from [hex], pool
[chars], alignment [dec]
```

Explanation The requested memory allocation is not available from the specified memory pool. The current system configuration, network environment, or possibly a software error might have exhausted or fragmented the router memory.

Action Copy the error message exactly as it appears on the console or in the system log, call your Cisco technical support representative, and provide the representative with the gathered information.

Should this task be part of a regular maintenance process that the user should do at regular intervals? If so, how frequently?

Ongoing.

What commands does the user issue?

The **show proc cpu** command will display output such as the following:

```
CPU utilization for five seconds:0%/0%; one minute:0%; five minutes:0%
PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
27 0 1 0 0.00% 0.00% 0.00% 0 MTP3 Input
28 30238 70601 428 0.00% 0.01% 0.00% 0 MTP3 Mgmt
53 56 353673 0 0.00% 0.00% 0.00% 0 CS7 MTP2 timer
```

The **show proc mem** command will display output such as the following:

```
Total:26494208, Used:4829456, Free:21664752
PID TTY Allocated Freed Holding Getbufs Retbufs Process
27 0 192 0 13036 0 0 MTP3 Input
28 0 267888 276 274456 0 0 MTP3 Mgmt
53 0 20948 340 27452 0 0 CS7 MTP2 timer
```

The **show mem** command will display output such as the following:

	Head	Total (b)	Used(b)	Free(b)	Lowest (b)	Largest (b)
Processor	80DBBB00	26494208	4829308	21664900	21615220	21640172
I/O	2700000	26214400	2227876	23986524	23979088	23979036

Refer to the “Command Reference” section of this document for detailed descriptions of the show commands.

Monitoring Linksets and Links

Why is this task important?

Links and linksets can change states from available to unavailable while the system is running. It is important to monitor when a linkset has become unavailable since it can indicate total or partial loss of a route to a destination node. When a link becomes unavailable, it can have a negative impact on the throughput, since there will be fewer links to carry the traffic.

Under what circumstances should this task be performed?

Link and linkset availability should be monitored at all times when there is traffic flowing over it.

What incidents or system messages should prompt the user to monitor Linksets and Links?

The user should monitor the links and linkset whenever a route or destination becomes unavailable.

Should this task be part of a regular maintenance process that the user should do at regular intervals? If so, how frequently?

Whenever a link or linkset becomes unavailable, error messages are displayed on the console and an SNMP trap is sent to the network management node.

What commands does the user issue?

To monitor all linksets, issue the **show cs7 linkset brief** command, which displays output such as the following:

```
lsn=to_2651_1      apc=0.3.3      state=UNAVAIL
lsn=to_helium      apc=0.2.2      state=avail
lsn=to_mgts_15     apc=1.1.1      state=UNAVAIL
```

The following explanations are based on the preceding output of the **show cs7 linkset brief** command.

- Linkset **to_helium** is available and for traffic. A linkset is in available state when it has at least one available link in it. The detailed display below indicates that the linkset has several links that are available.
- Linkset **to_2651_1** is unavailable because it does not have any available links. Link 0 has been shutdown via configuration.
- In linkset **to_helium**, link 5 has been locally inhibited and as such is unavailable to carry traffic.
- Link 6 has been remotely inhibited and is also unavailable to carry traffic. (If a link has been locally inhibited via the **cs7 inhibit** command, the Inhibit column will display **loc** to indicate that the link was locally inhibited. If a link is inhibited from the adjacent node, the show output will display **rem** to indicate that it was remotely inhibited.
- Linkset **to_mgts_15** is also not available to carry traffic because it does not have any available links.
- Link 0 has failed.

Linkset States

- **UNAVAIL** Indicates the linkset does not have any “available” links and cannot transport traffic.
- **shutdown** Indicates the linkset has been shutdown in the configuration.
- **avail** Indicates the linkset has at least one available link and can carry traffic.

Link States

- **UNAVAIL** Indicates the link is not available to carry traffic. This can occur if the link is remotely or locally inhibited by a user. It can also be unavailable if MTP2/M2PA has not been able to successfully activate the link connection or the link test messages sent by MTP3 are not being acknowledged.
- **shutdown** Indicates the link has been shutdown in the configuration. A link is **shutdown** when it is shutdown at the MTP3 layer.
- **avail** Indicates the link is active and able to transport traffic.
- **FAILED** A link is **FAILED** when the link is not shutdown but is unavailable at layer2 for some reason. It is **FAILED** when the link is unavailable because the link has been inhibited or it is blocked.

- **sys-shutdown** Indicates the link has been shutdown by the system. A link may be in this state when:
 - MTP3 offload is configured and the system is performing error recovery on the FlexWAN
 - MTP3 offload has been permanently disabled on a FlexWAN by the system due to excessive errors. When MTP3 offload has been permanently disabled on a FlexWAN (by the system) all links on that FlexWAN will be in the sys-shutdown state.

To monitor all linksets and all links in the linksets, issue the **show cs7 linkset** command. Refer to the “Command Reference” section of this document for descriptions of the show commands.

```
Router# show cs7 linkset
lsn=to_2651_1      apc=0.3.3      state=UNAVAIL
  SLC  Interface      Service  PeerState      Inhib
*00   10.10.10.5 5000 5000      shutdown OutOfService    -----

lsn=to_helium      apc=0.2.2      state=avail
  SLC  Interface      Service  PeerState      Inhib
00    Serial4/0/0      avail    -----        -----
01    Serial4/0/1      avail    -----        -----
02    Serial4/0/2      avail    -----        -----
03    Serial4/0/3      avail    -----        -----
04    Serial4/0/4      avail    -----        -----
*05    Serial4/0/5      UNAVAIL  -----        loc
*06    Serial4/0/6      UNAVAIL  -----        rem
07    Serial4/0/7      avail    -----        -----
08    Serial4/1/0:0     avail    -----        -----
09    Serial4/1/1:0     avail    -----        -----
10    Serial4/1/2:0     avail    -----        -----
11    Serial4/1/3:0     avail    -----        -----
12    Serial4/1/4:0     avail    -----        -----
13    Serial4/1/5:0     avail    -----        -----
14    Serial4/1/6:0     avail    -----        -----
15    Serial4/1/7:0     avail    -----        -----

lsn=to_mgts_15     apc=1.1.1      state=UNAVAIL
  SLC  Interface      Service  PeerState      Inhib
*00    Serial1/1/0      FAILED  -----        -----.
```

Monitoring MTP2 Links/Interfaces

Why is this task important?

Monitoring interfaces is useful for determining the status of MTP2/SCTP links, for providing statistical information about the performance of the interface.

Under what circumstances should this task be performed?

If an MTP2 link goes down.

If performance on an MTP2 link is degraded.

What incidents or system messages should prompt the user to monitor interfaces?

Should this task be part of a regular maintenance process that the user should do at regular intervals? If so, how frequently?

Regular monitoring is not necessary for link failure problems because system messages will indicate link failure conditions. Regular monitoring to find performance problems may be necessary.

What commands does the user issue?

```

show interface serial
show cs7 mtp2 state serial
show cs7 mtp2 congestion serial
show cs7 mtp2 statistics serial

```

The output of the **show interface serial** command can reveal possible Link Down problems. The fields to examine are indicated with arrows in the sample output below:

```

Router# show int ser 5/0/0:0
→ Serial5/0/0:0 is up, line protocol is up
    Hardware is Multichannel T1
    MTU 290 bytes, BW 64 Kbit, DLY 20000 usec,
      reliability 255/255, txload 1/255, rxload 1/255
→ Encapsulation SS7 MTP2, crc 16, CRC 16, Data non-inverted
    Keepalive set (10 sec)
    Last input 00:00:45, output 00:00:45, output hang never
    Last clearing of "show interface" counters 00:05:39
    Queueing strategy:fifo
    Output queue 0/40, 0 drops; input queue 0/75, 0 drops
    30 second input rate 0 bits/sec, 0 packets/sec
    30 second output rate 0 bits/sec, 0 packets/sec
    139 packets input, 1270 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    119 packets output, 856 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
    1 carrier transitions no alarm present
    Timeslot(s) Used:1, subrate:64Kb/s, transmit delay is 0 flags
    Transmit queue length 43

```

The field “line protocol” should display “line protocol is up” rather than down.

The field “Encapsulation” should display “SS7 MTP2” rather than (for example) HDLC.

The output of the **show cs7 mtp2 state serial** command indicates the status of the MTP2 state machine. The fields to examine are indicated with arrows in the sample output below:

```

Router# show cs7 mtp2 state ser 5/0/0:0
CS7 MTP2 states for interface Serial5/0/0:0
Protocol version for interface Serial5/0/0:0 is ITU-T Q.703 (1996) (White Book)

→ Link State Control (LSC) = In Service
  Initial Alignment Control (IAC) = Idle
→ Transmission Control (TXC) = In Service
→ Reception Control (RC) = In Service
  Signal Unit Error Rate Monitor (SUERM) = Monitoring
  Alignment Unit Error Rate Monitor (AERM) = Idle
  Congestion (CONG) = Idle

→ Layer3 link status = Started
  Layer3 congestion status = Abate

```

The field “Link State Control (LSC)” should display “In Service.”

The field “Transmission Control (TXC)” should display “In Service.”

The field “Reception Control (RC)” should display “In Service.”

The field “Layer3 link status” should display “Started.”

The output of the **show interface serial** command can reveal possible performance problems. The fields to examine are indicated with arrows in the sample output below:

```
Router# show int ser 5/0/0:0
→ Serial5/0/0:0 is up, line protocol is up
  Hardware is Multichannel T1
  MTU 290 bytes, BW 64 Kbit, DLY 20000 usec,
→   reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation SS7 MTP2, crc 16, CRC 16, Data non-inverted
  Keepalive set (10 sec)
  Last input 00:00:45, output 00:00:45, output hang never
  Last clearing of "show interface" counters 00:05:39
  Queueing strategy:fifo
→   Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
→   139 packets input, 1270 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
→   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  119 packets output, 856 bytes, 0 underruns
  0 output errors, 0 collisions, 0 interface resets
  0 output buffer failures, 0 output buffers swapped out
  1 carrier transitions no alarm present
  Timeslot(s) Used:1, subrate:64Kb/s, transmit delay is 0 flags
  Transmit queue length 43
```

The field “line protocol” should display “line protocol is up.”

The field “reliability” displays a fraction in the range 255/255 to x/255 which indicates the percentage of reliability. The fraction should represent 100%.

The field “txload” displays a fraction in the range 1/255 to x/255 which indicates the percentage of transmit load on the link.

- Under 40% txload is optimal.
- 40%-80% txload indicates a heavily loaded link.
- Over 80%txload indicates a heavily congested link.

The field “rxload” displays a fraction in the range 1/255 to x/255 which indicates the percentage of receive load on the link.

- Under 40% rxload is optimal.
- 40%-80% rxload indicates a heavily loaded link.
- Over 80% rxload indicates a heavily congested link.

In the field “Output queue 0/40, 0 drops; input queue 0/75, 0 drops”:

- Output drops indicate local txCongestion or rxCongestion at remote.
- Input drops indicate local rxCongestion or txCongestion at remote.

The field “<number> no buffer” indicates packet drops because of buffer shortage. The number should be 0.

The field “<number> input errors, <number> CRC, <number> frame, <number> overrun, <number> ignored, <number> abort” indicates problems with interface receive. The numbers should be 0.

In the field “<number> output errors, <number> collisions, <number> interface resets” all numbers should be 0.

The field “<number> output buffer failures, <number> output buffers swapped out” indicates problems with interface transmit.

The output of the **show cs7 mtp2 congestion serial** command indicates congestion levels. The fields to examine are indicated with arrows in the sample output below:

```
Router# show cs7 mtp2 congestion ser 5/0/0:0
CS7 MTP2 congestion status for interface Serial5/0/0:0
Protocol version for interface Serial5/0/0:0 is ITU-T Q.703 (1996) (White Book)

→ Layer3 congestion status      = Abate

→ CongestionRxInd               = Abate
→ CongestionTxInd               = Abate (Level0)

CongestionTxOnset Level1       = 250 ( 50% of xmitQ maxDepth)
CongestionTxOnset Level2       = 350 ( 70% of xmitQ maxDepth)
CongestionTxOnset Level3       = 450 ( 90% of xmitQ maxDepth)
CongestionTxOnset Level4       = 500 (100% of xmitQ maxDepth)

→ XmitQ depth (max-used)        = 15
→ XmitQ depth (max-allowed)     = 500
```

The field “Layer3 congestion status” should display “Abate” (MTP3 not congested) rather than “Onset” (MTP3 congested).

The fields “CongestionRxInd” and “CongestionTxInd” indicate current congestion levels.

The field “XmitQ depth (max-used)” indicates the maximum number of packets ever waiting on the queue and indicate how congested router might have been.

The output of the **show cs7 mtp2 statistics serial** command indicate congestion levels. The fields to examine are indicated with arrows in the sample output below:

```
Router# show cs7 mtp2 statistics ser 5/0/0:0
CS7 MTP2 Statistics for interface Serial5/0/0:0
Protocol version for interface Serial5/0/0:0 is ITU-T Q.703 (1996) (White Book)

OMtimeINSV (secs)              = 756
OMtimeNotINSV (secs)           = 49

OMIACAlignAttemptCount         = 10
OMIACAlignFailCount            = 4
OMIACAlignCompleteCount        = 2

OMMSU_L3_XMIT_Count            = 137
OMMSU_XMIT_Count                = 137
OMMSUBytesTransmitted           = 1429
→ OMMSU_RE_XMIT_Count           = 0
→ OMMSUBytesRetransmitted       = 0

OMMSU_RCV_Count                = 157
OMMSUBytesReceived              = 1625

OMFISU_XMIT_Count              = 159
OMFISU_RCV_Count               = 307

OMLSSU_XMIT_Count              = 24
OMLSSU_XMIT_SINCount           = 0
OMLSSU_XMIT_SIECount           = 2
OMLSSU_XMIT_SIOCount           = 10
OMLSSU_XMIT_SIOSCount          = 12
OMLSSU_XMIT_SIPOCount          = 0
OMLSSU_XMIT_SIBCount           = 0

OMLSSU_RCV_Count               = 8
```



```

OMLSSU_RCV_SINCount      = 0
OMLSSU_RCV_SIECount      = 4
OMLSSU_RCV_SIOCount      = 4
OMLSSU_RCV_SIOSCount     = 0
OMLSSU_RCV_SIPOCount     = 0
OMLSSU_RCV_SIBCount      = 0

OMT1_TMO_Count           = 0
OMT2_TMO_Count           = 4
OMT3_TMO_Count           = 0
OMT4_TMO_Count           = 2
OMT5_TMO_Count           = 0
OMT6_TMO_Count           = 0
OMT7_TMO_Count           = 0
OMAERMCount              = 2
OMAERMFailCount          = 0
OMSUERMCount              = 2
OMSUERMFailCount         = 0

→ OMCongestionRxCount    = 0
→ OMCongestionTxCount    = 0
→ OMRemote_Congestion_Cnt = 0

OMxmitQ_maxcount         = 15

OMNACK_XMIT_Count        = 0
OMNACK_RCV_Count         = 0

→ OMunreasonableFSN_rcvd = 0      (error)
→ OMunreasonableBSN_rcvd = 0      (error)
→ OMabnormalBSN_rcvd     = 0      (error)
→ OMabnormalFIB_rcvd     = 0      (error)

OMFISU_notAccepted       = 4      (packets dropped)
OMMSU_notAccepted        = 0      (packets dropped)
OMFISU_congestionDrops   = 0      (packets dropped)
→ OMMSU_congestionDrops  = 0      (packets dropped)
OMMSU_too_long           = 0      (packets dropped)
→ OMMSU_unexpectedFSN    = 0      (packets dropped)
→ OMMSU_discarded        = 0      (packets dropped)

```

The fields “OMMSU_RE_XMIT_Count” and “OMMSUBytesRetransmitted” indicate retransmission on the link. Retransmission is an indication of probable congestion.

The fields “OMCongestionRxCount”, “OMCongestionTxCount”, “OMRemote_Congestion_C indicate congestion counts on the local or remote device.

The fields “OMunreasonableFSN_rcvd”, “OMunreasonableBSN_rcvd”, “OMabnormalBSN_rcvd” and “OMabnormalFIB_rcvd” indicate protocol errors.

The field “OMMSU_congestionDrops” indicates the number of MSU packets dropped due to rxCongestion.

The field “OMMSU_unexpectedFSN” indicates packets dropped due to unexpected FSN received.

The field “OMMSU_discarded” indicates total MSU packets dropped, probably due to congestion.

Monitoring M2PA Links/Interfaces



Note

M2PA/SCTP links run over any interface that supports IP (serial, ethernet, fast ethernet, token ring, etc. The example used in this section is for fast ethernet.

Why is this task important?

Monitoring interfaces is useful for determining the status of M2PA/SCTP links and for providing statistical information about the performance of the interface.

Under what circumstances should this task be performed?

If the M2PA/SCTP links fail or if the M2PA/SCTP link performance is degraded.

What incidents or system messages should prompt the user to issue the monitor M2PA Links/Interfaces?

Should this task be part of a regular monitoring process that the user should do at regular intervals? If so, how frequently?

Regular monitoring is not necessary for link failure problems because system messages will indicate link failure conditions. Regular monitoring to identify performance problems may be necessary.

What commands does the user issue?

```
show interface interface-type
show cs7 m2pa state ls-name
```

The following output of the show interface ethernet command reveals possible link down problems:

```
Router# show int faste0/1
FastEthernet0/1 is up, line protocol is up
  Hardware is AmdFE, address is 0003.e348.5f41 (bia 0003.e348.5f41)
  Internet address is 50.50.50.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type:ARPA, ARP Timeout 04:00:00
  Last input 00:00:16, output 00:00:03, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy:fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
    75799 packets input, 11049547 bytes
    Received 5616 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog
    0 input packets with dribble condition detected
    155409 packets output, 15498764 bytes, 0 underruns(0/0/0)
    0 output errors, 0 collisions, 1 interface resets
    0 babbles, 0 late collision, 614 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
```

The field “line protocol” should display “line protocol is up.”

The field “Internet address” should display a valid IP address.

```
CS7 M2PA states for Peer (50.50.50.2 :9000)
M2PA Peer State           = InService
SCTP Peer State           =SCTP_ESTABLISHED
```

```
T1 aligned/ready          = 5000 ms
T6 remote cong            = 3000 ms
```

```
Local Processor Outage    = FALSE
Remote Processor Outage   = FALSE
InService LSSU Recv'd    = TRUE
Transport Handle          = 0
```

The field “M2PA Peer State” should display “InService.”

The field “SCTP Peer State” should display “SCTP_ESTABLISHED.”

The following output of the **show interface ethernet** command reveals possible performance problems:

```
Router# show int faste0/1
FastEthernet0/1 is up, line protocol is up
  Hardware is AmdFE, address is 0003.e348.5f41 (bia 0003.e348.5f41)
  Internet address is 50.50.50.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type:ARPA, ARP Timeout 04:00:00
  Last input 00:00:10, output 00:00:09, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy:fifo
  Output queue 0/40, 20 drops; input queue 0/75, 25 drops
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
  75895 packets input, 11064304 bytes
    Received 5641 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog
    0 input packets with dribble condition detected
  155709 packets output, 15529225 bytes, 0 underruns(0/0/0)
    0 output errors, 0 collisions, 1 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
```

The field “line protocol” should display “line protocol is up.”

The field “Internet address” should display a valid IP address.

The field “reliability” displays a fraction in the range 255/255 to x/255 which indicates the percentage of reliability. The fraction should represent 100%.

The field “txload” displays a fraction in the range 1/255 to x/255 which indicates the percentage of transmit load on the link.

- Under 40% txload is optimal.
- 40%-80% txload indicates a heavily loaded link.
- Over 80%txload indicates a heavily congested link.

The field “rxload” displays a fraction in the range 1/255 to x/255 which indicates the percentage of receive load on the link.

- Under 40% rxload is optimal.
- 40%-80% rxload indicates a heavily loaded link.
- Over 80% rxload indicates a heavily congested link.

In the field “Output queue 0/40, 0 drops; input queue 0/75, 0 drops”:

- Output drops indicate local txCongestion or rxCongestion at remote.
- Input drops indicate local rxCongestion or txCongestion at remote.

The field “<number> no buffer” indicates packet drops because of buffer shortage. The number should be 0.

The field “<number> input errors, <number> CRC, <number> frame, <number> overrun, <number> ignored, <number> abort” indicates problems with interface receive. The numbers should be 0.

In the field “<number> output errors, <number> collisions, <number> interface resets” all numbers should be 0.

The field “number output buffer failures, number output buffers swapped out” indicates problems with interface transmit.

```
Router# show cs7 m2pa statistics to_duck
CS7 M2PA Peer Statistics for (50.50.50.2 :9000)
M2PA Peer State           = InService
SCTP Peer State           = SCTP_ESTABLISHED
MSU_XMIT_Count             = 98658
MSU_RCV_Count              = 98913
MSU_XMIT_Fail_Count        = 0
MSU_XMIT_Drop_Count        = 0
LSSU_XMIT_Count            = 2
LSSU_XMIT_Fail_Count       = 0
LSSU_XMIT_SIISCount        = 2
LSSU_XMIT_SIPOCount        = 0
LSSU_XMIT_SIPOECount       = 0
LSSU_XMIT_SIBCount         = 0
LSSU_XMIT_SIBECCount       = 0
LSSU_RCV_Count             = 2
LSSU_RCV_SIISCount         = 2
LSSU_RCV_SIPOCount         = 0
LSSU_RCV_SIPOECount        = 0
LSSU_RCV_SIBCount          = 0
LSSU_RCV_SIBECCount        = 0
LSSU_RCV_InvalidCount      = 0
BytesTransmitted            = 3337163
BytesReceived               = 3340840
Remote_PO_Count            = 0
Remote_Congestion_Count    = 0
CongestionCount             = 0
Level 1 CongestionCount     = 1
Level 2 CongestionCount     = 0
Level 3 CongestionCount     = 0
Level 4 CongestionCount     = 0
T1_TMO_Count               = 0
T6_TMO_Count               = 0
```

The field “Level x CongestionCount” displays the number of times congestion level x has occurred.

```
Router# show ip sctp stat

** SCTP Overall Statistics **
Total Chunks Sent:         50141
Total Chunks Rcvd:         47738
Received Ordered Data Chunks: 10877
```

```

Received UnOrdered Data Chunks:0
Total Data Chunks Sent:      10877
Total Data Chunks Rcvd:      10877
Total Data Bytes Sent:       184924
Total Data Bytes Rcvd:       184924
Total Data Chunks Discarded:  0
Total Data Chunks Retrans:    0

Total SCTP Datagrams Sent:    41099
Total SCTP Datagrams Rcvd:    41099
Total ULP Datagrams Sent:     10877
Total ULP Datagrams Ready:    10877
Total ULP Datagrams Rcvd:     10877

```

The field “Total Data Chunks Retrans” displays the number of retransmissions that have occurred.

The field “Total Chunks Discarded” displays the number of packets that have been discarded due to duplicates.

Monitoring GTT Measurements

You can display CS7 GTT measurements based on system, map, counters, selector, application-group, or line card.

To display a report for each PC/SSN combination, including the number of times it was used by a successful translation, use the following command in privileged EXEC mode:

Command	Purpose
Router# show cs7 gtt measurements map	Displays a report for each PC/SSN combination.

To display measurements kept on a Selector basis, use the following command in privileged EXEC mode:

Command	Purpose
Router# show cs7 gtt measurements selector <i>[selector]</i>	Displays a report for each selector.

To display measurements for the system, use the following command in privileged EXEC mode:

Command	Purpose
Router# show cs7 gtt measurements systot	Displays a system report.

To display measurements for the application group, use the following command in privileged EXEC mode:

Command	Purpose
Router# show cs7 gtt measurements app-group <i>name</i>	Displays GTT measurements kept on a application group basis.

To display measurements for the line card, use the following command in privileged EXEC mode:

Command	Purpose
Router# show cs7 gtt measurements line-card [<i>line-card-num</i>]	Displays GTT measurements kept on a line card basis. If line-card-num is not specified, all line-card measurements for all line cards are displayed.

To reset all GTT measurements to 0, use the following command in privileged EXEC mode:

Command	Purpose
Router# clear cs7 gtt-meas	Resets all GTT measurements to 0.

Monitoring M3UA or SUA

This section includes information about the following monitoring tasks:

- [Monitoring M3UA, page 384](#)
- [Monitoring SUA, page 384](#)
- [Monitoring Point Code Status, page 385](#)
- [Monitoring AS, page 385](#)
- [Monitoring ASP, page 387](#)
- [Monitoring and Mated SG Pairs, page 389](#)

Monitoring M3UA

The following is sample output from the **show cs7 m3ua** command.

The “State” field should be “Active” and the number of active SUA and M3UA peers should math the number of ASPs available.

```
Router# show cs7 m3ua
Sigtran M3UA RFC number: 3332

M3UA Local port: 2905 State: active          SCTP instance handle: 5
Local ip address:                          172.18.48.39
Number of active M3UA peers:                0
Max number of inbound streams allowed:      17
Local receive window:                       64000
Max init retransmissions:                   8
Max init timeout:                           1000 ms
Unordered priority:                         equal
SCTP defaults for new associations
Transmit queue depth: 1000                  Cumulative sack timeout: 200 ms
Assoc retransmissions: 10                   Path retransmissions: 4
Minimum RTO: 1000 ms                       Maximum RTO: 1000 ms
Bundle status: on                           Bundle timeout: 5 ms
Keep alive status: true                     Keep alive timeout: 30000 ms
```

Monitoring SUA

The following is sample output from the **show cs7 sua** command:

```
Router# show cs7 sua
```

```

Sigtran SUA draft version: 14

SUA Local port: 14001 State: active          SCTP instance handle: 5
Local ip address:                          172.18.48.39
Number of active SUA peers:                 0
Max number of inbound streams allowed:      17
Local receive window:                       64000
Max init retransmissions:                   8
Max init timeout:                           1000 ms
Unordered priority:                         equal
SCTP defaults for new associations
  Transmit queue depth: 1000                Cumulative sack timeout: 200 ms
  Assoc retransmissions: 10                 Path retransmissions: 4
  Minimum RTO: 1000 ms                     Maximum RTO: 1000 ms
  Bundle status: on                         Bundle timeout: 5 ms
  Keep alive status: true                   Keep alive timeout: 30000 ms

```

Monitoring Point Code Status

The **show cs7 point-codes** command displays the type and status of all point codes configured as a destination point code in an M3UA or SUA routing key (default).

The **event-history** keyword displays the point code status history (default). The **ssn** keyword displays the status of all point codes configured as a DPC in an SUA routing key that also contains a valid SSN.

The following is sample output from the **show cs7 point-code** command

Router#**show cs7 point-codes**

CS7 Point Code	Type	Status
1.1.2	local	active
2.1.1	AS	SUA inactive

Router#**show cs7 point-code ssn**

SUA Point Code	SSN	Status
5.6.7	3	SUA inactive

Monitoring AS, ASP, Mated-SG

Monitoring AS

The **show cs7 as** command includes keywords to filter and format the output.

- The filter options are **active**, **all** ASes (the default), **m3ua**, **name asname**, **operational**, and **sua**.
- The GTT subfilters are **include-gtt**, **exclude-gtt**, or **only-gtt**
- The format options are **brief** (the default format), **details**, **event-history**, and **statistics**.

The following is output from the **show cs7 as** command entered with no format or filter keywords. The command uses the default filter (**all**) and the default format (**brief**):

Router# **show cs7 as**

AS Name	State	Routing Context
asp1	down	1
asp2	down	2

AS Name	State	Routing Context	Routing Key Dpc	Si	Opc	Cic Ssn	Cic Min	Cic Max
as1	down	111	2.1.1					

The following is output from the **show cs7 as** command entered with the **name asname** filter keyword and the **detail** format keyword:

```
Router#show cs7 as name owl5 detail
AS name: m3ua_s_176_0      State: active      Type: M3UA
RoutContxt: 6700          Class2 binding: enabled
Traf mode: loadshare bindings SLS
Mate AS state: unknown   Rerouting queue depth: 0
Recovery tmout: 2000 ms  Recovery queue depth: 0
QOS Class: 0              Burst recovery tmout: 4000 ms
PMP Status: N             Inbound/outbound DCS group: n/a / n/a
Routing Key:
  Dest PC: 2.1.1          Origin PC: n/a          Origin PC mask: n/a
  SI: n/a                 CIC min: n/a           CIC max: n/a
  SSN: n/a                GTT: n/a
ASP Name    AS Name      State    Type    Rmt Port Remote IP Addr  SCTP Assoc
asp2        owl5         down     SUA     9022  172.18.57.136
asp1        owl5         down     SUA     9012  172.18.57.136
cuba        owl5         down     SUA     14101 172.18.57.90
```

Traffic-mode states are: override, loadshare bindings, loadshare roundrobin, broadcast, or undefined.

AS and Mate-AS states are: shutdown, down, down-rerouting, inactive, inactive-rerouting, active, or pending.

Monitoring ASP

The following is output from the **show cs7 asp sua** command in the default brief format:

ASP Name	AS Name	State	Type	Rmt Port	Remote IP Addr	SCTP
-----	-----	-----	-----	-----	-----	-----
asp1	asp1	down	SUA	9012	172.18.57.136	
asp1	as1	down	SUA	9012	172.18.57.136	
asp2	asp2	down	SUA	9022	172.18.57.136	
asp2	as1	down	SUA	9022	172.18.57.136	
cuba	as1	down	SUA	14101	172.18.57.90	

ASP States are: shutdown, blocked, down, inactive, active, or active/congested.

If the ASP is down or shutdown, then the remote port and remote IP address display the configured values instead of the actual values.

The following is output from the **show cs7 asp** command in the detail format:

```
Router#show cs7 asp detail
ASP name: asp1                               Type: SUA
Availability: enabled                        ASP id: n/a
SCTP association state: closed                Association id: n/a
AS name: asp1
  ASP state: down      Traf mode: n/a      Active Time: Not Active
AS name: as1
  ASP state: down      Traf mode: n/a      Active Time: Not Active
Configured remote port: 9012                Actual remote port: n/a
Configured remote ip addresses: 172.18.57.136
Actual remote ip addresses:      n/a
Local port: 14001
ASP protocol class capability: class 0, class 1
ASP interworking with SS7 networks capability: ASP
Local receive window: 64000                Cumulative sack timeout: 200 ms
Assoc retrans: 10                          Path retrans: 4
Max init retrans: 8                        Max init RTO: 1000 ms
Minimum RTO: 1000 ms                      Maximum RTO: 1000 ms
Bundle status: on                          Bundle timeout: 5 ms
Keep alive status: true                    Keep alive timeout: 30000 ms
Unordered priority: equal                  Transmit queue depth: 20000
Unordered priority: equal                  Cleanup timeout: 0 ms
Link status T1 timeout: 0 ms               Remote congest T6 timeout: 0 ms
SCTP congestion level: 0                   SCON congestion level: 0
Transmit queue depth: 1000
Thresholds for congestion on transmit queue
  Level 1 onset: 500                      Level 1 abate: 300
  Level 2 onset: 700                      Level 2 abate: 500
  Level 3 onset: 900                      Level 3 abate: 700
  Level 4 onset: 1000                     Level 4 abate: 900
QOS Class: 0                             IP TOS: 0x0
Match Type: None
```

The following is sample output from the **show cs7 asp** command in the **statistics** format:

```
Router# show cs7 asp statistics
ASP name: asp1                               Type: SUA
Active Time: Not Active
Data Packets/MSU Stats
Inbound Packets Rcvd: 0                     Inbound Octets Rcvd: 0
Inbound Packets Sent: 0                    Inbound Octets Sent: 0
Outbound Packets Rcvd: 0                   Outbound Octets Rcvd: 0
Outbound Packets Sent: 0                   Outbound Octets Sent: 0
```

Inbound CLDTs Rcvd:	0	Inbound CLDTs Sent:	0
Outbound CLDTs Rcvd:	0	Outbound CLDTs Sent:	0
Inbound CLDRs Rcvd:	0	Inbound CLDRs Sent:	0
Outbound CLDRs Rcvd:	0	Outbound CLDRs Sent:	0

The following is sample output from the **show cs7 asp** command with the **statistics** and **detail** keywords:

```
Router# show cs7 asp statistics detail
ASP name: aspl                                     Type: SUA
  Active Time: Not Active
    Data Packets/MSU Stats
      Inbound Packets Rcvd: 0                      Inbound Octets Rcvd: 0
      Inbound Packets Sent: 0                      Inbound Octets Sent: 0
      Outbound Packets Rcvd: 0                     Outbound Octets Rcvd: 0
      Outbound Packets Sent: 0                     Outbound Octets Sent: 0
      Inbound CLDTs Rcvd: 0                        Inbound CLDTs Sent: 0
      Outbound CLDTs Rcvd: 0                       Outbound CLDTs Sent: 0
      Inbound CLDRs Rcvd: 0                        Inbound CLDRs Sent: 0
      Outbound CLDRs Rcvd: 0                       Outbound CLDRs Sent: 0
    ASP State Maintenance (ASPSM) Stats
      ASPUP Rcvd: 0                                ASPUP ACK Sent: 0
      ASPDN Rcvd: 0                                ASPDN ACK Sent: 0
      BEAT Rcvd: 0                                 BEAT ACK Sent: 0
    ASP Traffic Maintenance (ASPTM) Stats
      ASPAC Rcvd: 0                                ASPAC ACK Sent: 0
      SPIA Rcvd: 0                                 SPIA ACK Sent: 0
      ASPAC NRC Rcvd: 0                            SPIA NRC Rcvd: 0
      ASPAC Over-ride: 0
      ASPAC Load-share: 0
      ASPAC Broadcast: 0
      Active Routing Keys: 0
    MTP3 Stats
      MSUs Sent To MTP3: 0                          MSUs Dropped (Cong): 0
      MSUs Buffered: 0                              MSUs Dropped (Err): 0
    Buffer Allocation Stats
      Buffer Alloc Failures: 0                       Buffer Growth Failures: 0
      MSUs Sent To MTP3: 0                          MSUs Dropped By MTP3: 0
    XUA Error Messages Sent Stats
      ERR Invalid Version: 0                        ERR Unsupported Class: 0
      ERR Unsupported Type: 0                       ERR Traffic Mode: 0
      ERR Unexpected Msg: 0                         ERR Protocol Error: 0
      ERR Invalid Stream ID: 0                      ERR Refused, Mgmt Block: 0
      ERR ASP ID Required: 0                        ERR Invalid ASP ID: 0
      ERR Invalid Parm Value: 0                     ERR Parm Field Error: 0
      ERR Unexpected Parm: 0                        ERR Dest Status Unknown: 0
      ERR Inv Network App: 0                        ERR Missing Parm: 0
      ERR RK Change Refused: 0                      ERR Inv Routing Context: 0
      ERR No Cfg As For Asp: 0                      ERR Subsystem Status : 0
    XUA Error Messages Received Stats
      ERR Invalid Version: 0                        ERR Unsupported Class: 0
      ERR Unsupported Type: 0                       ERR Traffic Mode: 0
      ERR Unexpected Msg: 0                         ERR Protocol Error: 0
      ERR Invalid Stream ID: 0                      ERR Refused, Mgmt Block: 0
      ERR ASP ID Required: 0                        ERR Invalid ASP ID: 0
      ERR Invalid Parm Value: 0                     ERR Parm Field Error: 0
      ERR Unexpected Parm: 0                        ERR Dest Status Unknown: 0
      ERR Inv Network App: 0                        ERR Missing Parm: 0
      ERR RK Change Refused: 0                      ERR Inv Routing Context: 0
      ERR No Cfg As For Asp: 0                      ERR Subsystem Status : 0
    XUA Notify Messages Sent Stats
      NOTIFY-AS Inactive: 0                         NOTIFY-AS Active: 0
      NOTIFY-AS Pending: 0                         NOTIFY-Insuf ASP: 0
      NOTIFY-Alt ASP Active: 0                     NOTIFY-ASP Failure: 0
```

```

Outbound SSNM From SS7 Stats
TFAs Rcvd: 0
TFRs Rcvd: 0
Cong 0 TFCs Rcvd: 0
Cong 2 TFCs Rcvd: 0
TFPs Rcvd: 0
UPUs Rcvd: 0
Cong 1 TFCs Rcvd: 0
Cong 3 TFCs Rcvd: 0

Outbound SSNM to ASP Stats
DUNAs Sent: 0
DRSTs Sent: 0
Cong 0 SCONs Sent: 0
Cong 2 SCONs Sent: 0
Cong 4 SCONs Sent: 0
Cong 6 SCONs Sent: 0
DAVAs Sent: 0
DUPUs Sent: 0
Cong 1 SCONs Sent: 0
Cong 3 SCONs Sent: 0
Cong 5 SCONs Sent: 0
Cong 7 SCONs Sent: 0

Inbound SSNM to SS7 Stats
TFAs Sent: 0
TFRs Sent: 0
Cong 0 TFCs Sent: 0
Cong 2 TFCs Sent: 0
TFPs Sent: 0
UPUs Sent: 0
Cong 1 TFCs Sent: 0
Cong 3 TFCs Sent: 0

Inbound SSNM from ASP Stats
SCON No Level Rcvd: 0
DUNAs Rcvd: 0
Cong 0 SCONs Rcvd: 0
Cong 2 SCONs Rcvd: 0
Cong 4 SCONs Rcvd: 0
Cong 6 SCONs Rcvd: 0
DAUDs Rcvd: 0
DAVAs Rcvd: 0
Cong 1 SCONs Rcvd: 0
Cong 3 SCONs Rcvd: 0
Cong 5 SCONs Rcvd: 0
Cong 7 SCONs Rcvd: 0

Congestion Stats
Pkts Dropped At Lvl 1: 0
Pkts Dropped At Lvl 3: 0
Level 1 Congestion Cnt: 0
Level 3 Congestion Cnt: 0
T1 Timeouts: 0
Pkts Dropped At Lvl 2: 0
Level 2 Congestion Cnt: 0
Level 4 Congestion Cnt: 0
T6 Timeouts: 0

```

Options for ASP state include: Down/Inactive/Active/Standby

Options for ASP availability include: Shutdown/Enabled

Monitoring and Mated SG Pairs

The following is sample output from the **show cs7** command:

```

ITP# show cs7
  Local port: 14002      State: active      SCTP instance handle: 5
  Local ip address:      172.18.48.39
  Number of active peers: 0
  Max number of inbound streams allowed: 17
  Local receive window: 5555
  Max init retransmissions: 8
  Max init timeout: 1000 ms
  Unordered priority: equal
  Offload to FlexWAN: No Slot: -1
  SCTP defaults for new associations
    Transmit queue depth: 1000      Cumulative sack timeout: 200 ms
    Assoc retransmissions: 17      Path retransmissions: 4
    Minimum RTO: 1000 ms          Maximum RTO: 1000 ms
    Bundle status: on              Bundle timeout: 5 ms
    Keep alive status: true        Keep alive timeout: 30000 ms
    Initial cwnd: 3000             Idle cwnd rate: 50
    Retrans cwnd rate: 50          Retrans cwnd mode: RFC
    FastRetrans rate: 50

```

The following is sample output from the **show cs7 mated-sg** command in the default brief format:

Options for the SG Mate state include: Inactive/Active/Shutdown

If the Mate is shutdown, then the remote port and remote IP address display the configured values instead of the actual values.

Router# **show cs7 mated-sg**

Mate Name	State	Passive	Remote Port	Effect Primary Remote IP Addr	SCTP Assoc
bermuda	active	no	14002	172.18.48.15	0

The following is sample output from the **show cs7 mated-sg** command with the **detail** keyword:

Options for SG Mate state include: Inactive/Active/Shutdown

Router# **show cs7 mated-sg detail**

```

Mated SG name: bermuda                               Type:
State: active
SCTP association state: established                   Association id: 5
Configured remote port: 14002                         Actual remote port: 14002
Configured remote ip addresses: 172.18.48.15
Actual remote ip addresses: 172.18.48.15             State: active (effective prim)
Passive: yes                                           Nonpassive retry timeout: 30000 ms
Local receive window: 64000                           Cumulative sack timeout: 200 ms
Assoc retrans: 10                                     Path retrans: 4
Max init retrans: 8                                   Max init RTO: 1000 ms
Minimum RTO: 1000 ms                                Maximum RTO: 1000 ms
Bundle status: on                                     Bundle timeout: 5 ms
Keep alive status: true                               Keep alive timeout: 30000 ms
Unordered priority: equal                             Cleanup timeout: 0 ms
Link status T1 timeout: 0 ms                          Remote congest T6 timeout: 0 ms
SCTP congestion level: 0                             SCON congestion level: 0
Transmit queue depth: 20000                           Burst recovery timeout: 2002 ms
Thresholds for congestion on transmit queue
  Level 1 onset: 10000                                Level 1 abate: 6000
  Level 2 onset: 14000                                Level 2 abate: 10000
  Level 3 onset: 18000                                Level 3 abate: 14000
  Level 4 onset: 20000                                Level 4 abate: 18000

```

The following is sample output from the **show cs7 mated-sg** command with the **statistics** keyword:

Router# **show cs7 mated-sg statistics**

```

Mated-Sg name: bermuda                               Type:
Active Time: 00:01:23
  Data Packets/MSU Stats
    Inbound Packets Rcvd: 0                           Inbound Octets Rcvd: 0
    Inbound Packets Sent: 0                           Inbound Octets Sent: 0
    Outbound Packets Sent: 0                           Outbound Octets Sent: 0
  Buffer Allocation Stats
    Buffer Alloc Failures: 0                           Buffer Growth Failures: 0
    Buffer Reused: 0
  Congestion Stats
    Pkts Dropped At Pri 0: 0                           Pkts Dropped At Pri 1: 0
    Pkts Dropped At Pri 2: 0
    Level 1 Congestion Cnt: 0                           Level 2 Congestion Cnt: 0
    Level 3 Congestion Cnt: 0                           Level 4 Congestion Cnt: 0
    T1 Timeouts: 0                                     T6 Timeouts: 0

```

Monitoring Routes

Why is this task important?

Monitoring routes is important because it reveals the status of all the routes in the network, and thus the ability of the network to transport messages efficiently.

Under what circumstances should routes be monitored?

The status of routes should be monitored whenever the performance of the network is noticeably degraded. This may reveal congestion on specific routes, for example, which may indicate a need to deploy more links. In conjunction with other system messages it may reveal failures in various network components.

What incidents or system messages should prompt the user to issue the `show cs7 route` command?

Whenever a destination accessibility status change message such as the following appears on the console:

```
00:05:51:%CS7MTP3-5-DESTSTATUS:Destination 10.5.1 is inaccessible
```

Whenever a destination is reported to be inaccessible or restricted, the **show cs7 route detailed** command will reveal what caused the destination to enter that state.

Should this task be part of a regular monitoring process that the user should do at regular intervals? If so, how frequently?

Normally this should be performed to verify the configuration of new routes or deletion/modification of existing routes. A regular monitoring is not needed because system generated messages (such as in the example shown above) will inform the user of any abnormal operating conditions.

What commands does the user issue?

The **show cs7 route** command displays information such as the following:

```
router# show cs7 route
Routing table = system
```

Destination	Prio	Linkset	Name	Route
1.1.1/14	acces	1	bermuda	avail
3.1.1/14	acces	5	bermuda	avail

```
Routing table = XUA
```

Destination	Cong
2.1.1/14	INACC

Refer to the [ITP Command Set](#) chapter of this document for detailed descriptions of the show commands.

Monitoring Gateway Screening Violations

Why is this task important?

When screening is configured you can view screening activity.

Under what circumstances should this task be performed?

When screening is configured.

What incidents or system messages should prompt the user to monitor gateway screening violations?

None. Violations do not appear as system messages because of the volume of messages this might generate.

Should this task be part of a regular monitoring process that the user should do at regular intervals? If so, how frequently?

At user's discretion.

What commands does the user issue?

```
show cs7 access-lists
```

```
show cs7 accounting access-violations [checkpoint]
```

Refer to the “Command Reference” section of this document for detailed descriptions of the show commands.

Monitoring System Messages

Why is this task important?

System messages are part of the ITP alert infrastructure.

Under what circumstances should this task be performed?

Monitoring should be automated via an external syslog server.

What incidents or system messages should prompt the user to monitor system messages?

Refer to the Cisco IOS Software System Error Messages documentation at the following URL:
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121sup/index.htm>

Should this task be part of a regular monitoring process that the user should do at regular intervals? If so, how frequently?

Yes, this process should be ongoing and automated.

What commands does the user issue?

```
show log
```

Monitoring Accounting

Why is this task important?

Monitoring accounting provides information about user-specific usage.

Under what circumstances should this task be performed?

At user's discretion.

What incidents or system messages should prompt the user to monitor system messages?

Traffic degradation, debugging of problems.

Should this task be part of a regular monitoring process that the user should do at regular intervals? If so, how frequently?

At user's discretion. This task can be part of ongoing statistics collection to be used for network capacity planning or traffic profiling.

What commands does the user issue?

accounting

show cs7 accounting [checkpoint]

show cs7 linkset statistics

Refer to the "Command Reference" section of this document for detailed descriptions of the show commands.

Summary of Commands to Monitor Cisco ITP

The following is a summary of commands in EXEC mode to monitor various functions of Cisco ITP.

Command	Purpose
Router# show cs7 access-lists	Displays ITP access lists.
Router# show cs7 accounting [access-violations] [checkpoint]	Displays accounting details.
Router# show cs7 as [binding-table [m3ua [include-gtt exclude-gtt only-gtt]] [sua [include-gtt exclude-gtt only-gtt]] [all [include-gtt exclude-gtt only-gtt]] [name as-name] [operational active all] [statistics detail brief event-history]	Displays CS7 AS statistics.
Router# show cs7 [instance-number] asp [m3ua sua all name asp-name asname as-name] [statistics [detail] bindings detail event-history]	Displays CS7 ASP statistics.
Router# show cs7 gtt {address-conversion application-group concern-pclist config consistency gta selector map measurements selector}	Displays GTT statistics.
Router# show cs7 linkset [ls-name routes sls statistics timers ttmap] [brief detailed]	Displays ITP linkset statistics.
Router# show cs7 m2pa {[local-peer port-num] [peer ls-name [slc]] [state ls-name [slc]] [statistics ls-name [slc]]}	Displays ITP M2PA statistics.
Router# show cs7 m3ua local-port	Displays CS7 M3UA statistics.
Router# show cs7 mated-sg	Displays CS7 Mated SG statistics.

Command	Purpose
Router# show cs7 mtp2 [congestion state statistics timers variant] <i>interface</i>	Displays ITP MTP2 statistics.
Router# show cs7 mtp3 timers	Displays output from MTP3 timers.
Router# show cs7 ping <i>point-code</i>	Displays output from a Cisco ITP ping test.
Router# show cs7 point-codes [event-history ssn]	Displays point codes the ITP SG is responding to.
Router# show cs7 qos {[class <i>class</i>] [statistics <i>ls-name</i>]}	Displays QoS class information.
Router# show cs7 route [<i>destination</i>] [brief detailed]	Displays the routing table.
Router# show cs7	Displays Signaling Gateway Mate Protocol () information.
Router# show cs7 sua	Displays CS7 SUA information.

Tuning ITP

The following sections provide information about tuning the Cisco ITP:

- [Tuning HSL Parameters, page 394](#)
- [Tuning MTP3 Timers, page 397](#)
- [Tuning MTP2 Parameters, page 398](#)
- [Tuning SCTP Parameters, page 402](#)

Tuning HSL Parameters

ITP allows you to specify bundling, SSCF-NNI, and SSCOP parameters for ATM HSL support. You can choose either or both of two configuration methods. You can configure the parameters in a CS7 profile that you apply globally to all links in a linkset. Or, you can specify or modify the parameters on a specific link.

The following sections describe both methods for specifying HSL parameters:

[Create a Profile to Support HSL, page 394](#)

[Specify HSL Parameters on a Link, page 397](#)

Create a Profile to Support HSL

You can create a CS7 profile, specify the HSL parameters, then apply the profile to a linkset.

Step 1 Create a CS7 Profile

To create the profile use the following commands, beginning in global configuration mode:

Command	Purpose
Router(config)# cs7 profile <i>name</i>	Names the CS7 profile and enables CS7 profile configuration mode.
Router(config-cs7-profile)# hsl	Enables the CS7 profile mode for configuring HSL parameters.

Step 2 Specify HSL Parameters

A CS7 profile can specify values for SSCF-NNI parameters, SSCOP parameters, and bundling.

The SSCF NNI provides mapping of the services provided by SSCOP and of the SAAL to the ULP, in this case MTP3.

To configure the HSL parameters for SSCF-NNI, use the following commands in CS7 profile configuration mode:

Command	Purpose
Router(config-cs7-profile-hsl)# sscf-nni force-proving timer	Specify the time (in minutes) to monitor the link after proving. The range is 0 to 20 minutes. The default is 10 minutes.
Router(config-cs7-profile-hsl)# sscf-nni n1 num	Specify the number of PDUs sent during proving. The range is 5 to 180000 PDUs. The default for ITU is 1000 PDUs. The default for ANSI is 60000 PDUs.
Router(config-cs7-profile-hsl)# sscf-nni no-credit timer	Specify the time (in seconds) allowed with no credit. The range is 1 to 6 seconds. The default is 2 seconds.
Router(config-cs7-profile-hsl)# sscf-nni nrp num	Specify the maximum number of retransmissions allowed during proving. The range is 1 to 10 retransmissions. The default is 1 retransmission.
Router(config-cs7-profile-hsl)# sscf-nni sscop-recovery timer	Specify the time (in minutes) for SSCOP recovery. The range is 30 to 1440 minutes. The default is 60 minutes.
Router(config-cs7-profile-hsl)# sscf-nni t1 timer	Specify the time (in seconds) to reestablish connection. The range is 1 to 15 seconds. The default is 5 seconds.
Router(config-cs7-profile-hsl)# sscf-nni t2 timer	Specify the time (in seconds) for alignment to complete. The range is 15 to 180 seconds. The default for ITU is 30 seconds. The default for ANSI is 120 seconds.
Router(config-cs7-profile-hsl)# sscf-nni t3 timer	Specify the time (in milliseconds) to send proving packets. The range is 1 to 5000 milliseconds. The default is 1 millisecond.

The Service-Specific connection -Oriented Protocol (SSCOP) resides in the service-specific convergence sublayer (SSCS) of the ATM adaptation layer (AAL). SSCOP is used to transfer variable-length service data units (SDUs) between users of SSCOP. SSCOP provides for the recovery of lost or corrupted SDUs.

To configure the HSL parameters for SSCOP, use the following commands in CS7 profile configuration mode:

Command	Purpose
Router(config-cs7-profile-hsl)# sscop cc-timer timer	Specify the time (in milliseconds) to send BGN/END/RS/ER PDU at the connection control phase. The range is 100 to 2000 milliseconds. The default is 200 milliseconds.
Router(config-cs7-profile-hsl)# sscop idle-timer timer	Specify the time (in milliseconds) to send poll PDU at the idle phase. The range is 25 to 1000 milliseconds. The default is 100 milliseconds.
Router(config-cs7-profile-hsl)# sscop keepalive-timer timer	Specify the time (in milliseconds) to send poll PDU at the transient phase. The range is 25 to 500 milliseconds. The default is 100 milliseconds.

Command	Purpose
Router(config-cs7-profile-hsl)# sscop max-cc num	Specify the maximum number of retries for connection control operations. The range is 1 to 127 retries. The default is 4 retries.
Router(config-cs7-profile-hsl)# sscop max-pd num	Specify the maximum number of Sd frames to send before sending a Poll. The range is 1 to 500 Sd frames. The default is 500 Sd frames.
Router(config-cs7-profile-hsl)# sscop noResponse-timer timer	Specify the time (in milliseconds) in which at least one STAT PDU must be received. The range is 200 to 2000 milliseconds. The default is 1500 milliseconds.
Router(config-cs7-profile-hsl)# sscop poll-timer timer	Specify the times (in milliseconds) to send poll PDU at the active phase. The range is 25 to 500 milliseconds. The default is 100 milliseconds.
Router(config-cs7-profile-hsl)# sscop receive-window num	Specify the maximum number of Sd(p) frames our partner can send. The range is 1 to 1024 Sd(p) frames. The default is 1024 Sd(p) frames.
Router(config-cs7-profile-hsl)# sscop send-window num	Specify the maximum number of Sd frames to send before waiting for acknowledgement. The range is 1 to 1024 frames. The default is 1024 frames.

To configure HSL bundling, use the following command in CS7 profile configuration mode:

Command	Purpose
Router(config-cs7-profile-hsl)# bundling interval	Specifies (in milliseconds) the HSL packet bundling interval. The range is 5 to 100 milliseconds. The default is 5 milliseconds.

Step 3 Apply the CS7 Profile to a Linkset

After you have created the profile, apply it to a linkset by using the following commands, beginning in CS7 profile configuration mode:

Command	Purpose
Router(config-cs7-profile-hsl)# cs7 linkset ls-name	Specifies the linkset to which you will apply the profile, and enters linkset configuration mode.
Router(config-cs7-ls)# profile name	Applies the parameter values specified in the profile to all the links in the linkset.



Note

Whenever you change the CS7 profile, the revised profile automatically applies to the linkset.



Note

You can override parameter applied with the profile by configuring the specific parameter on the link.

Specify HSL Parameters on a Link

You can specify/modify individual HSL parameters on a link, or you can specify/modify all the HSL parameters on the link. To configure parameters on a link, use any of the commands described in [Step 2 Specify HSL Parameters, page 395](#) from CS7 link configuration mode. To enable CS7 link configuration mode, use the following commands, beginning in global configuration mode:

Command	Purpose
Router(config)# cs7 linkset <i>ls-name</i>	Specifies the linkset to which you will apply the profile, and enters linkset configuration mode.
Router(config-cs7-ls)# link <i>slc</i>	Identifies the link to which you intend to apply HSL parameters, and enter CS7 link configuration mode.

Tuning MTP3 Timers

MTP3 timers can be defined at 3 levels, global, linkset, and link.

All global, linkset, and link specific timers can be defined at the global level. These values serve as defaults and are propagated down to the lower levels.

To globally configure MTP3 timers, Use the following command in global configuration mode:

Command	Purpose
Router(config)# cs7 mtp3 timer <i>timer msec</i>	Configure MTP3 timers for the system, the linkset, or the link. ¹

1. For details about the MTP3 timers that you can configure with this command, see the Command Reference entry for [cs7 mtp3 timer](#).

Linkset and link specific timers can be defined at the linkset level. These values serve as defaults for the linkset and all links defined within that linkset. Any values defined at the linkset level will override any global values.

To configure MTP3 timers on a linkset, use the following commands in linkset configuration mode:

Command	Purpose
Router(config-ls)# timer <i>timer msec</i>	Configure MTP3 timers for a linkset, and (optionally) for links on the linkset. For details about the MTP3 timers that you can configure with this command, see the Command Reference page for timer .
Router(config-ls)# sls-shift {0-3}	Shift which SLS bits are used for link and linkset selection. Available for ITU variant only.

Link specific timers can be defined at the link level. Timers defined at the link level will apply to the link and will override any values for that timer defined at either the linkset, or global level.

To configure MTP3 timers on a link, use the following commands in linkset configuration mode:

Command	Purpose
Router(config-ls-link)# link-timer <i>timer msec</i>	Configure MTP3 link timers. For details about the MTP3 timers that you can configure with this command, see the Command Reference page for link-timer .

Tuning MTP2 Parameters

The following sections describe the MTP2 parameters that you can tune, and describes 2 methods for specifying MTP2 parameters for a link:

- [Understanding the MTP2 Parameters, page 398](#)
- [Specifying MTP2 Parameters in a CS7 Profile, page 399](#)
- [Specifying MTP2 Parameters Individually, page 401](#)

Understanding the MTP2 Parameters

You can customize MTP2 protocol parameters for timers, bundling, and transmit queue depth to control and influence the MTP2 behavior.

MTP2 Timers

You can adjust the following MTP2 timers:

- T1 (alignment ready)
- T2 (not aligned)
- T3 (aligned)
- T4E (emergency proving period)
- T4N (normal proving period)
- T5 (sending SIB)
- T6 (remote congestion)
- T7 (excessive delay of acknowledgment)
- TTC timers, including
 - **ttc ta timer**: TTC Timer for sending SIE. Valid range is 10 to 250 milliseconds. Default is 20 milliseconds.
 - **ttc te timer**: TTC Timer for error monitoring. Valid range is 10 to 250 milliseconds. Default is 20 milliseconds.
 - **ttc tf timer**: TTC Timer for sending FISU. Valid range is 10 to 250 milliseconds. Default is 20 milliseconds.
 - **ttc to timer**: TTC Timer for sending SIO. Valid range is 10 to 250 milliseconds. Default is 20 milliseconds.
 - **ttc ts timer**: TTC Timer for sending SIOS. Valid range is 10 to 250 milliseconds. Default is 20 milliseconds.

Bundling

The bundling parameter is used to set the bundling interval (an amount of time to wait for packets before sending the bundle). It is recommended that bundling be enabled for high packet rates (1000 pps or higher) with small packets (50 bytes and lower). Bundling can be less than optimal for lower data rates with small or large packets because of the transmission delay. Bundling is found to be effective for large packets at high data rates in networks with symmetrical traffic. Applications with low data rates should disable bundling if the increase in round-trip time is undesirable. It is recommended that bundling be enabled for applications sending small packets that may start with low data rates, but are capable of increasing to higher sustained data rates. The default bundling delay is 5 milliseconds.

Transmit Queue

The tx-queue-depth parameter is used to determine the onset and abate thresholds for congestion on transmit queue. The tx-queue-depth parameter controls the number of packets allowed on the transmit queue. The tx-queue exist to absorb inevitable traffic burst. When selecting the tx-queue-depth, there will be a compromise between hitting transmit congestion thresholds causing dropped packets and transmit delays due to queuing times. Applications that are sensitive to small delays should account for transmit delays due to queuing when selecting a tx-queue-depth. During periods of SCTP link congestion, the tx-queue-depth will control the number of packets that can be queued before packets are discarded, causing application retransmissions. The default tx-queue-depth is 1000 packets for M3UA and SUA. The default tx-queue-depth is 20,000 packets for SGMP.

Specifying MTP2 Parameters in a CS7 Profile

You can create a CS7 profile that specifies MTP2 parameters, then apply the profile to a link.

Step 1 Create a CS7 Profile.

A CS7 profile can specify values for MTP2 timers, bundling, and transmit queue depth. To create the profile use the following commands, beginning in global configuration mode:

Command	Purpose
Router(config)# cs7 profile <i>name</i>	Names the CS7 profile and enables CS7 profile submenu.
Router(config-cs7-profile)# mtp2	Enables the CS7 profile submenu for configuring MTP2 parameters.
Router(config-cs7-profile-mtp2)# bundling <i>msec</i>	Enables bundling and specifies the bundling interval (the length of time to wait for packets before sending a bundle).

Command	Purpose
Router(config-cs7-profile-mtp2)# timer { t1 t2 t3 t4e t4n t5 t6 t7 ttc timer } <i>msec</i>	Specifies the following MTP2 timers: ¹ - t1 -- T1 (alignment ready) - t2 -- T2 (not aligned) - t3 -- T3 (aligned) - t4e -- T4E (emergency proving period) - t4n -- T4N (normal proving period) - t5 -- T5 (sending SIB) - t6 -- T6 (remote congestion) - t7 -- T7 (excessive delay of acknowledgment) - ttc ta timer -- TTC Timer for sending SIE. Valid range is 10 to 250 milliseconds. Default is 20 milliseconds. - ttc te timer -- TTC Timer for error monitoring. Valid range is 10 to 250 milliseconds. Default is 20 milliseconds. - ttc tf timer -- TTC Timer for sending FISU. Valid range is 10 to 250 milliseconds. Default is 20 milliseconds. - ttc to timer -- TTC Timer for sending SIO. Valid range is 10 to 250 milliseconds. Default is 20 milliseconds. - ttc ts timer -- TTC Timer for sending SIOS. Valid range is 10 to 250 milliseconds. Default is 20 milliseconds.
Router(config-cs7-profile-mtp2)# tx-queue-depth <i>msec</i>	Specifies the number of packets that MTP2 will queue for transmission.
Router(config-cs7-profile-mtp2)# exit	Exits the CS7 profile submode for MTP2.
Router(config-cs7-profile)# exit	Exits the CS7 profile submode (returning you to global configuration mode).

1. For detailed information about MTP2 timers, refer to the appropriate standards.

Step 2 Apply the profile to all of the links in a linkset.

After you have created the profile, apply it to a linkset by using the following commands, beginning in global configuration mode:

Command	Purpose
Router(config)# cs7 linkset <i>ls-name</i>	Specifies the linkset to which you will apply the profile, and enters linkset configuration mode.
Router(config-cs7-ls)# profile <i>name</i>	Applies the parameter values specified in the profile to all the links in the linkset. (The no version of this command removes the profile from the linkset and resets the MTP2 parameters to the default values.)



Note

Whenever you change the CS7 profile, the revised profile automatically applies to the linkset.

**Note**

You can override an MTP2 parameter applied with the profile by configuring the specific parameter on the link.

Specifying MTP2 Parameters Individually

You can specify or change the values of MTP2 timers, bundling, and transmit queue depth individually at the link level.

To tune the MTP2 timers, use the following command in CS7 link submode:

Command	Purpose
Router(config-cs7-ls-link)# mtp2-timer {t1 t2 t3 t4e t4n t5 t6 t7} msec	Specifies the following MTP2 timers: ¹ - t1 -- T1 (alignment ready) - t2 -- T2 (not aligned) - t3 -- T3 (aligned) - t4e -- T4E (emergency proving period) - t4n -- T4N (normal proving period) - t5 -- T5 (sending SIB) - t6 -- T6 (remote congestion) - t7 -- T7 (excessive delay of acknowledgment)

1. For detailed information about MTP2 timers, refer to the appropriate ANSI and ITU standards.

To enable bundling of packets sent between MTP3 on the Route Processor and MTP2 on the FlexWAN, and to specify the bundling interval for the link, use the following command in CS7 link submode:

Command	Purpose
Router(config-cs7-ls-link)# bundling msec	Enables bundling and specifies the bundling interval (the length of time to wait for packets before sending a bundle).

You can adjust the number of packets that can be queued for transmission before reaching a state of transmit congestion. This parameter is known as the transmit queue depth.

The values for this parameter vary depending on the type of link. For an MTP2 link, the range is 25 to 5000 packets with a default of 500 packets. For an SCTP link, the range is 100 to 20000 packets, with a default of 1000 packets.

To tune the transmit queue depth for the link, use the following command in CS7 link submode:

Command	Purpose
Router(config-cs7-ls-link)# tx-queue-depth packets	Specifies the number of packets allowed on the transmit queue.

Tuning SCTP Parameters

The following sections describe SCTP parameters and tasks:

- [How SCTP Parameters Work, page 402](#)
- [Tuning SCTP Parameters for M2PA, page 404](#)
- [Tuning SCTP Parameters for M3UA and SUA, page 407](#)
- [Tuning SCTP Parameters for an ASP, page 408](#)
- [Tuning AS Options, page 408](#)
- [Tuning SCTP Parameters for a Mated SG, page 409](#)
- [Tuning SCTP Parameters for Satellite Channels, page 410](#)

How SCTP Parameters Work

SCTP provides several protocol parameters that can be customized by the upper layer protocol. These protocol parameters can be customized to control and influence SCTP performance behavior. Different network designs and implementations pose their own unique performance requirements. It is not possible to provide customized protocol parameters that are suitable for all implementations. The tuning information in this section is provided as a guide for understanding what the SCTP protocol parameters are and how they affect the various SCTP algorithms.

Connection Establishment

The protocol parameters `assoc-retransmit`, `init-retransmit` and `init-timeout` can be customized to control connection establishment. During SCTP association initialization sometimes packet retransmissions occur. When initialization packet retransmissions occur, the timeout value is doubled for each retransmission. The first initialization packet timeout occurs after 1 second. The maximum timeout value is bound by the `init-timeout` parameter. The `init-timeout` parameter is used to control the time between initialization packet retries. As a general rule, `init-timeout` should be configured to reflect the round-trip-time for packets to traverse the network. An `init-timeout` value that is too small, can cause excessive retries of initialization packets. Large `init-timeout` values can increase connection establishment times.

The number of retries allowed for connection establishment packets is controlled by the `init-retransmit` protocol parameter. When you configure the number of retries to attempt, take into account the varying network conditions that may prevent initialization packets from traversing the network.

The defaults used by M2PA are recommendations from RFC 2960 or RFC 4960 depending upon which RFC version has been provisioned. The `init-timeout` default is 1 second. The `init-retransmit` default is set for 8. The `init-retransmit` and `init-timeout` defaults are suitable for most high-speed links. The defaults may require adjusting for slower links.

SCTP Multi-homing

A key feature of SCTP is multi-homing. An SCTP endpoint is considered multi-homed if more than one IP address can be used as a destination to reach that endpoint. Upon failure of the primary destination address SCTP switches to an alternate address.

In the configuration of a multi-homed endpoint, the first remote IP address specified on the peer link is defined as the primary address. If the primary address is determined to be unreachable, SCTP multi-homing switches to one of the alternate addresses specified on the peer link. SCTP will monitor the reachability of the failed destination address. Upon notification that reachability is re-established to the primary address, M2PA directs SCTP to switch back to the primary address.

The protocol parameters `path-retransmit` and `retransmit-timeout` can be customized to control how long SCTP waits before switching to an alternate address. The `path-retransmit` parameter controls the number of times that SCTP attempts to retransmit a packet before declaring the destination address unreachable. The `retransmit-timeout` parameter is used to determine whether a packet must be retransmitted. If an acknowledgement is not received by the time the retransmission timer expires, all packets that have been transmitted, but not acknowledged are retransmitted.

Path-retransmit

The `path-retransmit` parameter is the number of packet retries before the destination address is deemed unreachable. The number of `path-retransmits` multiplied by the retransmission timer ultimately controls how fast an alternate address becomes the primary path for multi-homed nodes. This relationship suggests the RTO parameters and `path-retransmit` parameter should be considered together. Configuring the default RTO values and default `path-retransmit` value of 4 allows a multi-homed node to switch to an alternate destination address within 4 seconds.

Retransmit-timeout

The retransmission timeout (RTO) should be adjusted for round-trip delay between nodes. Preferably, the retransmission timeout should be greater than the round-trip delay between nodes. There will be a compromise between allowing a long delay, and having responsive discovery of lost frames. We can calculate a simplistic estimate of round-trip times (rtt) for various packet sizes (ignoring propagation delay and latencies in transmission equipment) using the following estimated rtt equation:

$$\text{estimated rtt} = ((\text{packet size} * \text{bits per byte}) / \text{link speed}) * 2$$

Assume a packet with a 20 byte IP header, 32 byte sctp header and 100 bytes of user data and a 1,544,000 bits/sec link between two nodes. Using the estimated rtt equation shown in the previous paragraph we estimate an rtt of 1.5 ms.

SCTP computes RTO values based on rtt measurements. When packet retransmission occurs, the timeout value is doubled for each retransmission, with an upper limit of `max rto`. Multi-homed nodes will have to compromise between allowing a long delay and having responsive switching to an alternate IP address. Switching to an alternate path is of primary importance for multi-homed nodes. The maximum `rto` value for multi-homed nodes should be set equal to or just slightly higher than the minimum RTO value. The number of outstanding bytes allowed decreases with each retransmission timeout. The trade-off of bounding the maximum RTO close to the minimum RTO is the frequency of retransmissions versus increasing transmit delays for packets on the transmit queue. During periods of retransmissions multi-homed nodes sends duplicate packets until the alternate address becomes the primary path. The alternate address becomes the primary when the number of retries exceed the `path-retransmit` parameter. The default value for minimum and maximum RTO is 1 second. Propagation delays and latencies vary in networks, so care should be taken when selecting an RTO value.

Bundling

It is recommended that bundling be enabled for high packet rates (1000 pps or higher) with small packets (50 bytes and lower). Bundling can be less than optimal for lower data rates with small or large packets because of the transmission delay. Bundling is found to be effective for large packets at high data rates in networks with symmetrical traffic. The default bundling delay is 5 ms. Applications with low data rates should disable bundling if the increase in round-trip time is undesirable. It is recommended that bundling be enabled for applications sending small packets that may start with low data rates, but are capable of increasing to higher sustained data rates.

Cumulative Selective Ack

The cumulative selective ack (cs-ack) is commonly known as “delayed ack.” The cs-ack parameter controls how long a receiver can delay before sending an acknowledgment. The ack is delayed hoping to have data going in the same direction as the ack, so the ack can “piggyback” with the data. The default of cs-ack is 200 ms. The cs-ack configured at the receiver should be less than the rto minimum value configured at the sender. When the cs-ack of the receiver is greater than the rto of the sender, unnecessary retransmissions may occur because the sender rto expires before the receiver sends the delayed acknowledgment.

Receive Window

The size of the receive window offered by the receiver generally can affect performance. SCTP adapts its transmission rate to suit the available network capacity by using a congestion-sensitive, sliding-window flow control mechanisms described in RFC 2581. At any given instance only a certain number of bytes can be outstanding through the network. Keeping the path full of packets requires both congestion window (cwnd) and receive window (rwnd) to reach the effective size of the “pipe” represented by the so-called bandwidth-delay product. We can calculate the capacity of the pipe using the following capacity equation:

$$\text{capacity (bits)} = \text{bandwidth (bits/sec)} \times \text{round-trip-time(sec)}$$

The bandwidth-delay product can vary widely depending on the network speed and round-trip-time (rtt) between the two end points. Using the capacity equation shown in the previous paragraph, we can estimate the minimum buffer size given the bandwidth of the communication media and the round-trip time between the nodes. Assuming the nodes are connected by a 1,544,000 bits/sec T1 link with a round-trip time of 60 ms, gives an estimated minimum buffer size of 11,580 bytes. The receive-window parameter default is set for 64000 bytes. The congestion control and windowing algorithms adjust to network conditions by controlling the number of bytes that can be outstanding through the network.

Transmit Queue

The tx-queue-depth parameter is used to determine the onset and abate thresholds for congestion on the transmit queue. The tx-queue-depth parameter controls the number of packets allowed on the transmit queue. The transmit queue exists to absorb the inevitable traffic bursts. When selecting the tx-queue-depth, there will be a compromise between hitting transmit congestion thresholds causing dropped packets and transmit delays due to queuing times. Applications that are sensitive to small delays should account for transmit delays due to queuing when selecting a tx-queue-depth. During periods of SCTP link congestion, the tx-queue-depth will control the number of packets that can be queued before packets are discarded, causing application retransmissions. The default tx-queue-depth is 1000 packets for M3UA and SUA. The default tx-queue-depth is 20,000 packets for SGMP.



Note

While changing the tx-queue-depth for a XUA, ensure there is no traffic on that ASP. If there is traffic on that ASP, as soon as the tx-queue-depth is changed, reset the ASP by using the **shutdown** and then the **no shutdown** commands. Resetting the ASP is required so the ASP is not stuck in congestion.

Tuning SCTP Parameters for M2PA

To tune the SCTP parameters at the M2PA level of the Cisco ITP, use the following commands in link configuration mode:

Command	Purpose
Router(config-cs7-ls-link)# assoc-retransmit <i>max-returns</i>	Configure the maximum number of consecutive retransmissions to a peer before the peer is considered unreachable.
Router(config-cs7-ls-link)# bundling <i>msec</i>	Enables bundling and specifies the bundling interval (the length of time to wait for packets before sending a bundle).
Router(config-cs7-ls-link)# cumulative-sack <i>msec</i>	Configures the cumulative selective acknowledgment time-out value for the link.
Router(config-cs7-ls-link)# init-retransmit <i>max-retries</i>	Configures the number of retransmissions for peer initialization messages.
Router(config-cs7-ls-link)# init-timeout <i>msec</i>	Configures the maximum time-out value for retransmission initialization messages.
Router(config-cs7-ls-link)# ip-precedence <i>ip-tos</i>	Sets the IP precedence.
Router(config-cs7-ls-link)# ip-dscp <i>ip-tos</i>	Sets the IP Differential Services Code Point.
Router(config-cs7-ls-link)# keepalive <i>msec</i>	Enable a peer link keepalive interval.
Router(config-cs7-ls-link)# large-msu-support	Allows an M2PA link to carry MSU sizes of up to 4096 bytes.
Router(config-cs7-ls-link)# path-retransmit <i>max-retries</i>	Configures path retransmissions on a remote peer address.
Router(config-cs7-ls-link)# peer-timer <i>timer msec</i>	Configures the alignment-ready timer.
Router(config-cs7-ls-link)# retransmit-timeout <i>rto-min</i> <i>rto-max</i>	Configure the retransmission time-out value on a link.
Router(config-cs7-ls-link)# tx-queue-depth <i>queue-depth</i>	Adjust the number of packets that M2PA will queue for transmission.

To tune the M2PA of the ITP on a local peer, use the following command in cs7 local-peer configuration submode:

Command	Purpose
Router(config-cs7-lp)# sctp-rfc-version {2960 4960}	Sets the RFC compliance to either SCTP RFC 2960 or SCTP RFC 4960. The default is SCTP RFC 2960.

To tune the M2PA levels of the ITP on a local peer, use the following command in CS7 local-peer configuration mode:

Command	Purpose
Router(config-cs7-lp)# receive-window <i>size</i>	Configures the local receive window size.

To tune the M2PA for all the links in the CS7 instance, use the following command in global configuration mode:

Command	Purpose
Router(config)# cs7 instance <i>instance-number</i> large-msu-support	Allows an instance to carry MSU sizes of up to 4096 bytes.

To tune the ITP all the M2PA links in the linkset, use the following command in cs7 m2pa profile configuration mode:

Command	Purpose
Router(config-cs7-profile-m2pa)# large-msu-support	Allows M2PA links to carry MSU sizes of up to 4096 bytes.

Tuning SCTP Parameters for M3UA and SUA

SCTP parameters that are set in the local instance are used as the defaults when an SCTP association is established. To configure SCTP parameters for M3UA or SUA local instance use the following commands in either CS7 M3UA, CS7, or CS7 SUA submode. The parameters function the same for all three modes and are shown here in CS7 M3UA mode:

Command	Purpose
Router(config-cs7-m3ua)# assoc-retransmit <i>max-returns</i>	Specifies the maximum number of association retransmissions to be used when a new SCTP association is started with the local port. Range is 2 to 20. Default is 10.
Router(config-cs7-m3ua)# bundling <i>msec</i>	Specifies that packet bundling is supported and configures the bundling interval to be used when a new SCTP association is started with the local port. Range is 5 to 1000 milliseconds. Default is 100.
Router(config-cs7-m3ua)# cumulative-sack <i>msec</i>	Configures the cumulative selective acknowledgment time-out value to be used when a new SCTP association is started with the local port. Range is 100 to 500 milliseconds. Default is 200.
Router(config-cs7-m3ua)# init-retransmit <i>max-retries</i>	Configures the maximum number of retransmissions of the peer initialization packets for the local port. Range is 2 to 20 milliseconds. Default is 8.
Router(config-cs7-m3ua)# init-timeout <i>msec</i>	Configures the maximum interval for the initialization packet retransmission timeout for the local port. Range is 1000 to 60000 milliseconds. Default is 1000.
Router(config-cs7-m3ua)# keepalive <i>msec</i>	Specifies that keepalive timer is supported and configures the keepalive interval to be used when a new SCTP association is started with the local port. Range is 300 to 30000 milliseconds. Default is 30000.
Router(config-cs7-m3ua)# max-inbound-streams <i>max-streams</i>	Specifies the maximum number of inbound streams allowed for the local port. Range is 2 to 25. Default is 17.
Router(config-cs7-m3ua)# path-retransmit <i>max-retries</i>	Configures the maximum number of path retransmissions on a remote address used when a new SCTP association is started with the local port. Range is 2 to 10 retries. Default is 4.
Router(config-cs7-m3ua)# receive-window <i>recv-win</i>	Specifies the local receive window size for the local port. Default is 24000.
Router(config-cs7-m3ua)# retransmit-timeout <i>rto-min</i> <i>rto-max</i>	Specifies the minimum retransmission timeout value used when a new SCTP association is started with the local port. Range is 40 to 60000 milliseconds. Default is 1000.
Router(config-cs7-m3ua)# sctp-rfc-version {2960 4960}	Sets the RFC compliance to either SCTP RFC 2960 or SCTP RFC 4960. The default is SCTP RFC 2960.
Router(config-cs7-m3ua)# tx-queue-depth <i>queue-depth</i>	Specifies the maximum transmit queue depth for new SCTP associations established with the local port.
Router(config-cs7-m3ua)# unordered-priority {equal high}	Specifies the priority of the unordered packets. The default is "equal."

Tuning SCTP Parameters for an ASP

SCTP parameters that are set in the local instance (in CS7 M3UA or CS7 SUA submode) are used as defaults when an SCTP association is established. You can override a default SCTP parameter by specifying an SCTP parameter in the CS7 ASP submode. To specify SCTP parameters under the ASP definition, use the following commands in CS7 ASP submode:

Command	Purpose
Router(config-cs7-asp)# assoc-retransmit <i>max-returns</i>	Specifies the maximum number of association retransmissions for the association. Range is 2 to 20. Default is the value specified under the local port instance.
Router(config-cs7-asp)# bundling <i>msec</i>	Specifies that packet bundling is supported and configures the bundling interval for the association. Range is 5 to 1000 milliseconds. Default is the value specified under the local port instance.
Router(config-cs7-asp)# cumulative-sack <i>msec</i>	Configures the cumulative selective acknowledgment time-out value for the association. Range is 100 to 500 milliseconds. Default is the value specified under the local port instance.
Router(config-cs7-asp)# keepalive <i>msec</i>	Specifies that keepalive timer is supported and configures the keepalive interval for the association. Range is 300 to 30000 milliseconds. Default is the value specified under the local port instance.
Router(config-cs7-asp)# path-retransmit <i>max-retries</i>	Configures the maximum number of path retransmissions on a remote address for the association. Range is 2 to 10 retries. Default is the value specified under the local port instance.
Router(config-cs7-asp)# retransmit-timeout <i>rto-min</i> <i>rto-max</i>	Specifies the minimum retransmission timeout value for the association. Range is 40 to 60000 milliseconds. Default is the value specified under the local port instance.
Router(config-cs7-asp)# tx-queue-depth <i>queue-depth</i>	Determines the onset and abate thresholds for congestion on transmit queue. Specifies the maximum transmit queue depth for the association. Default is the value specified under the local port instance.

Tuning AS Options

To configure the QoS class, recovery timeout value, or traffic mode for an AS, use the following commands in CS7 AS submode:

Command	Purpose
Router(config-cs7-as)# burst-recovery-timeout <i>msec</i>	Specifies the amount of time allowed for an association to recover from a burst of traffic caused by failover.
Router(config-cs7-as)# qos-class <i>class</i>	Specifies a QoS class for the packets sent to the ASPs in this AS. The QoS class defined under the ASP overrides the QoS class defined under the AS.

Command	Purpose
Router(config-cs7-as)# recovery-timeout <i>msec</i>	(Optional) Specifies the recovery timeout value. Range is 0 to 2000 milliseconds. Default is 2000.
Router(config-cs7-as)# traffic-mode { broadcast override loadshare [bindings roundrobin]}	(Optional) Specifies the traffic mode of operation of the ASP within an AS. Used to validate the traffic mode specified on the ASP Active messages. ASPs connecting with a different traffic mode will be failed.

Tuning SCTP Parameters for a Mated SG

SCTP parameters that are set in the local instance (in CS7 M3UA or CS7 SUA submode) are used as defaults when an SCTP association is established. You can override a default SCTP parameter by specifying an SCTP parameter in the CS7 Mated SG submode. To specify SCTP parameters under the Mated SG definition, use the following commands in CS7 Mated SG submode:

Command	Purpose
Router(config-cs7-mated-sg)# assoc-retransmit <i>max-returns</i>	Specifies the maximum number of association retransmissions for the association. Range is 2 to 20. Default is the value specified under the local port instance.
Router(config-cs7-mated-sg)# bundling <i>msec</i>	Specifies that packet bundling is supported and configures the bundling interval for the association. Range is 5 to 1000 milliseconds. Default is the value specified under the local port instance.
Router(config-cs7-mated-sg)# cumulative-sack <i>msec</i>	Configures the cumulative selective acknowledgment time-out value for the association. Range is 100 to 500 milliseconds. Default is the value specified under the local port instance.
Router(config-cs7-mated-sg)# keepalive <i>msec</i>	Specifies that keepalive timer is supported and configures the keepalive interval for the association. Range is 300 to 30000 milliseconds. Default is the value specified under the local port instance.
Router(config-cs7-mated-sg)# path-retransmit <i>max-retries</i>	Configures the maximum number of path retransmissions on a remote address for the association. Range is 2 to 10 retries. Default is the value specified under the local port instance.
Router(config-cs7-mated-sg)# qos-class <i>class</i>	Specifies the QoS class for the packets sent to the SG Mate.
Router(config-cs7-mated-sg)# retransmit-timeout <i>rto-min rto-max</i>	Specifies the minimum retransmission timeout value for the association. Range is 40 to 60000 milliseconds. Default is the value specified under the local port instance.
Router(config-cs7-mated-sg)# tx-queue-depth <i>queue-depth</i>	Determines the onset and abate thresholds for congestion on transmit queue. Specifies the maximum transmit queue depth for the association. Range is 100 to 65535 packets. Default is the value specified under the local port instance.

Tuning SCTP Parameters for Satellite Channels

This section includes the following information about SCTP and Satellite Channels

- [Overview of SCTP and Satellite Channels, page 410](#)
- [Tuning SCTP on Satellite Channels, page 411](#)
- [Verifying SCTP Parameters on Satellite Channels, page 413](#)

Overview of SCTP and Satellite Channels

There is an inherent delay in the delivery of a message over a satellite link due to the finite speed of light and the altitude of communication satellites. Satellite channels have several characteristics that are different from most terrestrial channels. These characteristics can degrade the performance and channel utilization of SCTP. Some of the characteristics include long delays, large delay-times-bandwidth products, and transmission errors. The delay-times-bandwidth product defines the amount of data a protocol should have outstanding at any one time to fully utilize the available channel capacity. Some satellite channels exhibit a higher bit-error rate than typical terrestrial networks. SCTP interprets all packet drops as signals of network congestion. Since SCTP cannot determine if a packet loss was due to corruption or congestion, SCTP must assume the packet loss was due to network congestion. Packet loss due to corruption can cause SCTP to reduce the amount of data that can be injected into the network. While performance of a transport protocol is not the only consideration when constructing a network containing satellite channels, SCTP congestion control algorithms have an unfavorable effect on performance and channel utilization.

SCTP employs congestion control algorithms to adjust the amount of unacknowledged data that can be injected into the network and to retransmit segments dropped by the network. The SCTP congestion control algorithms respond to packet loss as an indication of network congestion. Packet loss detected by SCTP congestion control algorithms can put the sender in slow-start with a reduced congestion window, thereby limiting the amount of data that can be transmitted. The slow-start algorithm will force the sender to wait for an acknowledgment before transmitting new data. The slow-start and congestion control algorithms can force poor utilization of the available channel bandwidth when using long delay networks.

SCTP congestion control uses two state variables to accomplish congestion control. The first variable is the congestion window (cwnd). The congestion window is an upper bound on the amount of data the sender can inject into the network before receiving an acknowledgment. The second variable is the slow-start threshold (ssthresh). The slow-start threshold variable determines which algorithm is used to increase cwnd. If cwnd is less than or equal to ssthresh, the slow-start algorithm is used to increase cwnd. If cwnd is greater than ssthresh the congestion avoidance algorithm is used to increase cwnd. There are two methods of packet loss detection (interpreted as congestion notification by the SCTP congestion controls) defined in SCTP:

- Timeout of the retransmission timer. The congestion control algorithms resets the congestion control state variables cwnd and ssthresh. The setting of the congestion control state variables have the effect of putting the sender in slow-start and assure that no more than one packet is outstanding until it receives an acknowledgment.

```
ssthresh = max (cwnd/2, 2*MTU)
cwnd    = 1*MTU
```


- Detection of gaps in received Transmission Sequence Numbers (TSNs) through Gap Ack reports in a Selective Acknowledgment (SACK). Normally a sender will wait four consecutive Gap Ack reports before reacting to the indication of packet loss. The congestion control algorithms reset the congestion control state variables cwnd and ssthresh as a result of detecting the packet loss. The setting of the congestion control variables will put the sender in slow-start with a reduced cwnd effectively limiting the amount of data the sender can transmit.

```
ssthresh = max(cwnd/2, 2*MTU)
cwnd = ssthresh
```

The SCTP congestion control algorithms generally respond unfavorably in networks that have large delays, a large delay-times-bandwidth product, and high bit-error rates. SCTP congestion control on the ITP has been enhanced to address the characteristics of satellite channels that contribute to low channel utilization of SCTP. SCTP on the ITP provides for the provisioning of four SCTP parameters that change how the SCTP congestion control algorithms responds to packet loss on satellite channels. The configuration of these parameters are shown in the [“Tuning SCTP on Satellite Channels” section on page 411](#).



Caution

The behavior of the SCTP congestion control algorithms is not compliant with RFC 2960 or RFC 4960 when this command is changed to values other than the default. This command should not be changed without a thorough understanding of SCTP congestion control algorithms.

Tuning SCTP on Satellite Channels

Before you can modify the SCTP parameters, you must create a basic ITP configuration, which is described fully in the “Configuring ITP Basic Functionality” chapter. If you are unfamiliar with ITP basic configuration, you are advised to refer to that chapter for more details before continuing.

The following SCTP parameters can be provisioned to change how SCTP congestion control responds to packet loss on satellite channels:

init-timeout

The init-timeout SCTP parameter controls the retransmission of SCTP association setup messages. The init-timeout is how long a SCTP endpoint will wait for a response to a setup message before retransmitting. The init-timeout parameter should be adjusted to for the expected round trip delays expected on the satellite channel.

retransmit-timeout

The retransmission timeout (RTO) should be adjusted for round-trip delays. Round-trip times for some satellite channels can range from 250 ms to 500 ms. Preferably, the retransmission timeout should be greater than the round-trip delay between nodes.

init-cwnd-size

The parameter init-cwnd-size specifies the initial window size used by the sender. If this parameter is provisioned, the window-size specified must match the receive-window size of the remote end of the SCTP association. Failure to match the init-cwnd-size to the remote receive-window will cause non deterministic congestion control behavior. This parameter should be used to overcome slow-start on satellite channels where large burst of sustainable traffic is present. Note the total sizes of the init-cwnd-size and receive-window sizes for all the SCTP associations should not exceed the amount of free memory available.

idle-cwnd-rate

When the endpoint does not transmit data on a given transport address, the congestion window of that transport address is decreased to $\max(\text{cwnd}/2, 2 * \text{MTU})$ per retransmission timeout. The `idle-cwnd-rate` allows the administrator to control the rate at which the congestion window is decreased due to being idle. Using the `idle-cwnd-rate`, the congestion window is decreased to $\max(\text{cwnd}/\text{idle-cwnd-rate}, \text{init-cwnd-size})$ per retransmission timeout.

fast-cwnd-rate

Normally a SCTP sender will wait four consecutive Gap Ack reports that indicates a missing packet before reacting to the indication of packet loss. On the fourth consecutive Gap Ack report, the SCTP congestion control algorithm decreases the slow-start threshold to $\max(\text{cwnd}/2, 2 * \text{MTU})$ and reduces the congestion window equal to the slow-start threshold. The setting of the congestion control variables as described will put the sender in slow-start with a reduced cwnd effectively limiting the amount of data the sender can transmit. The `fast-cwnd-rate` parameter allows the administrator to control the rate at which the congestion window is decreased. Using the `fast-cwnd-rate` parameter the slow-start threshold variable is set to $\max(\text{cwnd}/\text{fast-cwnd-rate}, 2 * \text{MTU})$. The congestion window variable is set to equal to the slow-start threshold as described previously. The sender is still put in slow-start, but depending on the value of the `fast-cwnd-rate` parameter the congestion window will be reduced conservatively or aggressively. Using the `fast-cwnd-rate`, we can effectively control how the congestion control algorithm responds to packet loss on satellite channels.

retransmit-cwnd-rate

When a retransmission timer timeout occurs, SCTP congestion control sets slow-start threshold to $\max(\text{cwnd}/2, 2 * \text{MTU})$ and reduces the congestion window to $1 * \text{MTU}$. This has the effect of putting the sender in slow-start and assure that no more than one packet is outstanding until it receives an acknowledgment. The `retransmit-cwnd-rate` parameter allows the administrator to control the rate at which the slow-start threshold is reduced and provides for the setting of the congestion window. Using the `retransmit-cwnd-rate` parameter the slow-start threshold variable is set to $\max(\text{cwnd}/\text{retransmit-cwnd-rate}, 2 * \text{MTU})$. The congestion window variable can be set using one of two methods. The first option for setting the congestion window variable sets the congestion window to its default of $1 * \text{MTU}$. The second option for setting the congestion window variable sets the congestion window equal to the slow-start threshold. Setting the congestion window equal to the slow-start threshold variable follows the same procedure for setting the congestion window variable as done for a fast-retransmit. The second option for setting the congestion window allows the congestion control algorithm to respond evenly to packet loss detected by either retransmission timer timeouts or fast-retransmits.

To specify SCTP parameters for satellite channels, use the following commands in CS7 Linkset submode:

Command	Purpose
Router(config-cs7-ls-link)# fast-cwnd-rate percent	Specifies the rate at which the size of the SCTP congestion window will be decreased due to fast transmission. The range is 0 to 100 percent. The default is 50 percent.
Router(config-cs7-ls-link)# idle-cwnd-rate percent	Specifies the rate at which the size of the SCTP congestion window will be decreased due to the association being idle. The Range is 0 to 100 percent. The default is 50 percent.
Router(config-cs7-ls-link)# init-cwnd-size bytes	Specifies the size of the SCTP initial congestion window. The range is 3000 to 20971520 bytes. The default is 2 times the smallest MTU of the SCTP interface, in bytes.

Command	Purpose
Router(config-cs7-ls-link)# init-timeout <i>msec</i>	Specifies how long a SCTP endpoint will wait for a response to a setup message before retransmitting. The init-timeout parameter should be adjusted for the round trip delays expected on the satellite channel. The range is 1000 to 60000 milliseconds. The default is 1000 milliseconds.
Router(config-cs7-ls-link)# retransmit-cwnd-rate <i>percent</i>	Specifies the rate at which the size of the SCTP congestion window will be decreased due to retransmission timer expiration. The range is 0 to 100 percent. The default is 50 percent.
Router(config-cs7-ls-link)# retransmit-timeout <i>rto-min rto-max</i>	Specifies the retransmission timeout value. The retransmission timeout (RTO) should be adjusted for round-trip delays. Round-trip times for some satellite channels range from 250 to 500 msec. The retransmission timeout should be greater than the round-trip delay between nodes. The range is 40 through 60000 milliseconds. The default is 1000 milliseconds.

Verifying SCTP Parameters on Satellite Channels

To verify the SCTP congestion control parameters, use the following command in EXEC mode:

Command	Purpose
Router# show cs7 m2pa sctp [parameters statistics] <i>ls-name</i> [<i>slc</i>]	Displays the current status and parameter values of a SCTP association.

The following is sample output from the **show cs7 m2pa** command using the **sctp** keyword:

```
Router#show cs7 m2pa sctp
** SCTP Association Parameters AssocID:0x00010002

AssocID:      0x00010002      Instance ID: 7      Offload: No
Assoc state: ESTABLISHED      Context:      2177134272      Uptime: 01:34:00.294
Local port: 9000
Local addresses: 172.18.44.162

Remote port: 9000
Primary dest addr: 172.18.44.170
Effective primary dest addr: 172.18.44.170
Destination addresses:

172.18.44.170      State: ACTIVE
Heartbeats:      Enabled      Timeout: 30000 ms
RTO/RTT/SRTT: 1000/0/154 ms      TOS:      0      MTU: 1500
cwnd:      3040      ssthresh: 64000      outstand: 0
Retrans cwnd rate: 50      Retrans cwnd mode: FastRetransmit
FastRetrans cwnd rate: 25      Idle dest cwnd rate: 50
Num retrans: 0      Max retrans: 4      Num times failed: 0
172.18.44.162 retrans: 0
```

```
Local vertag: 56773F4D Remote vertag: 4CCCC900
Num inbound streams: 2 outbound streams: 2
Max assoc retrans: 10 Max init retrans: 8 CumSack timeout: 200 ms Bundle timeout: 5 ms
enabled
Min RTO: 1000 ms Max RTO: 1000 ms
LocalRwnd: 64000 Low: 63951 RemoteRwnd: 64000 Low: 63988
Congest levels: 4 current level: 0 high mark: 2 chkSum: crc32
```



ITP Command Set: A - D

This section documents new or modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 Command Reference publication. Short Message Peer-to-Peer (SMPP) protocol is not supported. Some DSMR functionality is also not supported. It is recommended that commands pertaining to these features are not configured.

- [access-group, page 422](#)
- [access-list, page 423](#)
- [accounting \(cs7 as\), page 426](#)
- [addr \(cs7 mlr address-table\), page 427](#)
- [adjacent-sp-restart, page 429](#)
- [algorithm \(cs7 mlr result\), page 430](#)
- [algorithm \(cs7 sms group\), page 431](#)
- [allow-multi-message-dialogue \(cs7 mlr ruleset rule\), page 432](#)
- [ansi41 \(cs7 sms route-table\), page 434](#)
- [asname \(cs7 gtt application group\), page 435](#)
- [asname \(cs7 mlr result\), page 437](#)
- [asp, page 439](#)
- [assoc-retransmit \(cs7 asp\), page 441](#)
- [assoc-retransmit \(cs7 link\), page 442](#)
- [assoc-retransmit \(cs7 m2pa profile\), page 443](#)
- [assoc-retransmit \(cs7 m3ua\), page 444](#)
- [assoc-retransmit \(cs7 mated-sg\), page 445](#)
- [assoc-retransmit \(cs7 sgmp\), page 446](#)
- [assoc-retransmit \(cs7 sua\), page 447](#)
- [atm nni, page 448](#)
- [authorize, page 449](#)
- [bind-type \(cs7 sms profile parameters\), page 453](#)
- [bind-type \(cs7 sms session parameters\), page 454](#)
- [block, page 455](#)
- [broadcast, page 456](#)

- [bundling \(cs7 asp\), page 458](#)
- [bundling \(cs7 link\), page 459](#)
- [bundling \(cs7 m2pa profile\), page 461](#)
- [bundling \(cs7 m3ua\), page 463](#)
- [bundling \(cs7 mated-sg\), page 464](#)
- [bundling \(cs7 profile\), page 465](#)
- [bundling \(cs7 sgmp\), page 467](#)
- [bundling \(cs7 sua\), page 468](#)
- [burst-recovery-timeout, page 470](#)
- [cache-size, page 471](#)
- [cdpa \(cs7 mlr modify-profile\), page 472](#)
- [cdpa \(cs7 mlr trigger\), page 475](#)
- [cdpa \(cs7 pam\), page 478](#)
- [cgpa \(cs7 mlr modify-profile\), page 480](#)
- [cgpa \(cs7 mlr trigger\), page 483](#)
- [cgpa \(cs7 pam\), page 486](#)
- [clear cs7 accounting, page 488](#)
- [clear cs7 all, page 489](#)
- [clear cs7 as, page 490](#)
- [clear cs7 asp, page 491](#)
- [clear cs7 dynamic-route, page 492](#)
- [clear cs7 gtt-gta, page 493](#)
- [clear cs7 gtt-meas, page 494](#)
- [clear cs7 gws counters, page 495](#)
- [clear cs7 mated-sg statistics, page 496](#)
- [clear cs7 mlr-parse-error, page 497](#)
- [clear cs7 msu-rates, page 498](#)
- [clear cs7 mtp3 event-history, page 499](#)
- [clear cs7 pointcode event-history, page 500](#)
- [clear cs7 offload mtp3, page 501](#)
- [clear cs7 statistics, page 502](#)
- [clear cs7 tcap statistics, page 503](#)
- [clear ip sctp association, page 504](#)
- [c-link-linkset, page 505](#)
- [clock source \(interface\), page 507](#)
- [congestion-mode defer-to-backup \(cs7 mlr result\), page 509](#)
- [congestion-mode defer-to-backup \(cs7 sms group\), page 510](#)
- [cookie-life \(cs7 local peer\), page 511](#)

- [cookie-life \(cs7 m3ua\), page 513](#)
- [cookie-life \(cs7 sua\), page 515](#)
- [cs7 acc-audit-timer, page 517](#)
- [cs7 accounting, page 518](#)
- [cs7 address-table replace, page 520](#)
- [cs7 as, page 521](#)
- [cs7 asp, page 523](#)
- [cs7 audit, page 525](#)
- [cs7 billing account, page 526](#)
- [cs7 billing load, page 527](#)
- [cs7 billing options, page 528](#)
- [cs7 billing pc-table, page 529](#)
- [cs7 capability-pc, page 531](#)
- [cs7 cli, page 533](#)
- [cs7 dcs-group, page 536](#)
- [cs7 display-name, page 539](#)
- [cs7 distribute-sccp-sequenced, page 540](#)
- [cs7 distribute-sccp-unsequenced, page 541](#)
- [cs7 fast-restart, page 542](#)
- [cs7 fisu-audit-interval, page 543](#)
- [cs7 gtt address-conversion, page 544](#)
- [cs7 gtt application-group, page 545](#)
- [cs7 gtt concern-pclist, page 547](#)
- [cs7 gtt load, page 549](#)
- [cs7 gtt map, page 550](#)
- [cs7 gtt map sp, page 553](#)
- [cs7 gtt map ss, page 555](#)
- [cs7 gtt replace-db, page 557](#)
- [cs7 gtt selector, page 558](#)
- [cs7 gws action-set, page 560](#)
- [cs7 gws as, page 562](#)
- [cs7 gws replace, page 564](#)
- [cs7 gws-table replace, page 565](#)
- [cs7 gws load, page 566](#)
- [cs7 gws linkset, page 563](#)
- [cs7 gws table, page 567](#)
- [cs7 host, page 569](#)
- [cs7 ignore-sccp-pcconv, page 571](#)

- [cs7 large-msu-support, page 573](#)
- [cs7 linkset, page 574](#)
- [cs7 local-peer, page 576](#)
- [cs7 local-sccp-addr-ind, page 578](#)
- [cs7 log, page 580](#)
- [cs7 log checkpoint, page 582](#)
- [cs7 m3ua, page 583](#)
- [cs7 m3ua extended-upu, page 585](#)
- [cs7 mated-sg, page 586](#)
- [cs7 max-dynamic-routes, page 588](#)
- [cs7 mlr address-table, page 589](#)
- [cs7 mlr load, page 590](#)
- [cs7 mlr options, page 593](#)
- [cs7 mlr replace, page 594](#)
- [cs7 mlr result, page 595](#)
- [cs7 mlr ruleset, page 598](#)
- [cs7 mlr table, page 600](#)
- [cs7 msu-rates notification-interval, page 602](#)
- [cs7 msu-rates sample-interval, page 603](#)
- [cs7 msu-rates threshold-default, page 604](#)
- [cs7 msu-rates threshold-proc, page 606](#)
- [cs7 mtp3 crd, page 608](#)
- [cs7 mtp3 event-history, page 610](#)
- [cs7 mtp3 timer, page 612](#)
- [cs7 mtp3 tuning, page 617](#)
- [cs7 mtp3 tuning rx-congestion-threshold, page 618](#)
- [cs7 national-options, page 621](#)
- [cs7 network-indicator, page 623](#)
- [cs7 network-name, page 624](#)
- [cs7 nso, page 625](#)
- [cs7 offload mtp3, page 626](#)
- [cs7 offload mtp3 restart, page 627](#)
- [cs7 paklog, page 628](#)
- [cs7 pam, page 630](#)
- [cs7 pc-conversion, page 631](#)
- [cs7 pc-conversion default, page 633](#)
- [cs7 pmp, page 635](#)
- [cs7 pmp congestion-timer, page 637](#)

- [cs7 pmp hold-queue, page 638](#)
- [cs7 point-code delimiter, page 641](#)
- [cs7 point-code format, page 642](#)
- [cs7 profile, page 644](#)
- [cs7 prompt enhanced, page 646](#)
- [cs7 qos class, page 647](#)
- [cs7 rate-limit, page 649](#)
- [cs7 remote-congestion-msgs, page 651](#)
- [cs7 route-mgmt-sls, page 652](#)
- [cs7 route-table, page 654](#)
- [cs7 sami module, page 656](#)
- [cs7 save address-table, page 657](#)
- [cs7 save billing-cfg, page 658](#)
- [cs7 save gtt-table, page 659](#)
- [cs7 save gws, page 660](#)
- [cs7 save gws-table, page 661](#)
- [cs7 save log, page 662](#)
- [cs7 save mlr, page 664](#)
- [cs7 save route-table, page 665](#)
- [cs7 sccp-allow-pak-conv, page 666](#)
- [cs7 sccp-class1-loadshare, page 667](#)
- [cs7 sccp-class1-wrr, page 669](#)
- [cs7 sccp gti-conversion, page 670](#)
- [cs7 sccp instance-conversion, page 671](#)
- [cs7 sccp ssn-conversion, page 673](#)
- [cs7 sctp crc-type, page 675](#)
- [cs7 secondary-pc, page 676](#)
- [cs7 sg-event-history, page 678](#)
- [cs7 sgmp, page 679](#)
- [cs7 sls-shift, page 681](#)
- [cs7 sms ansi41, page 682](#)
- [cs7 sms gsm-map, page 684](#)
- [cs7 sms ruleset, page 686](#)
- [cs7 snmp dest-max-window, page 688](#)
- [cs7 snmp mgmt-max-window, page 690](#)
- [cs7 sua, page 691](#)
- [cs7 sua-allow-xudt-request, page 693](#)
- [cs7 summary-routing-exception, page 694](#)

- [cs7 tcap tid-timer](#), page 695
- [cs7 tcap variant](#), page 696
- [cs7 tfc-pacing-ratio](#), page 697
- [cs7 uninhibit](#), page 698
- [cs7 upgrade analysis](#), page 699
- [cs7 upgrade module](#), page 701
- [cs7 util-abate](#), page 702
- [cs7 util-plan-capacity](#), page 703
- [cs7 util-sample-interval](#), page 704
- [cs7 util-threshold](#), page 705
- [cs7 variant](#), page 706
- [cs7 xua-as-based-congestion](#), page 708
- [cs7 xua-daud-inactive](#), page 709
- [cs7 xua-err-diag-fmt](#), page 710
- [cs7 xua-errorHandling](#), page 711
- [cs7 xua-ssnm-filtering](#), page 713
- [cs7 xua-tfc-allowed](#), page 714
- [cumulative-sack \(cs7 asp\)](#), page 715
- [cumulative-sack \(cs7 link\)](#), page 716
- [cumulative-sack \(cs7 m2pa profile\)](#), page 717
- [cumulative-sack \(cs7 m3ua\)](#), page 718
- [cumulative-sack \(cs7 mated-sg\)](#), page 719
- [cumulative-sack \(cs7 sgmp\)](#), page 720
- [cumulative-sack \(cs7 sua\)](#), page 721
- [cdcs](#), page 722
- [cdcs](#), page 722
- [dcs-group](#), page 724
- [default result](#), page 728
- [description \(cs7 link\)](#), page 729
- [description \(cs7 linkset\)](#), page 730
- [dest-port \(cs7 mlr ruleset rule\)](#), page 731
- [dest-sme \(cs7 mlr ruleset rule\)](#), page 732
- [dest-sme \(cs7 mlr ruleset rule\)](#), page 732
- [dest-sme \(cs7 sms set rule\)](#), page 735
- [dest-sme-table \(cs7 mlr ruleset rule\)](#), page 737
- [dest-sme-table \(cs7 sms set rule\)](#), page 739
- [dest-smsc \(cs7 mlr ruleset rule\)](#), page 742
- [dest-smsc \(cs7 sms set rule\)](#), page 744

- [digits](#), page 746
- [display-name \(cs7 link\)](#), page 748
- [display-name \(cs7 linkset\)](#), page 749
- [distribute-sccp-sequenced-negate](#), page 750
- [dpc](#), page 752

access-group

To enable Cisco ITP gateway screening on a linkset, use the `access-group cs7 linkset` submode command. To disable access lists on the linkset, use the `no` form of this command.

access-group { **2700-2999** | *name* } [**in** | **out**]

no access-group { **2700-2999** | *name* } [**in** | **out**]

Syntax Description	2700-2999	Number of an access list.
	<i>name</i>	Name of an access list.
	in	Applies this access list to inbound packets.
	out	Applies this access list to outbound packets.

Defaults None.

Command Modes `cs7 linkset` submode

Command History

Usage Guidelines The **access-group** command assigns an ITP access list to a linkset to screen either inbound or outbound packets.

Examples The following example shows how to assign access list 2700 to filter inbound packets:

```
access-list 2700 permit dpc 4.100.0 0.0.255
.
.
cs7 linkset michael 10.1.1
  access-group 2700 in
```

Related Commands	Command	Description
	access-list	Defines an access list.
	show cs7 access-lists	Displays information about defined ITP access lists.

access-list

To define a Cisco ITP access list, use the **access-list** command in global configuration mode. To remove a Cisco SS7 access list, use the **no** form of this command.

```
access-list access-list-number [instance instance-number] [compiled] [dynamic-extended]
[rate-limit precedence | mask precedence-bitmask] {deny | permit} [dpc point-code
wildcard-mask | opc point-code wildcard-mask | si {0-15} | pattern offset hex-pattern | aftpc
point-code ss-number wildcard-mask ss-number-mask | cdpa point-code ss-number
wildcard-mask ss-number-mask | cgpa point-code ss-number wildcard-mask ss-number-mask |
```

```
selector | all] [remark line]
```

no access-list *access-list-number*

Syntax Description

<i>access-list-number</i>	Number of an access list. The Cisco SS7 access list range is a decimal number from 2700 to 2999. The other access list ranges are: 1–99 IP standard access list 100– 999 IP extended access list 1100–1199 Extended 48-bit MAC address access list 1300–1999 IP standard access list (expanded range) 200–299 Protocol type-code access list 2000–2699 IP extended access list (expanded range) 700–799 48-bit MAC address access list
instance	Indicates the specific instance, if the Multiple Instances feature is enabled.
<i>instance-number</i>	Instance number.
compiled	Enables IP access-list compilation.
dynamic-extended	Extends the dynamic ACL.
rate-limit	Simple rate-limit access list.
<i>precedence</i>	Precedence. Valid range is 0 to 7.
mask	Uses a precedence bitmask.
<i>precedence-bitmask</i>	Precedence bitmask. Valid range is 0 to FF.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
dpc	Applies the access list to the destination point code.
<i>point-code</i>	Point code to which the packet is being sent.
<i>wildcard-mask</i>	Specifies which bits of the point code to ignore for matching.
opc	Applies the access list to the origination point code.
<i>point-code</i>	Point code from which the packet is being sent.
<i>wildcard-mask</i>	Wildcard bits to be applied to the origination point code.
si	Service indicator.
<i>si-value</i>	Service indicator value. Range is 0 to 15.
pattern	Uses pattern matching to determine access.
<i>offset</i>	Decimal number indicating the number of bytes into the packet where the byte comparison should begin.
<i>hex-pattern</i>	Hexadecimal string of digits representing a byte pattern.

aftpc	Applies the access list to the affected point code and SSN in SCCP management messages.
<i>point-code</i>	Affected point code in the SCCP management message.
<i>ss-number</i>	Subsystem number at the affected point code.
<i>wildcard-mask</i>	Specifies which bits of the point code to ignore for matching.
<i>ss-number-mask</i>	Specifies which bits of the subsystem number to ignore for matching.
cdpa	Applies the access list to the called party address point code and SSN in SCCP messages.
<i>point-code</i>	Called party point code in the SCCP message.
<i>ss-number</i>	Subsystem number at the point code.
<i>wildcard-mask</i>	Specifies which bits of the point code to ignore for matching.
<i>ss-number-mask</i>	Specifies which bits of the subsystem number to ignore for matching.
cgpa	Applies the access list to the calling party point code and SSN in SCCP messages.
<i>point-code</i>	Calling party point code in the SCCP management message.
<i>ss-number</i>	Subsystem number at the point code.
<i>wildcard-mask</i>	Specifies which bits of the point code to ignore for matching.
<i>ss-number-mask</i>	Specifies which bits of the subsystem number to ignore for matching.
selector	Called party (gti tt np nai).
all	Permits or denies all (other) packets.
remark line	Includes a remark.

Defaults

Any message that does not match any of the access-list entries is, by default, denied.

Command Modes

Global configuration

Command History**Usage Guidelines**

The **access-list** command defines the access list. After defining the access list, you use the **access-group** command to apply the access list to a linkset.

SCCP screening screens MSUs on inbound and outbound linksets.

If the access list is inbound, when the ITP receives a packet it checks the access list criteria statements for a match. If the packet is permitted, the ITP continues to process the packet. If the packet is denied, the ITP discards it.

If the access list is outbound, after receiving and routing a packet to the outbound interface the ITP checks the access list criteria statements for a match. If the packet is permitted, the ITP transmits the packet. If the packet is denied, the ITP discards it.

The **selector** and **cgpa** keywords enable screening on the inbound linkset.

The **aftpc** and **cdpa** keywords enable screening on the outbound linkset.

Examples

The following example shows how to define an access list for the ITP:

```
access list 2700 permit dpc 4.100.0 0.0.255
!  
!  
cs7 linkset tony 4.100.2  
  access-group 2700 out  
!
```

The following example shows how to drop all SCCP management packets with affected point code 7.5.4 and SSN 10 but permit all the rest:

```
access-list 2710 deny aftp 7.5.4 10  
access-list 2710 permit all  
  
cs7 linkset tony 4.100.2  
  access-group 2710 in
```

Related Commands

Command	Description
access-group	Assigns an ITP access list to a linkset.
cs7 paklog	Configures the ITP Packet Logging facility.
show cs7 access-lists	Displays information about defined ITP access lists.

accounting (cs7 as)

To enable accounting for M3UA payload data and SUA CLDT/CLDR packets, use the **accounting cs7 as** submode command.

If the command is issued for an M3UA AS, normal M3UA accounting is enabled. For each OPC+DPC+SI combination, normal M3UA accounting tracks the number of M3UA payload data messages sent and received.

If the command is issued for an SUA AS, normal SUA accounting is enabled. SUA normal accounting tracks the number of SUA CLDT/CLDR packets received from and sent to the AS.

To disable accounting, use the **no** form of this command.

accounting

no accounting

Syntax Description This command has no arguments or keywords.

Defaults Accounting is not enabled.

Command Modes cs7 as submode

Command History	Release	Modification
	12.2(18)IXF	This command was introduced.
	12.4(15)SW1	
	12.2(33)IRA	

Usage Guidelines Because accounting is enabled by default, only the **no** form of the command displays as output from the **show configuration** command.

Examples The following example shows how to enable accounting on the AS named as1:

```
cs7 as as1
gtt-accounting
```

Related Commands	Command	Description
	clear cs7 accounting	Clears the ITP accounting databases.
	cs7 as	Enters cs7 as submode.

addr (cs7 mlr address-table)

To specify an MLR address within the MLR address table, use the **addr** command in cs7 mlr address-table configuration mode. To remove the definition, use the **no** form of this command.

```
addr address-name [exact] [result {asname as-name | block | continue | group group-name | gt
addr-string [tt tt gti {2 | 4 np np nai nai}}] | [instance instance-number] pc pc [ssn ssn] |
[sccp-error error]]
```

```
no addr address-name [exact] [result {asname as-name | block | continue | group group-name | gt
addr-string [tt tt gti {2 | 4 np np nai nai}}] | [instance instance-number] pc pc [ssn ssn] |
[sccp-error error]]
```

Syntax Description

<i>address-name</i>	Address of 1 to 20 hexadecimal digits.
exact	(Optional) Configured address must match address exactly.
result	(Optional) Configures result.
asname	(Optional) Routes message to an AS.
<i>as-name</i>	AS name.
block	(Optional) Drops message.
continue	(Message) Continues message processing.
group	(Optional) Routes messages using an MLR or SMS result group.
<i>group-name</i>	Group name.
gt	(Optional) Routes message using the SCCP global title. The specified address is placed in the SCCP Called Party Address (CdPA), the routing indicator (RI) is changed to RI=GT, and then the message is routed based on the locally provisioned global title translation table.
<i>addr-string</i>	Address string of 1 to 5 hexadecimal characters. The string is input in normal form, not in BCD-string format.
tt	Specifies a translation type.
<i>tt</i>	Translation type. In the Called Party field of the GTT message, the SSP sets the TT to indicate which GTT table the STP should use. The TT is a 1-byte field that usually maps to a specific service. Valid numbers range from 0 to 255.
gti	(Optional) Specifies a global title indicator. (Used only when the cs7 variant command specifies ITU or China.)
<i>gti</i>	Global title indicator. Valid numbers are 2 (primarily used in the ANSI domain) or 4 (used in the ITU domain).
np	(Optional) Specifies a numbering plan. (Used only when <i>gti</i> is 4.)
<i>np</i>	Numbering plan value. Valid range is 0 to 15.
nai	(Optional) Specifies a nature of address indicator. (Used only when <i>gti</i> is 4.)
<i>nai</i>	(Optional) Nature of address indicator. Valid range is 0 to 127.
instance	(Optional) Indicates the PC/PCSSN result in a local or other instance.
<i>instance-number</i>	(Optional) Instance number. The valid range is 0 to 7. The default instance is 0.
pc	(Optional) Routes point code message using PC.

■ **addr (cs7 mlr address-table)**

<i>pc</i>	Destination point code used to route message.
ssn	(Optional) Specifies a subsystem number.
<i>ssn</i>	Subsystem number. Valid range is 2 to 255.
sccp-error <i>error</i>	Configures block results and supports configuring an sccp-error on the block result.

Defaults

None.

Command Modes

cs7 mlr address-table configuration

Command History

Release	Modification
12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.
12.2(18)IXG 12.4(15)SW2 12.2(33)IRB	The instance keyword was added.

Examples

The following example shows how to specify an MLR address table named TABLE1 with an MLR address of 24. The configured address must match exactly, and the result group is SMSC-GROUP1.

```
cs7 mlr address-table TABLE1
  addr 24 exact result group SMSC-GROUP1
```

The following example shows how to specify an MLR address table named TABLE1 with the result configured for a GT address:

```
cs7 instance 0 mlr address-table TABLE1
  addr 123456 result gt 8282 tt 11 gti 2
  addr 12345 result gt 4545 tt 10 gti 4 np 2 nai 1
  addr 1234
  addr 180002 exact
```

The following example shows how to configure 1 as the instance in the **addr** command:

```
cs7 instance 0 mlr address-table test
  addr 133 result instance 1 pc 3.3.3 ssn 8
```

Related Commands

Command	Description
cs7 mlr address-table	Defines a table of addresses to be used when searching with the previously specified routing parameter.
show cs7 mlr address-table	Displays the addresses matched within the MLR address table.

adjacent-sp-restart

To indicate that the adjacent ITP node supports the adjacent-sp-restart process, use the **adjacent-sp-restart** cs7 linkset submode command. To remove the configuration, use the **no** form of this command.

adjacent-sp-restart

no adjacent-sp-restart

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Command Modes	cs7 linkset submode

Command History

Examples	The following example shows how to enable the adjacent-sp-restart process for the adjacent ITP node:

```
cs7 linkset to_doc 10.1.1
  adjacent-sp-restart
```

Related Commands	Command	Description
	show cs7 linkset detailed	Displays ITP linkset details.

algorithm (cs7 mlr result)

To specify the order of the coefficients used to calculate the dest-sme hash value, where **a** represents the last MSISDN digit, use the **algorithm** command in cs7 mlr result configuration mode. To remove the definition, use the **no** form of this command.

algorithm [abcd | dcba]

no algorithm [abcd | dcba]

Syntax Description

abcd	Order of the coefficients used to calculate the dest-sme hash value, where a represents the last MSISDN digit. (This algorithm is the default.)
dcba	Changes the order of the coefficients used to calculate the dest-sme hash value from the default of abcd to dcba.

Defaults

The default algorithm is **abcd**.

Command Modes

cs7 mlr result configuration

Command History

Release	Modification
12.2(25)SW12	This command was introduced.
12.2(18)IXF	
12.4(15)SW1	

Usage Guidelines

The **algorithm** command requires the **dest-sme-binding** keyword when you use the **cs7 mlr result** command, which enters cs7 mlr result configuration mode. Dest-sme-binding result groups default to the abcd algorithm.

Examples

The following example shows output from the **algorithm abcd** command:

```
Router# show cs7 mlr result MLR_BIND
Result Group: MLR_BIND      Instance: 0  Unavailable-routing: discard
Protocol: gsm-map           Mode: dest-sme-binding
                             Algorithm: dcba
```

Order	Result Type	Stat	Weight	Matches
10	PC 4.5.4	unav	1	0

Related Commands

Command	Description
cs7 mlr result	Enables cs7 mlr result configuration mode.

algorithm (cs7 sms group)

To specify the order of the coefficients used to calculate the dest-sme hash value, where **a** represents the last MSISDN digit, use the **algorithm** command in cs7 sms group configuration mode. To remove the definition, use the **no** form of this command.

algorithm [abcd | dcba]

no algorithm [abcd | dcba]

Syntax Description	abcd	Order of the coefficients used to calculate the dest-sme hash value, where a represents the last MSISDN digit. (This algorithm is the default.)
	dcba	Changes the order of the coefficients used to calculate the dest-sme hash value from the default of abcd to dcba.

Defaults The default algorithm is **abcd**.

Command Modes cs7 sms group configuration

Command History

Usage Guidelines The **algorithm** command requires the **dest-sme-binding** keyword when you use the **cs7 sms group** command, which enters cs7 sms group mode. Dest-sme-binding result groups default to the abcd algorithm.

Examples The following example shows output from the **algorithm abcd** command:

```
router# show cs7 sms group SMS_BIND
Instance: 0 Group: SMS_BIND          Type: smsc
Protocol: gsm-map                    Mode: dest-sme-binding
                                      Algorithm: abcd
```

Order	Result	Type	Stat	Weight	Matches
10	PC 4.3.2		unav	10	0
20	PC 4.3.3		unav	20	0
30	PC 5.3.2		unav	30	0

Related Commands	Command	Description
	cs7 sms group	Enables cs7 sms group configuration mode.

allow-multi-message-dialogue (cs7 mlr ruleset rule)

To match segmented TCAP short messages, short messages that have the More-Messages-To-Send indicator set, and short messages concatenated at the SMS layer, use the **allow-multi-message-dialogue** command in cs7 mlr ruleset rule configuration mode. To remove the specification, use the **no** form of this command.

allow-multi-message-dialogue

no allow-multi-message-dialogue

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Command Modes	cs7 mlr ruleset rule configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	If the allow-multi-message-dialogue command is configured, no other routing parameters can be configured within cs7 mlr ruleset rule configuration mode.

Unlike other routing commands, this command is valid in a rule defined with the **all** keyword.

The **allow-multi-message-dialogue** command is allowed for sms-mo and sms-mt operations. If specified, the following messages will match this operation:

- Empty BEGIN messages
- CONTINUE messages
- BEGIN and CONTINUE messages containing an INVOKE component with the More-Messages-to-Send indicator (sms-mt only)
- Concatenated messages

Examples	The following example shows how to use the allow-multi-message-dialogue command:

```
cs7 mlr ruleset ruleset1
rule 10 gsm-map sms-mt
  allow-multi-message-dialogue
result group SMS1
```

Related Commands	Command	Description
	rule (cs7 mlr ruleset)	Specifies the rules for a routing trigger within a multilayer ruleset table.

ansi41 (cs7 sms route-table)

To configure the routing information for received ANSI-41 messages, use the **ansi41** command in cs7 sms route-table configuration mode. To remove the definition, use the **no** form of this command.

ansi41 *operation-name*

no ansi41 *operation-name*

Syntax Description

<i>operation-name</i>	Specifies the operation: • smsNot identifies the input operation as the ANSI-41 SMS Notification operation.

Defaults

None.

Command Modes

cs7 sms route-table configuration

Command History

Usage Guidelines

The **ansi41** command with the **smsNot** keyword enables cs7 sms ansi41 smsnot configuration mode.

Examples

The following example shows how to configure SMS Notification proxy. The configuration specifies the input protocol as the ANSI-41 MAP layer and identifies the input operation as the ANSI-41 SMS Notification.

```
cs7 sms route-table
ansi41 smsNot
ruleset SMS-PROXY
```

Related Commands

Command	Description
cs7 sms route-table	Configures the SMS route table.

asname (cs7 gtt application group)

To assign an M3UA or SUA AS directly to a global title, use the **asname** command in cs7 gtt application group submode. To remove the configuration, use the **no** form of this command.

```
[instance instance-number] asname as-name { cost [ssn ssn] { gt [ntt ntt] | pcssn } [rate-limit rate] | wf
[ssn ssn] { gt [ntt ntt] | pcssn } } [sccp-allow-pak-conv number]
```

```
no [instance instance-number] asname as-name
```

Syntax Description

<i>as-name</i>	Application server name. You can assign a global title translation to an M3UA or SUA AS instead of to a point code and SSN. This argument also allows the administrator to have flexibility in assigning backup point codes and alternate AS names to handle a specific service.
<i>cost</i>	Index value (1 to 64) specifying the priority of PC (PC/SSN) within the application group.
ssn	Sets the subsystem number during the translation process.
<i>ssn</i>	Subsystem number.
gt	Sets RI to route on GT.
ntt	Configures a new translation type value to be set within the called party address global title selector data. The keyword is valid only when the gt keyword is specified.
<i>ntt</i>	New translation type value in the range of 0 to 255.
pcssn	Sets RI to route on point code and subsystem number.
rate-limit	Specifies the traffic-rate limitation to this PC/SSN. The over-flow traffic routes to higher cost DPC/ASNAME. If not specified, the PC does not have a rate-limit.
<i>rate</i>	An integrate value specifying the traffic rate. Valid range is 1 to 4294967296 MSU/sec.
<i>wf</i>	Weight factor. Any items added to the group require a cost if the multiplicity command specifies cgpa or wrr .
sccp-allow-pak-conv	Enables conversion of SCCP packet between XUDT/XUDTS and UDT/UDTS.
<i>number</i>	1 specifies XUDT/XUDTS to UDT/UDTS conversion 2 specifies UDT/UDTS to XUDT/XUDTS conversion 3 specifies NO CONVERSION

Defaults

None.

Command Modes

cs7 gtt application group submode

Command History

Release	Modification
12.4(15)SW9 12.2(33)IRI	The sccp-allow-pak-conv keyword was added.
12.2(33)IRA	The command was introduced.
12.2(33)IRD	The rate limit keyword and <i>rate</i> argument were introduced.
12.2(33)IRD	Noted that command requires a cost if the multiplicity command specifies wrr

Usage Guidelines

The **asname** command assigns an M3UA or SUA AS directly to a global title. You must configure a **cs7 as** command with the same name, and a **routing-key** subcommand of type **gtt** must be configured. Verification of the AS name is performed at execution time.

The destination in a GTT application group uses the *wf* argument when the **multiplicity** command was configured with the **cgpa** or **wrr** keyword.

Examples

The following example shows how to configure two AS names. AS1 has a cost value of four and RI set to route on GT. AS2 has a cost value of five and the RI set to route on point code and subsystem number.

```
cs7 gtt application-group abc
multiplicity cost
pc 7.7.1 3 gt
asname as1 4 gt
asname as2 5 pcssn
```

Related Commands

Command	Description
cs7 gtt application-group	Defines a GTT application group.
multiplicity	Specifies a method for selecting a destination in the application group.

asname (cs7 mlr result)

To specify a particular destination M3UA or SUA application server, use the **asname** command in cs7 mlr result configuration mode. To remove the definition, use the **no** form of this command.

asname *as-name* [**order** *order*] [**weight** *weight*][**preserve-dpc**]

no asname *as-name* [**order** *order*] [**weight** *weight*][**preserve-dpc**]

Syntax Description		
<i>as-name</i>		Identifies an M3UA or SUA application server name. The name can be 1 to 12 characters long.
order		Specifies the order in which the results are stored in the result group. Required for (and only present in the CLI for) results in a dest-sme-binding mode. Results in a WRR result group are not able to configure an order keyword.
<i>order</i>		An integer value ranging from 1 to 1000.
weight		Specifies the weight applied to the weighted round-robin (WRR) distribution algorithm used for MLR result groups.
<i>weight</i>		For dest-sme-binding mode, an integer value in the range 1 to 2147483647. The weight value should reflect the relative capacity of the result (smc). This value is used by the dynamic B-address routing algorithm to select a deterministic result (SMSC) based on the message B-address. If not configured, the default <i>weight</i> value is 1. For WRR mode, an integer value in the range of 0 to 10. A value of 10 indicates the resource should be selected 10 times more than a resource assigned a weight of 1. A weight of 0 indicates that the resource should only be used in the event that all nonzero-weighted resources are unavailable. If multiple zero-weighted resources exist, then messages are equally distributed between them if all nonzero-weighted resources fail. If not specified, a default weight of 1 is used.
preserve-dpc		Instructs MLR not to alter the DPC when routing the message to the specified M3UA AS name. If the AS name is an SUA AS, then the keyword is ignored. If the message must be routed to the AS using MTP3 C-link backup routing, then the keyword is ignored.

Defaults The default weight is 1.

Command Modes cs7 mlr result configuration

Command History

Usage Guidelines If multiple zero-weighted resources exist, then messages are equally distributed between them if all nonzero-weighted resources fail. If not specified, a default weight of 1 is used.

This result type is not currently supported by DSMR (SMS MO Proxy).

When using the **preserve-dpc** keyword, M3UA ASPs must support receiving messages that indicate a DPC different from the one configured under the routing-key definition within the associated M3UA AS submode.

The original DPC is not preserved when messages are routed over an MTP3 C-link used for M3UA/SUA backup routing. When routing these messages, the DPC is always set to the defined AS point code.

Examples

The following example shows how to specify a destination application server resource in the result group SMS-WEIGHTED. The application server, SMS_AS1, is assigned a weighted round-robin (WRR) value of 10.

```
cs7 mlr result SMS-WEIGHTED
  asname SMS_AS1 weight 10
```

The following example shows how to specify a destination application server resource in the result group SMS-BINDING. The application server, SMS_AS1, is assigned a weight value of 10 and an order of 1.

```
cs7 mlr result SMS-BINDING
  asname SMS_AS1 order 1 weight 10
```

Related Commands

Command	Description
cs7 mlr result	Specifies the name of the MLR results group. The result group contains the list of resources that process traffic to be routed based on multilayer information.

asp

To list the ASPs contained in the AS, use the **asp** command in **cs7** as configuration mode. To remove the ASP from the AS definition, use the **no** form of this command.

asp *asp-name* [**weight** *weight*]

no asp *asp-name* [**weight** *weight*]

Syntax Description

<i>asp-name</i>	ASP name. The name may be up to 12 characters long, and the first character must be alphabetic. The name must not match any reserved keyword (such as m3ua , sua , all , operational , active , statistics , bindings , or detail).
weight	Specifies the weighted round-robin ASP distribution within an AS.
<i>weight</i>	Weight assigned to the ASP. Valid range is 0 to 10. The default weight is 1.

Defaults

The default weight is 1.

Command Modes

cs7 as configuration

Command History

Usage Guidelines

You can associate multiple ASPs to an AS by specifying multiple **asp** commands. The number of ASPs associated with an AS should not exceed 16.

The ASP name must already be defined using the **cs7 asp** command before it can be associated with an AS.

The **no** form of the command deletes this ASP from the AS definition and inactivates the routing context for this ASP by generating a Notify message with this routing context.

You can assign a weight value in the range 0 to 10 to an ASP. A higher weight indicates a higher priority (similar to MLR weighted round-robin operation). If **weight** is not specified, the ASP has a default weight of 1.

In an override or broadcast AS, the **weight** keyword is unused. In a loadshare AS, an ASP of weight 0 receives packets only if all other ASPs in the AS are inactive or congested. If multiple active ASPs have a weight of 0, and no other active and uncongested ASPs are available, packets are evenly distributed to the ASPs of weight 0.

Examples

The following example shows how to define an M3UA application server named AS1 with a routing key of 01010101 and a destination point code of 3.3.3. AS1 contains two ASPs named ASP1 and ASP2.

```
cs7 as as1 m3ua
  routing-key 01010101 3.3.3
  asp asp1
  asp asp2
```

Related Commands

Command	Description
cs7 as	Defines an application server.
cs7 asp	Defines an application server process.

assoc-retransmit (cs7 asp)

An association retransmits packets when the sender does not receive an acknowledgement within a specified time period. To configure the maximum number of consecutive retransmissions, use the **assoc-retransmit** command in cs7 asp configuration mode. To disable the configuration, use the **no** form of this command.

assoc-retransmit *max-retrans*

no assoc-retransmit *max-retrans*

Syntax Description	<i>max-retrans</i>	Maximum association retransmissions. Range is 2 to 20. The default is the value specified under the local M3UA or SUA instance.

Defaults	The default retransmission value is the value specified under the local M3UA or SUA instance.

Command Modes	cs7 asp configuration

Command History

Usage Guidelines	The assoc-retransmit counter includes retransmissions of association initialization packets and retransmissions to all the destination transport addresses of the peer if it is multihomed.

Examples	The following example shows how to set the maximum number of retransmissions to 20:

```
cs7 asp ASP1 2904 2905 m3ua
remote-ip 1.1.1.1
assoc-retransmit 20
```

Related Commands	Command	Description
	cs7 asp	Defines an application server process and enables cs7 asp submode.
	show cs7 asp detail	Displays ASP information.

assoc-retransmit (cs7 link)

An association retransmits packets when the sender does not receive an acknowledgement within a specified time period. To configure the maximum number of consecutive retransmissions to a peer before the peer is considered unreachable, use the **assoc-retransmit** command in cs7 link configuration mode. When the maximum number is exceeded all transmission is stopped and the association is closed. To disable the configuration, use the **no** form of this command.

assoc-retransmit *max-retrans*

no assoc-retransmit *max-retrans*

Syntax Description

<i>max-retrans</i>	Maximum association retransmissions. Range is 2 to 20.

Defaults

10 retransmissions

Command Modes

cs7 link configuration

Command History

Usage Guidelines

The assoc-retransmit counter includes retransmissions of association initialization packets and retransmissions to all the destination transport addresses of the peer if it is multihomed.

Examples

The following example shows how to set the maximum number of retransmissions to 20:

```
cs7 linkset michael 10.1.1
link 0 sctp 172.18.44.147 7000 7000
  assoc-retransmit 20
```

Related Commands

Command	Description
cs7 linkset	Specifies a linkset and enters cs7 linkset submode.
show cs7 m2pa	Displays ITP M2PA statistics.

assoc-retransmit (cs7 m2pa profile)

An association retransmits packets when the sender does not receive an acknowledgement within a specified time period. To configure the maximum number of consecutive retransmissions to a peer before the peer is considered unreachable, use the **assoc-retransmit** command in cs7 m2pa profile configuration mode. When the maximum number is exceeded all transmission is stopped and the association is closed. To disable the configuration, use the **no** form of this command.

assoc-retransmit *max-retrans*

no assoc-retransmit *max-retrans*

Syntax Description

<i>max-retrans</i>	Maximum association retransmissions. Range is 2 to 20.

Defaults

10 retransmissions

Command Modes

cs7 m2pa profile configuration

Command History

Usage Guidelines

The assoc-retransmit counter includes retransmissions of association initialization packets and retransmissions to all the destination transport addresses of the peer if it is multihomed.

Examples

The following example shows how to define a profile named m2parfc. The profile supports M2PA RFC, specifies the **assoc-retransmit** command, and applies to all the links in the linkset named to_nyc.

```
cs7 profile m2parfc
 m2pa
  assoc-retransmit
.
.
.
cs7 linkset to_nyc
 profile m2parfc
```

Related Commands

Command	Description
m2pa	Specifies M2PA parameters in a CS7 profile.

assoc-retransmit (cs7 m3ua)

An association retransmits packets when the sender does not receive an acknowledgement within a specified time period. To configure the maximum number of consecutive retransmissions to be allowed when a new SCTP association is started with the local port, use the **assoc-retransmit** command in **cs7 m3ua** configuration mode. When the maximum number is exceeded all transmission is stopped and the association is closed. To disable the configuration, use the **no** form of this command.

assoc-retransmit *max-retrans*

no assoc-retransmit *max-retrans*

Syntax Description	<i>max-retrans</i>	Maximum association retransmissions. Range is 2 to 20.

Defaults	10 retransmissions

Command Modes	cs7 m3ua configuration

Command History	

Usage Guidelines	The assoc-retransmit counter includes retransmissions of association initialization packets and retransmissions to all the destination transport addresses of the peer if it is multihomed.

Examples	The following example shows how to set the maximum number of retransmissions to 20: <pre>cs7 m3ua 2905 offload local-ip 4.4.4.4 assoc-retransmit 20</pre>

Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>cs7 m3ua</td><td>Specifies the local port number for M3UA and enters cs7 m3ua submode.</td></tr> <tr> <td>show cs7 m3ua</td><td>Displays M3UA node information.</td></tr> </table>	Command	Description	cs7 m3ua	Specifies the local port number for M3UA and enters cs7 m3ua submode.	show cs7 m3ua	Displays M3UA node information.
Command	Description						
cs7 m3ua	Specifies the local port number for M3UA and enters cs7 m3ua submode.						
show cs7 m3ua	Displays M3UA node information.						

assoc-retransmit (cs7 mated-sg)

An association retransmits packets when the sender does not receive an acknowledgement within a specified time period. To configure the maximum number of association retransmissions for the association, use the **assoc-retransmit** command in **cs7 mated-sg** configuration mode. To disable the configuration, use the **no** form of this command.

assoc-retransmit *max-retrans*

no assoc-retransmit *max-retrans*

Syntax Description	<i>max-retrans</i>	Maximum association retransmissions. Range is 2 to 20.

Defaults	The value of <i>max-retrans</i> defaults to the value specified under the local port instance.

Command Modes	cs7 mated-sg configuration

Command History

Usage Guidelines	The assoc-retransmit counter includes retransmissions of association initialization packets and retransmissions to all the destination transport addresses of the peer if it is multihomed.

Examples	The following example shows how to set the maximum number of retransmissions to 20:

```
cs7 mated-sg BLUE 5000
  remote-ip 5.5.5.5
  assoc-retransmit 20
```

Related Commands	Command	Description
	cs7 mated-sg	Specifies a connection to a mated SG and enters cs7 mated-sg submode.
	show cs7 mated-sg detail	Displays mated-SG information.

assoc-retransmit (cs7 sgmp)

An association retransmits packets when the sender does not receive an acknowledgement within a specified time period. To configure the maximum number of consecutive retransmissions to be allowed when a new SCTP association is started with the local port, use the **assoc-retransmit** command in **cs7 sgmp** configuration mode. When the maximum number is exceeded all transmission is stopped and the association is closed. To disable the configuration, use the **no** form of this command.

assoc-retransmit *max-retrans*

no assoc-retransmit *max-retrans*

Syntax Description	<i>max-retrans</i> Maximum association retransmissions. Range is 2 to 20.	
Defaults	10 retransmissions	
Command Modes	cs7 sgmp configuration	
Command History		
Usage Guidelines	The assoc-retransmit counter includes retransmissions of association initialization packets and retransmissions to all the destination transport addresses of the peer if it is multihomed.	
Examples	The following example shows how to set the maximum number of retransmissions to 20: cs7 sgmp 5000 local-ip 4.4.4.4 assoc-retransmit 20	
Related Commands	Command	Description
	cs7 sgmp	Specifies the local port number for SGMP and enters cs7 sgmp submode.
	show cs7 sgmp	Displays SGMP information.

assoc-retransmit (cs7 sua)

An association retransmits packets when the sender does not receive an acknowledgement within a specified time period. To configure the maximum number of consecutive retransmissions to be allowed when a new SCTP association is started with the local port, use the **assoc-retransmit** command in cs7 sua configuration mode. When the maximum number is exceeded all transmission is stopped and the association is closed. To disable the configuration, use the **no** form of this command.

assoc-retransmit *max-retrans*

no assoc-retransmit *max-retrans*

Syntax Description	<i>max-retrans</i>	Maximum association retransmissions. Range is 2 to 20.

Defaults	10 retransmissions

Command Modes	cs7 sua configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	The assoc-retransmit counter includes retransmissions of association initialization packets and retransmissions to all the destination transport addresses of the peer if it is multihomed.

Examples	The following example shows how to set the maximum number of retransmissions to 10:

```
cs7 sua 15000
 local-ip 4.4.4.4
 assoc-retransmit 20
```

Related Commands	Command	Description
	cs7 sua	Specifies the local port number for SUA and enters cs7 sua submode.
	show cs7 sua	Displays SUA node information.

atm nni

To specify the Service Specific Coordination Function for Network Node Interface (SSCF-NNI), use the **atm nni** command in interface configuration mode. To remove the specification, use the **no** form of this command.

atm nni

no atm nni

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

Interface configuration

Command History

Release	Modification
112.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Examples

The following example shows how to configure an ATM interface for NNI:

```
interface atm1/0/0
 no shutdown
 atm nni
 pvc atm_pvc1 0/5 qsaal
```

Related Commands

Command	Description
pvc	Specifies the PVC.

authorize

Authorization of the IMSI must be performed by accessing the subscriber's profile stored in the HLR. This subscriber profile is obtained by initiating a MAP version 2 Restore Data operation to the HLR servicing the IMSI. To authorize the IMSI, use the **authorize** command in gsm-authent-vlr configuration mode. To disable the IMSI, use the **no** form of this command.

authorize {**bs** *bs-number* | **ts** *ts-number*}

no authorize {**bs** *bs-number* | **ts** *ts-number*}

Syntax Description

bs	Performs the subscriber authorization check against a provisioned bearer service field in the subscriber's profile.
<i>bs-number</i>	A decimal coded integer in the range of 0 to 255. This value represents the decimal encoded value of the bearer service as specified in the GSM MAP specification 09.02 ¹ . Refer to Table 26 for a list of common values.
ts	Performs the subscriber authorization check against a provisioned teleservice field in the subscriber's profile.
<i>ts-number</i>	A decimal coded integer ranging from 0 to 255. This value represents the decimal encoded value of the teleservice as specified in the GSM MAP specification (09.02). Refer to Table 27 for a list of common values.

1. ETS 300 599: "Digital cellular telecommunications system (Phase 2); Mobile Application Part (MAP) specification (GSM 09.02 version 4.19.1).

Defaults

If the **authorize** command is not specified, then no authorization check is performed. There is no default bearer service or teleservice value.

Command Modes

gsm-authent-vlr configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

[Table 26](#) lists the bearer services defined in ETSI specification GSM 02.02 and the MAP encoded values in the MSU. ITP uses the decimal representation of the MAP encoded value.

Table 26 *Bearer Services and Decimal MAP Values*

Bearer Service	GSM 02.02 Bearer Service Number	Decimal MAP Value for Configuring ITP
allBearerServices		0
allDataCDA-Services		16

Table 26 *Bearer Services and Decimal MAP Values (continued)*

Bearer Service	GSM 02.02 Bearer Service Number	Decimal MAP Value for Configuring ITP
Asynchronous General Bearer Service	20	23
Asynchronous 300 bps	21	17
Asynchronous 1.2 kbps	22	18
Asynchronous 1200/75 kbps	23	19
Asynchronous 2.4 kbps	24	20
Asynchronous 4.8 kbps	25	21
Asynchronous 9.6 kbps	26	22
allDataCDS-Services		24
Synchronous General Bearer Service	30	31
Synchronous 1.2 kbps	31	26
Synchronous 2.4 kbps	32	28
Synchronous 4.8 kbps	33	29
Synchronous 9.6 kbps	34	30
allPadAccessCA-Services		32
General PAD Access Bearer Service	40	39
PAD Access 300 bps	41	33
PAD Access 1.2 kbps	42	34
PAD Access 1 200/75 bps	43	35
PAD Access 2.4 kbps	44	36
PAD Access 4.8 kbps	45	37
PAD Access 9.6 kbps	46	38
allDataPDS-Services		40
General Packet Access Bearer Service	50	47
Packet Access 2.4 kbps	51	44
Packet Access 4.8 kbps	52	45
Packet Access 9.6 kbps	53	46
Alternate Speech/Data	61	48 allAlternateSpeech-DataCDA 56 allAlternateSpeech-DataCDS
GPRS	70	
Speech Followed by Data	81	64 allSpeechFollowedByDataCDA 72 allSpeechFollowedByDataCDS
allDataCircuitAsynchronous		80
allAsynchronousServices		96
allDataCircuitSynchronous		88
allSynchronousServices		104

Table 26 *Bearer Services and Decimal MAP Values (continued)*

Bearer Service	GSM 02.02 Bearer Service Number	Decimal MAP Value for Configuring ITP
allPLMN-specificBS		208
plmn-specificBS-1		209
plmn-specificBS-2		210
plmn-specificBS-3		211
plmn-specificBS-4		212
plmn-specificBS-5		213
plmn-specificBS-6		214
plmn-specificBS-7		215
plmn-specificBS-8		216
plmn-specificBS-9		217
plmn-specificBS-A		218
plmn-specificBS-B		219
plmn-specificBS-C		220
plmn-specificBS-D		221
plmn-specificBS-E		222
plmn-specificBS-F		223

Table 27 lists the teleservices defined in ETSI specification GSM 02.03 and the MAP encoded values in the MSU. ITP uses the decimal representation of the MAP encoded value.

Table 27 *Teleservices and Decimal MAP Values*

Teleservice	GSM 02.03 Teleservice Number (Hex)	Decimal MAP Value for Configuring ITP
allTeleservices	0	0
allSpeechTransmission		16
Speech Transmission - Telephony	11	17
Speech Transmission - Emergency Calls	12	18
allShortMessageServices		32
SMS - Short Message MT/PP	21	33
SMS - Short Message MO/PP	22	34
SMS - Short Message Cell Broadcast	23	35
allFacsimileTransmissionServices		96
FAX - Alternate Speech and FAX group 3	61	97
FAX - Automatic FAX group 3	62	98
FAX - facsimileGroup4		99

Table 27 **Teleservices and Decimal MAP Values**

Teleservice	GSM 02.03 Teleservice Number (Hex)	Decimal MAP Value for Configuring ITP
Voice Group Service - Voice Group Call Service	91	145
Voice Group Service - Voice Broadcast Service	92	146
allPLMN-specificTS		208
plmn-specificTS-1		209
plmn-specificTS-2		210
plmn-specificTS-3		211
plmn-specificTS-4		212
plmn-specificTS-5		213
plmn-specificTS-6		214
plmn-specificTS-7		215
plmn-specificTS-8		216
plmn-specificTS-9		217
plmn-specificTS-A		218
plmn-specificTS-B		219
plmn-specificTS-C		220
plmn-specificTS-D		221
plmn-specificTS-E		222
plmn-specificTS-F		223

Examples

The following example shows how to configure bs 17 on the ITP to perform the subscriber authorization check against bearer service 21 (Asynchronous 300 bps data service), which is provisioned in the subscriber's profile on the HLR.

```
gsm-authent-vlr
  authorize bs 17
  cache-size 10000
  max-return 2
```

Related Commands

Command	Description
gsm-authent-vlr	Enables authent-vlr submode for provisioning parameters specific to the Process_Obtain_Authentication_Sets_VLR service.

bind-type (cs7 sms profile parameters)

To set the SMPP bind type parameter, use the **bind-type** command in cs7 sms profile parameters configuration mode. To return to the default bind type, use the **no** form of this command.

bind-type {any | receiver | transceiver | transmitter}

no bind-type {any | receiver | transceiver | transmitter}

Syntax Description

any	Allows receipt of any SMPP bind type; sends transceiver binds.
receiver	Receives or sends SMPP receiver binds only.
transceiver	Receives or sends SMPP transceiver binds only.
transmitter	Receives or sends SMPP transmitter binds only.

Defaults

The default bind type is **any**.

Command Modes

cs7 sms profile parameters configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

Received SMPP binds are checked against this command and rejected if they do not match.

The **bind-type** command is valid for SMPP profiles only. It cannot be configured in UCP profiles.

Examples

Related Commands

Command	Description
keepalive-timer (cs7 sms profile parameters)	Specifies session keepalive timer.
response-timer (cs7 sms profile parms)	Specifies session response timer.
send-window (cs7 sms profile parms)	Specifies send window size.
session-init-timer (cs7 sms profile parms)	Specifies session initiation timer.

bind-type (cs7 sms session parameters)

To set the SMPP bind type parameter, use the **bind-type** command in cs7 sms session parameters configuration mode. To return to the default bind type, use the **no** form of this command.

bind-type {any | receiver | transceiver | transmitter}

no bind-type {any | receiver | transceiver | transmitter}

Syntax Description

any	Allows receipt of any SMPP bind type; sends transceiver binds.
receiver	Receives or sends SMPP receiver binds only.
transceiver	Receives or sends SMPP transceiver binds only.
transmitter	Receives or sends SMPP transmitter binds only.

Defaults

The default bind type is **any**.

Command Modes

cs7 sms session parameters configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

Received SMPP binds are checked against this command and rejected if they do not match.

The **bind-type** command is valid for SMPP profiles only. It cannot be configured in UCP profiles.

Related Commands

Command	Description
response-timer (cs7 sms session parms)	Specifies session response timer.
send-window (cs7 sms session parms)	Specifies send window size.
session-init-timer (cs7 sms session parms)	Specifies session initiation timer.

block

To allow a new SCTP association to be established but prevent the ASP from going into the active state, use the **block** cs7 asp submode command. To reverse the block, use the **no** form of this command.

block

no block

Syntax Description This command has no arguments or keywords.

Defaults None.

Command Modes cs7 asp submode

Command History	Release	Modification
	12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.

Usage Guidelines The **block** and **shutdown** cs7 asp submode commands differ significantly.

The **shutdown** command terminates the SCTP association with this ASP. New SCTP associations are rejected when the ASP is in shutdown mode. Each time the SCTP tries to establish the association, it fails to receive an asp-up acknowledgement.

The **block** command sends an unsolicited asp-inactive acknowledgement. However, the ITP does not terminate the SCTP association. The SCTP keeps trying until it receives an asp-active acknowledgement.

Examples The following example shows how to block the ASP from entering an active state:

```
cs7 asp ASP1 2904 2905 m3ua
block
```

Related Commands	Command	Description
	cs7 asp	Defines an application server process and enables cs7 asp submode.
	show cs7 asp	Displays ASP information.
	shutdown (cs7 asp)	Terminates the SCTP association with this ASP.

broadcast

To enable the broadcast of route management messages, use the **broadcast** command in cs7 linkset configuration mode. To disable broadcasting, use the **no** form of this command.

ANSI Variant

broadcast {all | txa-txr | txp}

no broadcast {all | txa-txr | txp}

ITU or China Variant

broadcast {all | tfa | tfp}

no broadcast {all | tfa | tfp}

Syntax Description

all	Broadcasts all route management messages.
tfa	Broadcasts TFA.
tfp	Broadcasts TFP.
txa-txr	Broadcasts TFA/TCA and TFR/TCR.
txp	Broadcasts TFP/TCP.

Defaults

The ANSI, ITU, and China variants broadcast all route management messages.

Command Modes

cs7 linkset configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

This command is used to manage the ITP. Whenever a destination status changes on the ITP (due to received route management messages and linkset status changes), the ITP broadcasts the new status to the adjacent nodes by sending route management messages (TFP, TFR, TFA, TCP, TCR, TCA). The adjacent nodes use these messages to update their route tables.

If a large number of messages are sent to any adjacent node, that node can become temporarily overloaded, because processing a large number of management messages can be processor intensive. The **broadcast** command allows you to regulate the broadcast of route management messages to prevent this potential overloading.

You can disable broadcast messages on a per-linkset basis. If broadcast is disabled, the adjacent nodes do not receive the new status right away. However, when the nodes attempt to route the next MSU to the concerned destination via the ITP, the ITP sends a response method TFP or TFR (if the destination status is inaccessible or restricted). If the response method is TFP, the MSU is dropped.

Examples

ANSI, ITU, China Variants

The following example shows how to enable the broadcast of all route management messages on linkset1:

```
cs7 linkset linkset1
 broadcast all
```

The following example shows how to disable the broadcast of all route management messages on linkset1:

```
cs7 linkset linkset1
 no broadcast all
```

ANSI Variant

The following example shows how to enable the broadcast of TFA/TCA and TFR/TCR messages on linkset1:

```
cs7 linkset linkset1
 broadcast txa-txr
```

ITU or China Variants

The following example shows how to enable the broadcast of TFP messages on linkset1:

```
cs7 linkset linkset1
 broadcast tfp
```

Related Commands

Command	Description
cs7 linkset	Specifies a linkset and enters cs7 linkset submode.
show cs7 linkset detail	The detail keyword displays whether broadcast is on or off on the linkset.
snmp-server enable traps cs7	Enables SNMP network management traps to be sent to the specified host.

bundling (cs7 asp)

Multiple user messages can be bundled into a single SCTP packet. To configure message bundling, use the **bundling** command in cs7 asp configuration mode. To disable bundling, use the **no** form of this command.

bundling *msec*

no bundling *msec*

Syntax Description

<i>msec</i>	Maximum amount of time that to wait for messages for bundling. Valid range is 5 to 1000 milliseconds. The default is the value specified under the M3UA or SUA instance.

Defaults

The waiting time defaults to the value specified under the M3UA or SUA instance.

Command Modes

cs7 asp configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

When message bundling is enabled, packets might experience a delay before being sent. The delay is the amount of time the ITP waits for messages to be bundled. When messages are bundled, the resulting packet (including IP and SCTP headers) must be less than or equal to the MTU for the current path.

During periods of congestion, the ITP bundles messages (when possible) even if bundling is disabled. During these periods, abatement messages are bundled whenever possible, with no impact on performance.

Examples

The following example shows how to set the bundling interval to 500 milliseconds:

```
cs7 asp ASP1 2905 2905 m3ua
  remote-ip 1.1.1.1
  bundling 500
```

Related Commands

Command	Description
cs7 asp	Specifies an application server process and enables cs7 asp submode.
show cs7 asp detail	Displays ASP information.

bundling (cs7 link)

Multiple user messages can be bundled into a single packet. To configure message bundling, use the **bundling** command in cs7 link configuration mode. To disable bundling, use the **no** form of this command.

bundling *msec*

no bundling *msec*

Syntax Description

<i>msec</i>	Maximum amount of time to wait for messages for bundling. Valid range is 5 to 1000 milliseconds. The default is 5 milliseconds.

Defaults

This command is enabled.
The default waiting time is 5 milliseconds.

Command Modes

cs7 link configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced to enable bundling.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

When message bundling is enabled, packets might experience a delay before being sent. The delay is the amount of time the ITP waits for messages to be bundled. When messages are bundled, the resulting packet (including IP and SCTP headers) must be less than or equal to the MTU for the current path.

During periods of congestion, the ITP bundles messages (when possible) even if bundling is disabled. During these periods, abatement messages are bundled whenever possible, with no impact on performance.

MTP2 parameters can also be specified in a CS7 profile.

Examples

The following example shows how to set the bundling interval to 500 milliseconds:

```
cs7 linkset michael 10.1.1
 link 0 sctp 172.18.44.147 7000 7000
  bundling 500
```

Related Commands

Command	Description
cs7 linkset	Specifies a linkset and enters cs7 linkset submode.
cs7 profile	Defines a profile of MTP2 parameters that you can apply to all links in a linkset.
show cs7 m2pa	Displays ITP M2PA statistics.

bundling (cs7 m2pa profile)

Multiple user messages can be bundled into a single packet. To configure message bundling, use the **bundling** command in cs7 m2pa profile configuration mode. To disable bundling, use the **no** form of this command.

bundling *msec*

no bundling *msec*

Syntax Description

<i>msec</i>	Maximum amount of time to wait for messages for bundling. Valid range is 5 to 1000 milliseconds. The default is 5 milliseconds.

Defaults

This command is enabled.
The default waiting time is 5 milliseconds.

Command Modes

cs7 m2pa profile configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

When message bundling is enabled, packets might experience a delay before being sent. The delay is the amount of time the ITP waits for messages to be bundled. When messages are bundled, the resulting packet (including IP and SCTP headers) must be less than or equal to the MTU for the current path.

During periods of congestion, the ITP bundles messages (when possible) even if bundling is disabled. During these periods, abatement messages are bundled whenever possible, with no impact on performance.

MTP2 parameters can also be specified in a CS7 profile.

Examples

The following example shows how to define a profile named m2parfc. The profile supports M2PA RFC, specifies the **bundling** command, and applies to all the links in the linkset named to_nyc.

```
cs7 profile m2parfc
  m2pa
    bundling 100
  .
  .
  .
cs7 linkset to_nyc
  profile m2parfc
```

 bundling (cs7 m2pa profile)**Related Commands**

Command	Description
m2pa	Specifies M2PA parameters in a CS7 profile.

bundling (cs7 m3ua)

Multiple user messages can be bundled into a single SCTP packet. To specify whether packet bundling is supported and the bundling interval to be used when a new SCTP association is started with the local port, use the **bundling** cs7 m3ua submode command. To disable bundling, use the **no** form of this command.

bundling *msec*

no bundling *msec*

Syntax Description

<i>msec</i>	Maximum amount of time to wait for messages for bundling. Valid range is 5 to 1000 milliseconds. The default is 5 milliseconds.

Defaults

This command is enabled.
The default waiting time is 5 milliseconds.

Command Modes

cs7 m3ua submode

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

When message bundling is enabled, packets might experience a delay before being sent. The delay is the amount of time the ITP waits for messages to be bundled. When messages are bundled, the resulting packet (including IP and SCTP headers) must be less than or equal to the MTU for the current path.

During periods of congestion, the ITP bundles messages (when possible) even if bundling is disabled. During these periods, abatement messages are bundled whenever possible, with no impact on performance.

Examples

The following example shows how to set the bundling interval to 500 milliseconds:

```
cs7 m3ua 2905
 local-ip 4.4.4.4
 bundling 500
```

Related Commands

Command	Description
cs7 m3ua	Specifies the local port number for M3UA and enters cs7 m3ua submode.
show cs7 m3ua	Displays M3UA node information.

bundling (cs7 mated-sg)

Multiple user messages can be bundled into a single SCTP packet. To configure message bundling, use the **bundling** command in cs7 mated-sg configuration mode. To disable bundling, use the **no** form of this command.

bundling *msec*

no bundling *msec*

Syntax Description

<i>msec</i>	Maximum amount of time to wait for messages for bundling. Valid range is 5 to 1000 milliseconds. The default is the value specified under the local port instance.

Defaults

The waiting time defaults to the value specified under the SGMP instance.

Command Modes

cs7 mated-sg configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

When message bundling is enabled, packets might experience a delay before being sent. The delay is the amount of time the ITP waits for messages to be bundled. When messages are bundled, the resulting packet (including IP and SCTP headers) must be less than or equal to the MTU for the current path.

During periods of congestion, the ITP bundles messages (when possible) even if bundling is disabled. During these periods, abatement messages are bundled whenever possible, with no impact on performance.

Examples

The following example shows how to set the bundling interval to 500 milliseconds:

```
cs7 mated-sg BLUE 5000
  remote-ip 5.5.5.5
  bundling 500
```

Related Commands

Command	Description
cs7 mated-sg	Specifies a connection to a mated SG and enters cs7 mated-sg submode.
show cs7 mated-sg detail	Displays SGMP information.

bundling (cs7 profile)

Multiple user messages can be bundled into a single packet. To configure message bundling in a CS7 profile, use the **bundling** command in cs7 profile configuration mode. To disable bundling, use the **no** form of this command.

bundling *msec*

no bundling *msec*

Syntax Description

<i>msec</i>	Maximum amount of time to wait for messages for bundling. Valid range is 5 to 1000 milliseconds. The default is 5 milliseconds.

Defaults

This command is enabled.
The default waiting time is 5 milliseconds.

Command Modes

cs7 profile configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

When message bundling is enabled, packets might experience a delay before being sent. The delay is the amount of time the ITP waits for messages to be bundled. When messages are bundled, the resulting packet (including IP and SCTP headers) must be less than or equal to the MTU for the current path.

During periods of congestion, the ITP bundles messages (when possible) even if bundling is disabled. During these periods, abatement messages are bundled whenever possible, with no impact on performance.

Examples

The following example shows how to define a profile named timers. The profile supports MTP2, configures the packet bundling, t1, and t2 settings, and applies to all the links in the linkset named itpa.

```
cs7 profile timers
 mtp2
  timer t1 15000
  timer t2 9000
.
.
.
cs7 linkset itpa
 profile timers
```

Related Commands	Command	Description
	cs7 linkset	Specifies a linkset and enters cs7 linkset submode.
	cs7 profile	Defines a profile of MTP2 parameters that you can apply to all the links in a linkset.
	show cs7 m2pa	Displays ITP M2PA statistics.

bundling (cs7 sgmp)

Multiple user messages can be bundled into a single SCTP packet. To specify whether packet bundling is supported and the bundling interval to be used when a new SCTP association is started with the local port, use the **bundling** command in cs7 sgmp configuration mode. To disable bundling, use the **no** form of this command.

bundling *msec*

no bundling *msec*

Syntax Description	<i>msec</i>	Maximum amount of time to wait for messages for bundling. Valid range is 5 to 1000 milliseconds. The default is 5 milliseconds.

Defaults	This command is enabled. The default waiting time is 5 milliseconds.

Command Modes	cs7 sgmp configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	When message bundling is enabled, packets might experience a delay before being sent. The delay is the amount of time the ITP waits for messages to be bundled. When messages are bundled, the resulting packet (including IP and SCTP headers) must be less than or equal to the MTU for the current path. During periods of congestion, the ITP bundles messages (when possible) even if bundling is disabled. During these periods, abatement messages are bundled whenever possible, with no impact on performance.

Examples	The following example shows how to set the bundling interval to 500 milliseconds:

```
cs7 sgmp 5000
 local-ip 4.4.4.4
 bundling 500
```

Related Commands	Command	Description
	cs7 sgmp	Specifies the local port number for SGMP and enters cs7 sgmp submode.
	show cs7 sgmp	Displays SGMP statistics.

bundling (cs7 sua)

Multiple user messages can be bundled into a single SCTP packet. To specify whether packet bundling is supported and the bundling interval to be used when a new SCTP association is started with the local port, use the **bundling** command in cs7 sua configuration mode. To disable bundling, use the **no** form of this command.

bundling *msec*

no bundling *msec*

Syntax Description

<i>msec</i>	Maximum amount of time to wait for messages for bundling. Valid range is 5 to 1000 milliseconds. The default is 5 milliseconds.

Defaults

This command is enabled.

The default waiting time is 5 milliseconds.

Command Modes

cs7 sua configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

When message bundling is enabled, packets might experience a delay before being sent. The delay is the amount of time the ITP waits for messages to be bundled. When messages are bundled, the resulting packet (including IP and SCTP headers) must be less than or equal to the MTU for the current path.

During periods of congestion, the ITP bundles messages (when possible) even if bundling is disabled. During these periods, abatement messages are bundled whenever possible, with no impact on performance.

Examples

The following example shows how to set the bundling interval to 500 milliseconds:

```
cs7 sua 15000
 local-ip 4.4.4.4
 bundling 500
```

Related Commands

Command	Description
cs7 sua	Specifies the local port number for SUA and enters cs7 sua submode.
show cs7 sua	Displays SUA node information.

burst-recovery-timeout

To specify the amount of time allowed for an association to recover from a burst of traffic due to failover, use the **burst-recovery-timeout** command in **cs7** as configuration mode. To disable the configuration, use the **no** form of this command.

burst-recovery-timeout *msec*

no burst-recovery-timeout *msec*

Syntax Description	<i>msec</i>	Recovery timeout value. The valid range is 1000 to 10000 milliseconds. The default is 4000 milliseconds.

Defaults	4000 ms

Command Modes	cs7 as configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples The following example shows how to set the burst-recovery timeout to 1000 ms:

```
cs7 as BLUE m3ua
  burst-recovery-timeout 1000
```

Related Commands	Command	Description
	cs7 as	Defines an application server.

cache-size

To specify the total number of IMSIs for which authentication triplets are cached, use the **cache-size** command in cs7 authentic-vlr configuration mode. To disable caching, use the **no** form of this command. (Also, if the value of 0 is specified, caching is disabled.)

cache-size *cache-size*

no cache-size *cache-size*

Syntax Description	<i>cache-size</i>	Total number of IMSIs for which authentication triplets are cached. Valid value is a decimal number ranging from 1024 to 65535.

Defaults	The default cache size is 65535.

Command Modes	cs7 authentic-vlr configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	A maximum of five triplets can be stored for each IMSI.
	If you specify 0 for the cache size, caching is disabled. If you do not specify a value, the default cache size is 65535.

Examples	The following example shows how to specify a cache size of 100:

```
gsm-authent-vlr
  cache-size 100
  max-return 2
```

Related Commands	Command	Description
	ttl	Specifies the amount of elapsed time in seconds that a cached authentication triplet will be stored.
	gsm-authent-vlr	Enables authentic-vlr submode, in which you can provision parameters specific to the GSM MAP Process_Obtain_Authentication_Sets_VLR service.
	max-return	Specifies the maximum number of authentication triplets that may be returned to a MAPUA client for a single request.

cdpa (cs7 mlr modify-profile)

To indicate that the SCCP calling party address (cdpa) needs to be modified, use the **cdpa** command in cs7 mlr modify-profile mode. To disable modifications, use the **no** form of this command.

This command may be specified within the modify-profile for the ANSI-41 protocol or within any gsm-map operation. The cdpa routing indicator (RI) is unchanged during the modifications.

```
cdpa [gt [prefix {prefix-remove-num | *} {prefix-add-digits | *}] [tt tt] [gti {2 | 4 np np nai nai}] ]
[pc pc] [ssn ssn]
```

```
no cdpa [gt [prefix {prefix-remove-num | *} {prefix-add-digits | *}] [tt tt] [gti {2 | 4 np np nai
nai}] ] [pc pc] [ssn ssn]
```

Syntax Description

gt	Indicates global title information to modify. GT modifications apply only to packets with RI=GT. If GT modifications are configured and the received packet has a CdPA with RI=SSN, then the GT modifications are ignored.
prefix	Performs prefix modification on the address.
<i>prefix-remove-num</i>	An integer in the range from 1 to 15 that defines the number of prefix digits to remove from the address. If no prefix digits are to be removed, then specify a wildcard (*). Only GTAs with fewer than 15 digits can be replaced. To replace the entire address, specify that the maximum 15 digits are to be removed.
<i>prefix-add-digits</i>	A string of 1 to 15 hexadecimal digits to add to the beginning of the address. The string is input in normal form (not in BCD-string format). If no digits are to be added, then specify a wildcard (*) in this field.
tt	Indicates the global title translation type (tt) for the modified cdpa.
<i>tt</i>	Integer from 0 to 255 that replaces the existing <i>tt</i> value in the cdpa.
gti	Identifies the global title indicator value for the modified cdpa. This value is used only when the cs7 variant command specifies ITU or China.
<i>gti</i>	Integer value of 2 or 4.
np	Identifies the global title numbering plan for the modified cdpa.
<i>np</i>	Integer value from 0 to 15.
nai	Identifies the global title nature of address indicator for the modified cdpa. Specified only when <i>gti</i> is 4.
<i>nai</i>	Integer value from 0 to 127.
pc	Indicates that the cdpa trigger being defined is RI=PC. Identifies the point code for the modified cdpa.
<i>pc</i>	Point code in variant-specific point code format.
ssn	Identifies the subsystem number for the modified cdpa.
<i>ssn</i>	Subsystem number in decimal. Valid range is 2 to 255.

Defaults

None.

Command Modes cs7 mlr modify-profile

Command History 12.2(18)IXE This command was introduced.
 12.4(15)SW
 12.2(33)IRA

Examples cs7 mlr modify-profile *SRISM* gsm-map sri-sm
 orig-smsc prefix 2 351
 cdpa gt prefix 2 351

Usage Guidelines CdPA modification includes support for inserting a point code (PC) and subsystem number (SSN), as well as modifying the existing GT information, PC, and SSN. The CdPA routing indicator (RI) is unchanged during these modifications. The PC and the SSN may be inserted or modified regardless of the RI.
**Note**

 GT modifications apply only to packets with RI=GT.

If GT modifications are configured and the received packet has a CdPA with RI=SSN, then the GT modifications are ignored. The GT information that can be modified includes the GT address digits, the GT translation type (tt), the global title indicator (gti), the numbering plan (np), and the nature of address indicator (nai).

For prefix-based GT address translation, you can configure the number of prefix digits to be removed from the address and the digit string that should be prefixed to the address. Specifying a wildcard (*) for the number of prefix digits indicates that no digits will be removed. Specifying a wildcard (*) for the digit string indicates that no prefix digits are added to the address string. If the resulting modified address exceeds the maximum allowed number of digits, then MLR fails the modification and discards the packet by default. You can optionally configure the preferred action for failed modifications using the **modify-failure** command within mlr options submode.

Operations for applying MLR message modifications are in the following order:

1. Modifications specified using global MLR options
2. Modifications specified using MLR **modify-profile** within the selected rule
3. Modifications specified using MLR **result** within the selected rule

For example, MLR modifications to the CdPA using **modify-profile** are done before the processing of the selected MLR result. If result gt was selected, then any CdPA modifications made using **modify-profile** will be overwritten with the address specified in the result gt. Use **result route** to initiate routing of the packet to the CdPA that has been modified using **modify-profile**.

If the number of digits in the modified address is less than 1 digit or more than 30 digits, the address modification cannot be performed. In this case, the action taken is based on the configured **modify-failure** option. By default, the packet is discarded if it cannot be modified as specified.

**Note**

 The CdPA routing indicator (RI) is unchanged during these modifications.

Related Commands	Command	Description
	cs7 mlr modify-profile	Specifies an MLR modify profile.
	modify-failure (mlr options)	Specifies the desired action when MLR packet modification fails.

cdpa (cs7 mlr trigger)

You can configure a secondary trigger in conjunction with the primary trigger address to create a combination trigger used to match a packet. To create a combination trigger based on the combination of the calling party and the called party, use the **cdpa** command in cs7 mlr trigger configuration mode within a calling party address trigger. To disable the specific routing trigger, use the **no** form of this command.

```
cdpa {gt addr-string [gt-addr-type] | pc point-code ssn ssn} {block | continue | ruleset
ruleset-name | result {pc pc [ssn ssn] | asname as-name | gt gta [gt-addr-type] | group
group-name}}
```

```
no cdpa {gt addr-string [gt-addr-type] | pc point-code ssn ssn} {block | continue | ruleset
ruleset-name | result {pc pc [ssn ssn] | asname as-name | gt gta [gt-addr-type] | group
group-name}}
```

Syntax Description	
gt	Indicates that the CdPA secondary trigger being defined is received with RI=GT.
<i>addr-string</i>	Address string of 1 to 15 hexadecimal characters. The string is input in normal form, not in BCD-string format.
<i>gt-addr-type</i>	(Optional) Parameters that identify attributes of the global title address being used as a trigger. The parameters are variant-specific, and are identical to those parameters specified on the cs7 gtt selector command. If not specified, the default is the standard E.164 address type for the network variant being used. tt <i>tt</i> [gti <i>gti</i>] [np <i>np</i> nai <i>nai</i>] tt Identifies the translation type specified within the address. <i>tt</i> An integer value from 0 to 255. gti Identifies the global title indicator value for the specified address. This value is used only when the cs7 variant command specifies ITU or China. <i>gti</i> Integer value of 2 or 4. np Identifies the numbering plan of the specified address. Used only when the <i>gti</i> value is 4. <i>np</i> Integer value from 0 to 15. nai Identifies the nature of address indicator. Used only when the <i>gti</i> value is 4. <i>nai</i> Integer value from 0 to 127.
pc	Matches the trigger if it contains the specified point code. The PC within the SCCP CdPA is inspected first. If the PC is not present, then the OPC is used.
<i>point-code</i>	Point code in variant-specific point code format.
ssn	(Optional) Routes based on PC and subsystem number.
<i>ssn</i>	Subsystem number in decimal. Valid range is 2 to 255.
block	Drops messages matching this trigger. This keyword is ignored if combination triggers are defined within cs7 mlr trigger mode.

continue	Routes messages matching this trigger as received. This behavior is the same as if no primary trigger had been matched. This keyword is ignored if combination triggers are defined within cs7 mlr trigger mode.
ruleset	Specifies the MLR ruleset table that should be used if this trigger is matched, and overrules the ruleset specified on the trigger command.
<i>ruleset-name</i>	Name of a defined CS7 MLR ruleset table. The name is specified as a character string with a maximum of 12 characters.
result	Routes the message based on the trigger alone. Result groups with dest-sme-binding mode are not valid trigger results.
pc	Routes based on point code.
<i>pc</i>	Point code.
ssn	(Optional) Specifies the subsystem number.
<i>ssn</i>	Subsystem number.
asname	Routes based on AS name.
<i>as-name</i>	AS name.
gt	Routes based on global title.
<i>gta</i>	Global title address.
group	Routes based on result group.
<i>group-name</i>	Result group name.

Defaults

None.

Command Modes

cs7 mlr trigger configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

A combination trigger uses more than one network layer address for identifying a trigger match. Within a combination trigger, one address is defined as the primary trigger and the other address is the secondary trigger.

The primary trigger must correlate with a defined GTT GTA, GTT selector, or GTT MAP entry. The GTT and GTT MAP databases are used as the lookup mechanism for primary triggers. After a primary trigger match occurs, then the list of secondary triggers (defined within the primary trigger submode) is checked. If one or more secondary triggers have been defined, the secondary triggers are sequentially searched for a match. If no match on the secondary trigger occurs, then the packet is not routed using MLR. If no secondary triggers have been defined, then MLR processing continues based on the primary trigger only.

If you configure a secondary address in cs7 mlr trigger mode, then *both* addresses must match for the packet to be blocked or routed using the specified ruleset.

The primary trigger must be for a calling party address for the **cdpa** command to be valid.

CdPA GT and CdPA GT secondary triggers do not require a matching GTT entry.

In all primary and secondary trigger definitions:

- The **pc** keyword is matched only if RI=SSN.
- The **ssn** keyword is matched only if RI=SSN.

With the configurable **result** trigger action, MLR users can route messages based on the trigger alone. If a trigger result is configured, the TCAP/MAP/SMS layers are not parsed. If a message matches a trigger with a **result** trigger action, then the message is redirected as indicated in the trigger result. Result groups with dest-sme-binding mode are not valid trigger results.

Examples

The following example shows how to create a combination trigger based on the combination of the primary trigger (the CgPA) and the secondary trigger (the CdPA). The example applies ruleset-5 if the combination trigger is found.

```
cs7 mlr table sms-router
trigger cgpa gt 9991117770
cdpa gt 9991116 ruleset ruleset-5
```

The following example shows how to create a combination trigger based on the combination of the primary trigger (the CgPA) and the secondary trigger (the CdPA), and places the **block** keyword at the end of the secondary trigger:

```
cs7 mlr table sms-blocking
trigger cgpa gt 9991117777 tt 10
cdpa gt 9991115555 tt 10 block
```

The following example shows how to create a combination trigger based on the combination of the primary trigger (the CgPA) and the secondary trigger (the CdPA). If a message matches the trigger, the message is redirected to point code 3.3.3.

```
cs7 mlr table sms-router
trigger cgpa gt 9991117770
cdpa gt 9991116 result pc 3.3.3
```

Related Commands

Command	Description
cs7 mlr ruleset	Specifies sets of rules that will be used to process traffic-matching triggers defined in a multilayer routing table.
default	Specifies the routing of packets on primary triggers when defined secondary triggers are not matched.
show cs7 mlr table	Displays MLR information.
trigger cgpa (cs7 mlr table)	Specifies a primary routing trigger that is located in the SCCP calling party address field of the incoming MSU.

cdpa (cs7 pam)

To configure one called party address (cdpa) entry in the PAM table, use the **cdpa** command in CS7 PAM configuration submode. To disable modifications, use the **no** form of this command.

```
cdpa [gt [prefix {prefix-remove-num | *} {prefix-add-digits | *}]] [tt tt] [gti {2 | 4 np np nai nai}] [pc pc] [ssn ssn]
```

```
no cdpa [gt [prefix {prefix-remove-num | *} {prefix-add-digits | *}]] [tt tt] [gti {2 | 4 np np nai nai}] [pc pc] [ssn ssn]
```

Syntax Description

gt	Indicates global title information to modify.
prefix	Performs prefix modification on the address.
<i>prefix-remove-num</i>	An integer in the range from 1 to 15 that defines the number of prefix digits to remove from the address. If no prefix digits are to be removed, then specify a wildcard (*). Only GTAs with fewer than 16 digits can be replaced.
<i>prefix-add-digits</i>	A string of 1 to 15 hexadecimal digits which are to be added to the beginning of the address. The string is input in normal form (not BCD-string format). If no digits are added, then "*" should be specified in this field. If the number of digits in the modified address would exceed the 30 digits, then the address modification cannot be performed. In this failure case, the action taken is based on the configured modify-failure parameter. By default, the packet is discarded.
tt	Indicates the global title translation type (tt) for the modified CgPA.
<i>tt</i>	Integer from 0 to 255 that replaces the existing <i>tt</i> value.
gti	Identifies the global title indicator value for the modified cdpa. This value is used only when the cs7 variant command specifies ITU or China.
<i>gti</i>	Integer value of 2 or 4.
np	Identifies the global title numbering plan.
<i>np</i>	Integer value from 0 to 15.
nai	Identifies the global title nature of address indicator for the modified cdpa. Specified only when <i>gti</i> is 4.
<i>nai</i>	Integer value from 0 to 127.
pc	Identifies the point code for the modified cdpa.
<i>pc</i>	Point code in variant-specific point code format.
ssn	Identifies the subsystem number for the modified cdpa.
<i>ssn</i>	Subsystem number in decimal. Valid range is 2 to 255.

Defaults

None.

Command Modes

CS7 PAM configuration submode

Command History

12.4(15)SW5	This command was introduced.
12.2(33)IRE	

Examples

The following example shows a cdpa entry configured for the PAM table named pam1:

```
cs7 instance 0 pam pam1
  cgpa gt prefix tt 0 pc 1.2.3 ssn 12
  cdpa gt prefix 15 123456789abcdef tt 250 gti 4 np 15 nai 127 pc 1.123.4 ssn 255\n
  opc 1.2.3
  dpc 2.3.4
  modify-failure resume
```

Usage Guidelines

CdPA modification includes support for inserting a point code (PC) and subsystem number (SSN), as well as modifying the existing GT information, PC, and SSN. The CdPA routing indicator (RI) is unchanged during these modifications. The PC and the SSN may be inserted or modified regardless of the RI.

The GT information that can be modified includes the GT address digits, the GT translation type (tt), the global title indicator (gti), the numbering plan (np), and the nature of address indicator (nai).

For prefix-based GT address translation, you can configure the number of prefix digits to be removed from the address and the digit string that should be prefixed to the address. Specifying a wildcard (*) for the number of prefix digits indicates that no digits will be removed. Specifying a wildcard (*) for the digit string indicates that no prefix digits are added to the address string. If the resulting modified address exceeds the maximum allowed number of digits, then PAM fails the modification and discards the packet by default. You can optionally configure the preferred action for failed modifications using the modify-failure command within mlr options submenu.

If the number of digits in the modified address is less than 1 digit or more than 30 digits, the address modification cannot be performed. In this case, the action taken is based on the configured modify-failure option. By default, the packet is discarded if it cannot be modified as specified.

The CdPA routing indicator (RI) is unchanged during these modifications.

Related Commands

Command	Description
cs7 pam	Identifies a packet address modification (PAM) table and enters the CS7 PAM submenu.
cgpa (cs7 pam)	Configures one cgpa entry in the PAM table.
opc	Configures an opc entry in the PAM table.
dpc	Configures a dpc entry in the PAM table.
modify-failure (pam)	Specifies the desired action when the PAM table packet modification fails.
cs7 gws action-set	Defines gateway screening action sets that may include a PAM table.
gta asname	Creates or modifies a GTA entry that translates to an M3UA or SUA application server name. The GTA entry may include a PAM table.

cgpa (cs7 mlr modify-profile)

To indicate that the SCCP calling party address (CgPA) needs to be modified, use the **cgpa** command in global configuration mode. To disable modifications, use the **no** form of this command.

```
cgpa [gt [prefix {prefix-remove-num | *} {prefix-add-digits | *}] [tt tt] [gti {2 | 4 np np nai nai}] ] |
[pc pc] [ssn ssn]
```

```
no cgpa [gt [prefix {prefix-remove-num | *} {prefix-add-digits | *}] [tt tt] [gti {2 | 4 np np nai nai}] ] |
[pc pc] [ssn ssn]
```

Syntax Description

cgpa	Indicates that the SCCP calling party address (CgPA) needs to be modified. The CgPA routing indicator (RI) is unchanged during these modifications.
gt	Indicates global title information to modify. GT modifications apply only to packets with RI=GT. If GT modifications are configured and the received packet has a CdPA with RI=SSN, then the GT modifications are ignored.
prefix	Performs prefix modification on the address.
<i>prefix-remove-num</i>	An integer in the range of 1 to 15 that defines the number of prefix digits to remove from the address. If no prefix digits are to be removed, then specify a wildcard (*). Only GTAs with fewer than 15 digits can be replaced. To replace the entire address, specify that the maximum 15 digits are to be removed.
<i>prefix-add-digits</i>	A string of 1 to 15 hexadecimal digits to add to the beginning of the address. The string is input in normal form (not in BCD-string format). If no digits are to be added, then specify a wildcard (*) in this field. If the number of digits in the modified address exceeds 30 digits, then the address cannot be modified. In this case, the action taken is based on the configured build-failure parameter. By default, a UDTs is sent with an unqualified sccp-error.
tt	Indicates the global title translation type (tt) for the modified CgPA.
<i>tt</i>	Integer from 0 to 255 that replaces the existing <i>tt</i> value in the CgPA.
gti	Identifies the global title indicator value for the modified CgPA. This value is used only when the cs7 variant command specifies ITU or China.
<i>gti</i>	Integer value of 2 or 4.
np	Identifies the global title numbering plan for the modified CgPA.
<i>np</i>	Integer value from 0 to 15.
nai	Identifies the global title nature of address indicator for the modified CgPA. Specified only when the <i>gti</i> value is 4.
<i>nai</i>	Integer value from 0 to 127.
pc	Indicates that the CgPA trigger being defined is RI=PC. Identifies the point code for the modified CgPA.
<i>pc</i>	Point code in variant-specific point code format.
ssn	Identifies the subsystem number for the modified CgPA.
<i>ssn</i>	Subsystem number in decimal. Valid range is 2 to 255.

Defaults

None.

Command Modes

cs7 mlr modify-profile

Command History

12.2(18)IXC	This command was introduced.
12.4(11)SW	
12.2(33)IRA	
12.2(18)IXE	The cgpa keyword may be specified for the ansi-41
12.4(15)SW	
12.2(33)IRA	

Examples

cs7 mlr modify-profile *SRISM* gsm-map sri-sm
 orig-smsc prefix 2 351
 cgpa gt prefix 2 351

Usage Guidelines

This command may be specified within the modify-profile for the ANSI-41 protocol or within any gsm-map operation. The CgPA routing indicator (RI) is unchanged during the modifications.

CgPA modification includes support for inserting a point code (PC) and subsystem number (SSN), as well as modifying the existing GT information, PC, and SSN. The CgPA routing indicator (RI) is unchanged during these modifications. The PC and the SSN may be inserted or modified regardless of the RI.

**Note**

GT modifications apply only to packets with RI=GT.

If GT modifications are configured and the received packet has a CgPA with RI=SSN, then the GT modifications are ignored. The GT information that can be modified includes the GT address digits, the GT translation type (tt), the global title indicator (gti), the numbering plan (np), and the nature of address indicator (nai).

For prefix-based GT address translation, you can configure the number of prefix digits to be removed from the address and the digit string that should be prefixed to the address. Specifying a wildcard (*) for the number of prefix digits indicates that no digits will be removed. Specifying a wildcard (*) for the digit string indicates that no prefix digits are added to the address string. If the resulting modified address exceeds the maximum allowed number of digits, then MLR fails the modification and discards the packet by default. You can optionally configure the preferred action for failed modifications using the **modify-failure** command within mlr options submode.

Operations for applying MLR message modifications are in the following order:

1. Modifications specified using global MLR options
2. Modifications specified using MLR **modify-profile** within the selected rule
3. Modifications specified using MLR **result** within the selected rule

For example, MLR modifications to the CgPA using **modify-profile** are done before the processing of the selected MLR result. If result **gt** was selected, then any CgPA modifications made using **modify-profile** will be overwritten with the address specified in the result **gt**. Use **result route** to initiate routing of the packet to the CdPA that has been modified using **modify-profile**.

If the number of digits in the modified address is less than 1 digit or more than 30 digits, the address modification cannot be performed. In this case, the action taken is based on the configured **modify-failure** option. By default, the packet is discarded if it cannot be modified as specified.

**Note**

The CgPA routing indicator (RI) is unchanged during these modifications.

Related Commands

Command	Description
cs7 mlr modify-profile	Specifies an MLR modify profile.
modify-failure (mlr options)	Specifies the desired action when MLR packet modification fails.

cgpa (cs7 mlr trigger)

You can configure a secondary trigger in conjunction with the trigger address to create a combination trigger used to match a packet. To create a combination trigger based on the combination of the calling party and the called party, use the **cgpa** command in cs7 mlr trigger configuration mode within a called party address trigger. To disable the specific routing trigger, use the **no** form of this command.

```
cgpa {gt addr-string [gt-addr-type] | pc point-code ssn ssn} {block | continue | ruleset
ruleset-name | result {pc pc [ssn ssn] | asname as-name | gt gt [gt-addr-type] | group
group-name}}
```

```
no cgpa {gt addr-string [gt-addr-type] | pc point-code ssn ssn} {block | continue | ruleset
ruleset-name | result {pc pc [ssn ssn] | asname as-name | gt gt [gt-addr-type] | group
group-name}}
```

Syntax Description

gt	Indicates that the CgPA trigger being defined is received with RI=GT.
<i>addr-string</i>	Address string of 1 to 15 hexadecimal characters. The string is input in normal form, not in BCD-string format.
<i>gt-addr-type</i>	(Optional) Identifies attributes of the global title address being used as a trigger. The parameters are variant-specific, and are identical to those parameters specified on the cs7 gtt selector command. If not specified, the default is the standard E.164 address type for the network variant being used. tt <i>tt</i> [gti <i>gti</i>] [np <i>np</i> nai <i>nai</i>] tt Identifies the translation type specified within the address. <i>tt</i> An integer value from 0 to 255. gti Identifies the global title indicator value for the specified address. This value is used only when the cs7 variant command specifies ITU or China. <i>gti</i> Integer value of 2 or 4. np Identifies the numbering plan of the specified address. Used only when the <i>gti</i> value is 4. <i>np</i> Integer value from 0 to 15. nai Identifies the nature of address indicator. Used only when the <i>gti</i> value is 4. <i>nai</i> Integer value from 0 to 127.
pc	Matches the trigger if it contains the specified point code. The PC within the SCCP CdPA is inspected first. If the PC is not present, then the DPC in the routing label is used.
<i>point-code</i>	Point code in variant-specific point code format.
ssn	(Optional) Routes based on PC and subsystem number.
<i>ssn</i>	Subsystem number in decimal. Valid range is 2 to 255.
block	Drops messages matching this trigger. This keyword is ignored if combination triggers are defined within cs7 mlr trigger mode.

continue	Routes messages matching this trigger as received. This behavior is the same as if no primary trigger had been matched. This keyword is ignored if combination triggers are defined within cs7 mlr trigger mode.
ruleset	Specifies the MLR ruleset table that should be used if this trigger is matched, and not overruled by a secondary trigger ruleset.
<i>ruleset-name</i>	Name of an already defined cs7 mlr ruleset table. The name is specified as a character string with a maximum of 12 characters.
result	Routes the message based on the trigger alone. Result groups with dest-sme-binding mode are not valid trigger results.
pc	Routes based on point code.
<i>pc</i>	Point code.
ssn	(Optional) Routes based on PC and subsystem number.
<i>ssn</i>	Subsystem number.
asname	Routes based on AS name.
<i>as-name</i>	AS name.
gt	Routes based on global title.
<i>gta</i>	Global title address.
group	Routes based on result group.
<i>group-name</i>	Result group name.

Defaults

None.

Command Modes

cs7 mlr trigger configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

A combination trigger uses more than one network layer address for identifying a trigger match. Within a combination trigger, one address is defined as the primary trigger and the other address is the secondary trigger.

The primary trigger must correlate with a defined GTT GTA, GTT selector, or GTT MAP entry. The GTT and GTT MAP databases are used as the lookup mechanism for primary triggers. After a primary trigger match occurs, then the list of secondary triggers (defined within the primary trigger submode) is checked. If one or more secondary triggers have been defined, the secondary triggers are sequentially searched for a match. If no match on the secondary trigger occurs, then the packet is not routed using MLR. If no secondary triggers have been defined, then MLR processing continues based on the primary trigger only.

If you configure a secondary address in cs7 mlr trigger submode, then *both* addresses must match for the packet to be blocked or routed using the specified ruleset.

The primary trigger must be for a called party for the **cgpa** submode command to be valid.

CDPA GT and CGPA GT secondary triggers do not require a matching GTT entry.

In all primary and secondary trigger definition:

- The **pc** keyword is matched only if RI=SSN.
- The **ssn** keyword is matched only if RI=SSN.

With the configurable **result** trigger action, MLR users can route messages based on the trigger alone. If a trigger result is configured, the TCAP/MAP/SMS layers are not parsed. If a message matches a trigger with a **result** trigger action, then the message is redirected as indicated in the trigger result. Result groups with dest-sme-binding mode are not valid trigger results.

Examples

The following example shows how to create a combination trigger based on the combination of the primary trigger (the called party, cdpa) and the secondary trigger (the calling party, cgpa). The example applies ruleset-5 if the combination trigger is found.

```
cs7 mlr table sms-router
trigger cdpa gt 9991117770
cgpa gt 9991116 ruleset ruleset-5
```

The following example shows how to create a combination trigger based on the combination of the primary trigger (the CdPA) and the secondary trigger (the CgPA), and places the **block** keyword at the end of the secondary trigger:

```
cs7 mlr table sms-blocking
trigger cdpa gt 11111 tt 10
cgpa gt 22222 tt 10 block
```

The following example shows how to create a combination trigger based on the combination of the primary trigger (the CdPA) and the secondary trigger (the CgPA). If a messages matches the trigger, the message is redirected to point code 3.3.3.

```
cs7 mlr table sms-router
trigger cdpa gt 9991117770
cgpa gt 9991116 result pc 3.3.3
```

Related Commands

Command	Description
cs7 mlr ruleset	Specifies sets of rules that will be used to process traffic-matching triggers defined in a multilayer routing table.
default	Creates a trigger to be used if all other subtriggers are unmatched.
show cs7 mlr table	Displays multilayer SMS routing information.
trigger cdpa (cs7 mlr table)	Specifies a routing trigger that is located in the SCCP called party address field of the incoming MSU.

cgpa (cs7 pam)

To configure a calling party address (cgpa) entry in the PAM table, use the **cgpa** command in CS7 PAM configuration submode. To disable modifications, use the **no** form of this command.

```
cgpa [gt [prefix {prefix-remove-num | *} {prefix-add-digits | *}] [tt tt] [gti {2 | 4 np np nai nai}] ]
[pc pc] [ssn ssn]
```

```
no cgpa [gt [prefix {prefix-remove-num | *} {prefix-add-digits | *}] [tt tt] [gti {2 | 4 np np nai nai}] ]
[pc pc] [ssn ssn]
```

Syntax Description

gt	Indicates global title information to modify.
prefix	Performs prefix modification on the address.
<i>prefix-remove-num</i>	An integer in the range from 1 to 15 that defines the number of prefix digits to remove from the address. If no prefix digits are to be removed, then specify a wildcard (*). Only GTAs with fewer than 16 digits can be replaced.
<i>prefix-add-digits</i>	A string of 1 to 15 hexadecimal digits which are to be added to the beginning of the address. The string is input in normal form (not BCD-string format). If no digits are added, then "*" should be specified in this field. If the number of digits in the modified address would exceed the 30 digits, then the address modification cannot be performed. In this failure case, the action taken is based on the configured modify-failure parameter. By default, the packet is discarded.
tt	Indicates the global title translation type (tt) for the modified CgPA.
<i>tt</i>	Integer from 0 to 255 that replaces the existing <i>tt</i> value.
gti	Identifies the global title indicator value for the modified cgpa. This value is used only when the cs7 variant command specifies ITU or China.
<i>gti</i>	Integer value of 2 or 4.
np	Identifies the global title numbering plan.
<i>np</i>	Integer value from 0 to 15.
nai	Identifies the global title nature of address indicator for the modified cgpa. Specified only when <i>gti</i> is 4.
<i>nai</i>	Integer value from 0 to 127.
pc	Identifies the point code for the modified cgpa.
<i>pc</i>	Point code in variant-specific point code format.
ssn	Identifies the subsystem number for the modified cgpa.
<i>ssn</i>	Subsystem number in decimal. Valid range is 2 to 255.

Defaults

None.

Command Modes

CS7 PAM configuration submode

Command History

12.4(15)SW5	This command was introduced.
12.2(33)IRE	

Examples

The following example shows a cgpa entry configured for the PAM table named pam1:

```
cs7 instance 0 pam pam1
  cgpa gt prefix tt 0 pc 1.2.3 ssn 12
  cdpa gt prefix 15 123456789abcdef tt 250 gti 4 np 15 nai 127 pc 1.123.4 ssn 255\n
  opc 1.2.3
  dpc 2.3.4
  modify-failure resume
```

Usage Guidelines

CgPA modification includes support for inserting a point code (PC) and subsystem number (SSN), as well as modifying the existing GT information, PC, and SSN. The PC and the SSN may be inserted or modified regardless of the RI.

The GT information that can be modified includes the GT address digits, the GT translation type (tt), the global title indicator (gti), the numbering plan (np), and the nature of address indicator (nai).

For prefix-based GT address translation, one can configure the number of prefix digits to be removed from the address and the digit string that should be prefixed to the address. Specifying a wildcard (*) for the number of prefix digits (prefix-remove-num) indicates that no digits will be removed. Specifying a wildcard (*) for the prefix-add-digits digit string indicates that no prefix digits are added to the address string. If the resulting modified address exceeds the maximum allowed number of digits, then PAM fails the modification and discards the packet by default. You can optionally configure the preferred action for failed modifications using the modify-failure command within mlr options submenu.

If the number of digits in the modified address is less than 1 digit or more than 30 digits, the address modification cannot be performed. In this case, the action taken is based on the configured modify-failure option. By default, the packet is discarded if it cannot be modified as specified.

The CgPA routing indicator (RI) is unchanged during these modifications.

Related Commands

Command	Description
cs7 pam	Identifies a packet address modification (PAM) table and enters the CS7 PAM submenu.
cdpa (cs7 pam)	Configures one cdpa entry in the PAM table.
opc	Configures an opc entry in the PAM table.
dpc	Configures a dpc entry in the PAM table.
modify-failure (pam)	Specifies the desired action when the PAM table packet modification fails.
cs7 gws action-set	Defines gateway screening action sets that may include a PAM table.
gta asname	Creates or modifies a GTA entry that translates to an M3UA or SUA application server name. The GTA entry may include a PAM table.

clear cs7 accounting

To clear the ITP accounting databases, use the **clear cs7 accounting** EXEC command.

clear cs7 [*instance-number*] **accounting** [**access-violations** | **gtt** | **unrouteable**] [**checkpoint**]

Syntax Description

<i>instance-number</i>	Instance number.
access-violations	Clears the access-violation accounting database.
checkpoint	Clears all checkpointed accounting databases.
gtt	Clears the GTT accounting database, including all the linksets and xUA ASes.
unrouteable	Clears all unrouteable accounting databases.

Defaults

None.

Command Modes

EXEC

Command History

Usage Guidelines

The **clear cs7 accounting** command resets counters. It is useful in debugging because it can track new message activity.

This command can be issued either globally or on an instance.

Examples

The following example shows how to clear the ITP access violations database:

```
clear cs7 accounting access-violations
```

Related Commands

Command	Description
show cs7 accounting	Displays ITP accounting details.
clear cs7 all	Clears accounting details.

clear cs7 all

To clear all accounting, statistics, and GTT measurements, use the **clear cs7 all** EXEC command.

clear cs7 [*instance-number*] **all** [**checkpoint**]

Syntax Description	checkpoint	(Optional) Clears all data, including all checkpoint tables.
	<i>instance-number</i>	Instance number.

Defaults	None.

Command Modes	EXEC

Command History

Usage Guidelines	This command can be issued either globally or on an instance.

Examples

The following example shows how to clear all accounting, statistics, and GTT measurements, including all checkpoint tables:

```
clear cs7 all checkpoint
```

Related Commands	Command	Description
	clear cs7 accounting	Clears the ITP accounting databases.
	clear cs7 gtt-meas	Resets all GTT measurements to 0.
	clear cs7 mtp3 event-history	Clears the MTP3 event-history log.
	clear cs7 statistics	Clears statistics concerning MSU throughput on a linkset basis.
	show cs7	Displays ITP basic configuration status.

clear cs7 as

To clear all application server statistics, use the **clear cs7 as** EXEC command.

clear cs7 [*instance-number*] **as** {**event-history** | **statistics**} {*as-name* | **all**}

Syntax Description	<i>instance-number</i>	Instance number.
	event-history	Event-history log.
	statistics	AS statistics.
	<i>as-name</i>	AS name.
	all	Clears all statistics.

Defaults	None.

Command Modes	EXEC

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples	The following example shows how to clear all application server statistics: clear cs7 as statistics all

Related Commands	Command	Description
	cs7 as	Specifies an application server and enters cs7 as submode.
	show cs7 as	Displays AS and routing key information.
	show cs7 asp statistics	Displays ASP statistics.

clear cs7 asp

To clear all application server process statistics, use the **clear cs7 asp** EXEC command.

```
clear cs7 asp {event-history | statistics} {asp-name | all}
```

Syntax Description	event-history	Event-history log.
	statistics	ASP statistics.
	<i>asp-name</i>	ASP name.
	all	Clears all statistics.

Defaults	None.

Command Modes	EXEC

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples	The following example shows how to clear all application server process statistics: <pre>clear cs7 asp statistics all</pre>

Related Commands	Command	Description
	cs7 asp	Specifies an application server process and enables cs7 asp submode.
	show cs7 asp statistics	Displays ASP statistics.

clear cs7 dynamic-route

To clear a dynamic route, use the **clear cs7 dynamic-route** EXEC command.

clear cs7 [*instance-number*] **dynamic-route** {*point-code* | **all** [*minutes*]}

Syntax Description	<i>instance-number</i>	Instance number.
	<i>point-code</i>	Clears the dynamic route with this point code.
	all	Clears all dynamic routes.
	<i>minutes</i>	Purges only if older than specified time. Range is 0 to 20160 minutes.

Defaults	None.

Command Modes	EXEC

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	This command can be issued either globally or on an instance.

Examples	The following example shows how to clear all dynamic routes: clear cs7 dynamic-route all

clear cs7 gtt-gta

To clear all GTA_MATCH counters, use the **clear cs7 gtt-gta** command in privileged EXEC mode.

clear cs7 gtt-gta

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.4(15)SW8	This command was introduced.
	12.2(33)IRH	

Usage Guidelines	GTA-MATCH counters apply only for LC. Hence, the counters do not increment on SUP. If the command is executed on SUP, the output is zero for GTA_MATCH counters.

Examples	The following example shows how to clear all GTA_MATCH counters:

```
clear cs7 gtt-gta
```

Related Commands	Command	Description
	show cs7 gtt gta	Displays a summary of CS7 GTT GTA entries.

clear cs7 gtt-meas

To reset all GTT measurements to 0, use the **clear cs7 gtt-meas** privileged EXEC command.

clear cs7 [*instance-number*] **gtt-meas**

Syntax Description

<i>instance-number</i>	Instance number.

Defaults

None.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

This command can be issued either globally or on an instance.

Examples

The following example shows how to clear all GTT measurements:

```
clear cs7 gtt-meas
```

Related Commands

Command	Description
show cs7 gtt measurements	Displays a summary of CS7 GTT/SCCP measurements.

clear cs7 gws counters

To clear all counters in GWS packet processing, use the **clear cs7 gws counters** command in privileged EXEC mode.

clear cs7 gws counters

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.4(15)SW8 12.2(33)IRH	This command was introduced.

Examples	The following example shows how to clear all GWS debugging counters: <pre>clear cs7 gws counters</pre>

Related Commands	Command	Description
	clear counters	

clear cs7 mated-sg statistics

To clear all SG mated-pair statistics, use the **clear cs7 mated-sg statistics** EXEC command.

clear cs7 mated-sg statistics

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Command Modes	EXEC

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples	The following example shows how to clear all SG mated-pair statistics: <pre>clear cs7 mated-sg statistics</pre>

Related Commands	Command	Description
	cs7 mated-sg	Specifies a connection to a mated SG and enters cs7 mated-sg submode.
	show cs7 mated-sg statistics	Displays mated-SG statistics.

clear cs7 mlr-parse-error

To clear all counters in MLR packet error parsing, use the **clear cs7 mlr-parse-error** command in privileged EXEC mode.

clear cs7 mlr-parse-error

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.4(15)SW8	This command was introduced.
	12.2(33)IRH	

Examples	The following example shows how to clear all counters in MLR packet error parsing: <code>clear cs7 mlr-parse-error</code>

Related Commands	Command	Description
	—	—

clear cs7 msu-rates

To clear the MSU traffic rate values, use the **clear cs7 msu-rates** command at the privileged EXEC mode.

clear cs7 msu-rates [**peak** *slot cpu*]

Syntax Description

peak	Indicates the maximum peak values for MSU traffic rate.
<i>slot</i>	Slot number.
<i>cpu</i>	Bay or processor number.

Defaults

None.

Command Modes

privileged EXEC mode

Command History

Release	Modification
12.4(15)SW7	The peak option was introduced.
12.2(33)IRG	

Usage Guidelines

This command resets all the counters associated with MSU traffic rate. Use the peak option to clear the maximum values of MSU traffic rate for a specified slot and CPU processor.

Examples

The following example shows how to clear the maximum MSU traffic rate values:

```
clear cs7 msu-rates peak 1 0
```

Related Commands

Command	Description
show cs7 msu-rates	Displays information about configured SS7 MSU rates.

clear cs7 mtp3 event-history

To clear the MTP3 event-history log, use the **clear cs7 mtp3 event-history** EXEC command.

clear cs7 [*instance-number*] **mtp3 event-history**

Syntax Description	<i>instance-number</i> Instance number.

Defaults	None.

Command Modes	EXEC

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	To collect MTP3 problem determination information for further analysis of a known problem, clear the event history just before a known problem is about to recur. Do not clear event history otherwise, because vital information will be lost. This command can be issued either globally or on an instance.

Examples	The following example shows how to clear the MTP3 event history log: <pre>clear cs7 mtp3 event history</pre>

Related Commands	Command	Description
	cs7 mtp3 event-history	Specifies the maximum number of events to store in memory.
	show cs7 mtp3 event-history	Displays logged ITP MTP3 events.

clear cs7 pointcode event-history

To clear the CS7 M3UA or SUA point code measurements, use the **clear cs7 pointcode event-history** privileged EXEC command.

clear cs7 [*instance-number*] **pointcode event-history**

Syntax Description

<i>instance-number</i>	Instance number.

Defaults

None.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Examples

The following example shows how to clear the CS7 point code measurements:

```
clear cs7 pointcode event-history
```

Related Commands

Command	Description
show cs7 point-codes event-history	Displays the point codes that this router is responding to.

clear cs7 offload mtp3

To clear all counters maintained by the MTP3 offload feature, use the **clear cs7 offload mtp3** EXEC command.

clear cs7 offload mtp3 *slot*

Syntax Description	<i>slot</i> Line card slot number.

Defaults	None.

Command Modes	EXEC

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples	The following example shows how to clear all MTP3 offload counters for line card 0: clear cs7 offload mtp3 0

Related Commands	Command	Description
	show cs7 offload detailed	Displays the current status, counters, and events maintained by the MTP3 offload feature.

clear cs7 statistics

To clear statistics concerning MSU throughput on a linkset basis, use the **clear cs7 statistics** EXEC command.

clear cs7 [*instance-number*] **statistics** [*linkset* [*link*]]

Syntax Description

<i>instance-number</i>	Instance number.
<i>linkset</i>	Name of the linkset.
<i>link</i>	Number of the link.

Defaults

None.

Command Modes

EXEC

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

This command can be issued either globally or on an instance.

The ITP statistics are helpful in debugging and analyzing MSU throughput. The **clear cs7 statistics** command can be used by a customer or TAC engineer any time a starting point is needed to see statistics counted.

The ITP keeps the following statistics: MSU In, MSU Out, LSSU In, LSSU Out, ByteCnt In, ByteCnt Out, and Drop.

You can display statistics with the **show cs7 linkset statistics** command.

Examples

The following example shows how to reset to zero all counters for all linksets, then reset to zero all counters on the linkset named rosebud:

```
clear cs7 statistics
!resets all counts to zero for all linksets)
clear cs7 statistics rosebud
!resets all counts on the linkset rosebud to zero)
```

Related Commands

Command	Description
show cs7 linkset statistics	Displays ITP statistics.

clear cs7 tcap statistics

To clear CS7 TCAP statistics, use the **clear cs7 tcap statistics** EXEC command.

clear cs7 [*instance-number*] **tcap statistics**

Syntax Description	<i>instance-number</i> Instance number.						
Defaults	None.						
Command Modes	EXEC						
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>12.2(18)IXA</td><td rowspan="3">This command was introduced.</td></tr><tr><td>12.4(11)SW</td></tr><tr><td>12.2(33)IRA</td></tr></table>	Release	Modification	12.2(18)IXA	This command was introduced.	12.4(11)SW	12.2(33)IRA
Release	Modification						
12.2(18)IXA	This command was introduced.						
12.4(11)SW							
12.2(33)IRA							
Usage Guidelines	This command can be issued either globally or on an instance.						
Examples	The following example shows how to clear all CS7 TCAP statistics: <pre>clear cs7 tcap statistics</pre>						
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>show cs7 tcap</td><td>Displays TCAP information.</td></tr></table>	Command	Description	show cs7 tcap	Displays TCAP information.		
Command	Description						
show cs7 tcap	Displays TCAP information.						

clear ip sctp association

An SCTP (Stream Control Transmission Protocol) association is a protocol relationship between SCTP endpoints. The relationship consists of two endpoints and the protocol state information.

To clear the errors, statistics, and monitor values for the specified SCTP association, use the **clear ip sctp association** EXEC command.

clear ip sctp association *assoc-id*

Syntax Description	<i>assoc-id</i> Association identifier. Shows the associated ID statistics for the SCTP association.							
Defaults	None.							
Command Modes	EXEC							
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>12.2(18)IXH</td><td rowspan="3">This command was introduced.</td></tr><tr><td>12.4(15)SW3</td></tr><tr><td>12.2(33)IRA</td></tr></table>		Release	Modification	12.2(18)IXH	This command was introduced.	12.4(15)SW3	12.2(33)IRA
Release	Modification							
12.2(18)IXH	This command was introduced.							
12.4(15)SW3								
12.2(33)IRA								
Usage Guidelines	The clear ip sctp association command is related to the general Cisco IOS command clear ip sctp statistics .							
Examples	The following example shows how to clear the SCTP association identified as 0x00010001: clear ip sctp association 0x00010001							
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>show ip sctp</td><td>Displays SCTP statistics.</td></tr><tr><td>clear ip sctp statistics</td><td>Resets all SCTP global counters and clears counters for all SCTP associations.</td></tr></table>		Command	Description	show ip sctp	Displays SCTP statistics.	clear ip sctp statistics	Resets all SCTP global counters and clears counters for all SCTP associations.
Command	Description							
show ip sctp	Displays SCTP statistics.							
clear ip sctp statistics	Resets all SCTP global counters and clears counters for all SCTP associations.							

c-link-linkset

A C-link links connecting mated STPs. To tag a linkset as a C-link linkset, use the **c-link-linkset** **cs7** linkset configuration submode command. To disable the command, use the **no** form of this command.

c-link-linkset [secondary]

no c-link-linkset [secondary]

Syntax Description	secondary (Optional) C-link linkset to the connected secondary point code.

Defaults	This command is disabled.

Command Modes	cs7 linkset configuration submode

Command History	Release	Modification
	12.2(18)IXG	This command was introduced.
	12.4(15)SW2	
	12.2(33)IRB	

Usage Guidelines	You can configure one or two C-link linksets. Two linksets comprise a primary linkset and a secondary linkset. Both linksets are treated equally; “secondary” means only that one end of the link is a secondary point code (when multiple local PCs are configured). If two C-link linksets exist and only one has been tagged, when MTP circular route detection (CRD) is configured, the links in the untagged linkset will fail. The links fail because configuring CRD also turns on OPC verification, which drops MSUs with an OPC equal to the mate's PC if they do not arrive on a C-link. The verification process also drops signaling link test messages. To avoid link failures, we recommend that all changes to C-link linkset configuration be made while CRD is turned off.

Examples	The following example shows the configuration of the C-link linkset: <pre>cs7 instance 0 linkset lsnam c-link-linkset</pre>

clock source (controller)

To set the clock source, use the **clock source** command in controller configuration mode. To restore the clock source to its default setting, use the **no** form of this command.

clock source { **bits** | **line** } { **primary** | **secondary** *priority* } | { **free-running** | **internal** }

no clock source

Syntax Description

bits	Clocking for all nodes is derived from one designated source.
line	Clocking is derived from the external source to which the port is connected.
primary	Primary source of clock.
secondary	Secondary source of clock.
<i>priority</i>	Priority of the clock source. The valid range is 1 to 8.
free-running	A free-running clock derived from the oscillator on the motherboard.
internal	Clocking is derived from the controller's internal phase-locked loop (PLL).

Defaults

The default clock source is **line**.

Command Modes

Controller configuration

Command History

Release	Modification
12.2(18)IXA	This command was modified to include the bits keyword and the <i>priority</i> argument.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

A controller that is configured for BITS clocking cannot be used to carry data. If BITS clocking has been set, no channel groups can be configured. If channel groups have been configured, BITS cannot be configured.

Examples

The following example shows how to specify the BITS clock source as the primary clock:

```
controller t1 4/0/7
 clock source bits primary
```

Related Commands

Command	Description
framing	Selects the frame type for the T1 or E1 data line.

clock source (interface)

To set the clock source, use the **clock source** command in interface configuration mode. To restore the clock source to its default setting, use the **no** form of this command.

clock source { **common** | **internal** | **line** } *interface-number*

no clock source

Syntax Description	common	Interface clocks its transmitted data from a common clock source.
	internal	Interface clocks its transmitted data from its internal clock.
	line	Interface clocks its transmitted data from a clock recovered from the line's receive data stream. This source is the default.
	<i>interface-number</i>	Specific physical link or port number of the common clock source. Valid range is 0 to 7.

Defaults The default clock source is **line**.

Command Modes Interface configuration

Command History	Release	Modification
	12.4(11)SW	This command was introduced.
	12.2(33)IRA	

Usage Guidelines



Caution

You cannot configure the clock source for an ATM interface when the interface is in the administratively down state. The clock source may revert to the original clock source when the interface becomes active.

The **common** keyword is used as part of a configuration that provides BITS clocking to SS7 ATM high-speed links (HSL). A BITS clock is delivered, via a T1 crossover cable, *from* an SS7 port adapter controller that has been configured as the primary BITS clock *to* a T1 Inverse Multiplexing for ATM (IMA) port adapter interface. The IMA port adapter interface receives the BITS clock source for all other interfaces on that IMA port adapter. All other interfaces on the IMA port adapter accept the BITS clock by specifying **clock source common** *interface-number*, where *interface-number* is the IMA port adapter interface that is connected by a crossover cable to the SS7 port adapter.

Examples

The following example shows how to provide BITS clocking to ATM HSLs. Controller 0 of the SS7 port adapter is configured as the primary source of the BITS clock. Controller 1 of the SS7 port adapter is configured as the secondary source. Controller 2 of the SS7 port adapter is connected to the IMA port adapter interface 0 with a T1 crossover cable and provides the BITS clock to the IMA.

clock source (interface)

```
controller T1 2/0/0
  clock source bits primary
  description PRIMARY BITS CLOCK RCVD

controller T1 2/0/1
  clock source bits secondary 1
  description SECONDARY BITS CLOCK RCVD

controller T1 2/0/2
  clock source internal
  description PROVIDES BITS CLOCK TO T1 ATM12/0/0
  description INTERFACE IS CONNECTED TO ATM12/0/0

interface ATM12/0/0
  no ip address
  no ima-group
  no atm ilmi-keepalive
  description RECEIVES BITS CLOCK SOURCE FOR ALL INTERFACES ON THIS IMA PA
  description INTERFACE IS CONNECTED TO T1 2/0/3

interface ATM12/0/1
  clock source common 0
  atm nni
  pvc 0/5 qsaal

interface ATM12/0/2
  clock source common 0
  atm nni
  pvc 0/5 qsaal
```

congestion-mode defer-to-backup (cs7 mlr result)

With this command, **congestion-mode** specifies the occurrence of local congestion and **defer-to-backup** specifies the option of using a backup server.

To choose backup servers when all primary servers are unavailable or congested, use the **congestion-mode defer-to-backup** command in cs7 mlr result configuration mode. To return to the default backup server selection scheme, use the **no** form of this command.

congestion-mode defer-to-backup

no congestion-mode defer-to-backup

Syntax Description

This command has no arguments or keywords.

Defaults

The backup server is used when the primary server is unavailable, and the presence of congestion is not recognized as a factor.

Command Modes

cs7 mlr result configuration

Command History

Release	Modification
12.2(18)IXH	This command was introduced.
12.4(15)SW3	
12.2(33)IRC	

Usage Guidelines

This same command configured in SMS groups sets congestion as a factor in determining the server chosen for SMS results.

Examples

The following example shows how to enable congestion as a factor in the MLR backup server choice:

```
cs7 instance 1 mlr result mo-proxy mode wrr
  congestion-mode defer-to-backup
  pc 1.16.0 ssn 8 weight 5
  pc 3.2.3 ssn 8 weight 0
```

Related Commands

Command	Description
cs7 mlr result	Enters cs7 mlr result configuration mode.
cs7 sms offload	Enables SMS-MO Proxy and SMSNot Proxy offload.
pc (cs7 mlr result)	Specifies the destination point code.

congestion-mode defer-to-backup (cs7 sms group)

With this command, **congestion-mode** specifies the occurrence of local congestion and **defer-to-backup** specifies the option of using a backup server.

To choose backup servers when all primary servers are unavailable or congested, use the **congestion-mode defer-to-backup** command in cs7 sms group configuration mode. To return to the default backup server selection scheme, use the **no** form of this command.

congestion-mode defer-to-backup

no congestion-mode defer-to-backup

Syntax Description

This command has no arguments or keywords.

Defaults

The backup server is used when the primary server is unavailable, and the presence of congestion is not factored into using the backup server.

Command Modes

cs7 sms group configuration

Command History

Release	Modification
12.2(18)IXH	This command was introduced.
12.4(15)SW3	
12.2(33)IRC	

Usage Guidelines

This same command configured in MLR result groups sets congestion as a factor in determining the server chosen for results.

Examples

The following example shows how to enable congestion as a factor in the backup server choice:

```
cs7 sms group SMSCGRP smsc
  congestion-mode defer-to-backup
pc 1.16.0 ssn 8 weight 5
pc 3.2.3 ssn 8 weight 0
```

Related Commands

Command	Description
cs7 sms group	Enters cs7 sms group configuration mode.
cs7 sms offload	Enables SMS-MO Proxy and SMSNot Proxy offload.
pc (cs7 sms result)	Specifies the destination point code.

cookie-life (cs7 local peer)

To configure the valid cookie life of an SCTP association, use the **cookie-life** command in cs7 local-peer configuration submode. To return to the default congestion threshold, use the **no** form of this command.

cookie-life *cookie-life-milliseconds*

no cookie-life *cookie-life-milliseconds*

Syntax Description	<i>cookie-life-milliseconds</i> The lifespan of the cookie used in the SCTP handshake in milliseconds (5000-120000).

Defaults	5000 milliseconds (or 5 seconds)

Command Modes	cs7 local peer configuration mode

Command History	Release	Modification
	12.2(33)IRE	This command was introduced.

Usage Guidelines	The cookie is part of the four-step handshake procedure that occurs during the SCTP association start up. The lifespan of this cookie is an SCTP parameter. You can tune this parameter for your network with the cookie-life command.

Examples	The following example shows the valid cookie life of an SCTP association set for 20 seconds:

```
cs7 multi-instance
cs7 instance 0 variant ANSI
cs7 instance 0 network-name ANSI
cs7 instance 0 point-code 6.0.1
cs7 instance 0 secondary-pc 6.0.2
cs7 instance 0 capability-pc 6.0.3
cs7 instance 0 description ANSI:6.0.1

cs7 instance 2 variant ITU
cs7 instance 2 network-name ITU
cs7 instance 2 point-code 6.2.1
cs7 instance 2 secondary-pc 6.2.2
cs7 instance 2 capability-pc 6.2.3
cs7 instance 2 description ITU:6.2.1
!
cs7 local-peer 42411 offload 3 4
  local-ip 192.170.88.30
  local-ip 192.171.88.30
  sctp-rfc-version 4960
  cookie-life 2000
```

Related Commands	Command	Description
	cs7 local-peer	Specifies the local peer.
	sctp-rfc-version (cs7 local peer)	Specifies SCTP RFC 2960 or SCTP RFC 4960.

cookie-life (cs7 m3ua)

To configure the valid cookie life of an SCTP association, use the **cookie-life** command in cs7 m3ua configuration submode. To return to the default congestion threshold, use the **no** form of this command.

cookie-life *cookie-life-milliseconds*

no cookie-life *cookie-life-milliseconds*

Syntax Description	<i>cookie-life-milliseconds</i>	The lifespan of the cookie used in the SCTP handshake in milliseconds (5000-120000).

Defaults	5000 milliseconds (or 5 seconds)

Command Modes	cs7 m3ua submode configuration

Command History	Release	Modification
	12.2(33)IRE	This command was introduced.

Usage Guidelines	The cookie is part of the four-step handshake procedure that occurs during the SCTP association start up. The lifespan of this cookie is an SCTP parameter. You can tune this parameter for your network with the cookie-life command.

Examples	The following example shows the valid cookie life of an SCTP association set for 20 seconds on the M3UA port 9000:

```
router#show cs7 m3ua 9000
Sigtran M3UA RFC number: 4666

M3UA Local port: 9000          State: active          SCTP instance handle: 9000
Local ip address:              117.117.200.1
                               118.118.200.1
Number of active M3UA peers:   16
Max number of inbound streams allowed: 17
Local receive window:         64000
Max init retransmissions:      8
Max init timeout:              1000 ms
Unordered priority:            equal
Extended UPU support:          disabled
Handling DUPU from ASPs:       disabled
Offload to linecard:           Yes      Slot: 8 1
SCTP defaults for new associations
Transmit queue depth: 1000      Cumulative sack timeout: 200 ms
Assoc retransmissions: 10       Path retransmissions: 4
Minimum RTO: 1000 ms          Maximum RTO: 1000 ms
Bundle status: on              Bundle timeout: 5 ms
Keep alive status: true        Keep alive timeout: 30000 ms
```

```

Initial cwnd:          3000          Idle cwnd rate:          50
Retrans cwnd rate:     50            Retrans cwnd mode:       RFC
FastRetrans cwnd rate: 50            SCTP RFC Version:        2960
Cookie Life:           20000

```

The following example shows how information on the configured cookie life is also displayed with the **show running-config** command:

```

router#show running-config
!
cs7 m3ua 9000 offload 8 1
local-ip 117.117.200.1
local-ip 118.118.200.1
cookie-life 20000
!

```

Related Commands

Command	Description
cs7 m3ua	Specifies the local port number for M3UA and enter m3ua submode.
sctp-rfc-version (cs7 m3ua)	Specifies SCTP RFC 2960 or SCTP RFC 4960.
show cs7 m3ua	Displays M3UA information.

cookie-life (cs7 sua)

To configure the valid cookie life of an SCTP association, use the **cookie-life** command in cs7 sua configuration submode. To return to the default congestion threshold, use the **no** form of this command.

cookie-life *cookie-life-milliseconds*

no cookie-life *cookie-life-milliseconds*

Syntax Description	<i>cookie-life-milliseconds</i> The lifespan of the cookie used in the SCTP handshake in milliseconds (5000-120000).

Defaults	5000 milliseconds (or 5 seconds)

Command Modes	cs7 sua submode configuration

Command History	Release	Modification
	12.2(33)IRE	This command was introduced.

Usage Guidelines	The cookie is part of the four-step handshake procedure that occurs during the SCTP association start up. The lifespan of this cookie is an SCTP parameter. You can tune this parameter for your network with the cookie-life command.

Examples	The following example shows the valid cookie life of an SCTP association set for 20 seconds on the SUA port 9100:

```
router#show cs7 sua 9100
Sigtran SUA RFC number: 3868

SUA Local port: 9100          State: active          SCTP instance handle: 9100
Local ip address:              119.119.200.1
                                120.120.200.1
Number of active SUA peers:    16
Max number of inbound streams allowed: 17
Local receive window:         64000
Max init retransmissions:      8
Max init timeout:              1000 ms
Unordered priority:            equal
Offload to linecard:           Yes      Slot: 9 0
SCTP defaults for new associations
Transmit queue depth: 1000      Cumulative sack timeout: 200 ms
Assoc retransmissions: 10       Path retransmissions: 4
Minimum RTO: 1000 ms           Maximum RTO: 1000 ms
Bundle status: on               Bundle timeout: 5 ms
Keep alive status: true         Keep alive timeout: 30000 ms
Initial cwnd: 3000              Idle cwnd rate: 50
Retrans cwnd rate: 50           Retrans cwnd mode: RFC
```

```
FastRetrans cwnd rate: 50          Sctp Rfc Version: 2960
Cookie Life: 20000
```

The following example shows how information on the configured cookie life is also displayed with the **show running-config** command:

```
router#show running-config
!
cs7 sua 9100 offload 9 0
local-ip 119.119.200.1
local-ip 120.120.200.1
cookie-life 20000
!
```

Related Commands

Command	Description
cs7 sua	Specifies the local port number for SUA and enter cs7 sua submode.
sctp-rfc-version (cs7 sua)	Specifies SCTP RFC 2960 or SCTP RFC 4960.

cs7 acc-audit-timer

To configure CS7 accounting timer and cp measurement timer, use the **cs7 acc-audit-timer** command in global configuration mode. To remove the configuration, use the default value of the timer, 10 seconds.

cs7 acc-audit-timer *seconds*

cs7 acc-audit-timer 10

Syntax Description	<i>seconds</i>	Timer value in seconds. Range is 5 to 300 seconds.

Defaults	The default timer value is 10 seconds.

Command Modes	Global configuration

Command History	Release	Modification
	12.4(15)SW9	This command was introduced.
	12.2(33)IRI	

Usage Guidelines	This command is configurable for only instance zero. Do not use the no form of this command. To reset the timer value, issue this command with the time value of 10 seconds. To check the value of the timer, issue the show cs7 offload mtp3 detailed command. If configured on instances 1 to 7, there is no impact to ITP. To prevent memory depletion on the SUP, the recommended value for this timer is 20 seconds on a system loaded with 4 SAMIs.

Examples	The following example shows how to set the timer to 100 seconds: <pre>cs7 instance 0 acc-audit-timer 100</pre>

Related Commands

cs7 accounting

To configure CS7 accounting options, use the **cs7 accounting** command in global configuration mode. To remove the configuration, use the **no** form of this command.

cs7 accounting { **checkpoint-interval** *min* | **checkpoint-limit** *entries* | **global-gtt** | **global-mtp3** | **global-unrouteable** | **global-xua** | **global-virtual-linkset** | **gtt-checkpoint-interval** *gtt_min* }

Syntax Description		
<i>min</i>		An accounting checkpoint interval. The range is 1 to 3600 minutes. The default is 5 minutes.
<i>entries</i>		Maximum number of entries for all accounting tables. The range is 5000 to 1000000 entries.
global-gtt		Enables GTT accounting on all linksets. Same effect as specifying the gtt-accounting command on all linksets.
global-mtp3		Enables MTP3 accounting on all linksets. Same effect as specifying the accounting command on all linksets.
global-xua		Enables xUA normal accounting on all xUA (M3UA and SUA) ASes. This setting allows counting of the M3UA payload data messages received from and sent to M3UA ASes. This setting also allows the counting of the number of CLDT/CLDR packets received from and sent to the SUA AS.
global-unrouteable		Enables unroutable accounting on all linksets and xUA ASes.
global-virtual-linkset		Enables virtual linkset accounting globally, including normal MTP3 accounting, unroutable accounting, and SCCP accounting. This keyword controls the collection of all types of accounting information for virtual linksets. After it is enabled, information for traffic sent and received over virtual linksets appears in the MTP3, unroutable, and GTT accounting tables.
<i>gtt_min</i>		GTT accounting checkpoint interval. The range is 1 to 3600 minutes. The default is 5 minutes.

Defaults

The default accounting checkpoint interval is 5 minutes.
The default GTT accounting checkpoint interval is 5 minutes.

Command Modes

Global configuration

Command History

Usage Guidelines

The **global-gtt**, **global-mtp3**, and **global-unrouteable** keywords have the same effect.

Examples

The following example shows how to set the GTT accounting checkpoint interval to 30 minutes:

```
cs7 accounting gtt-checkpoint-interval 30
```

Related Commands

Command	Description
show cs7 accounting	Displays ITP accounting details.

cs7 address-table replace

To replace an already configured or new address table with one specified in a URL, use the **cs7 address-table replace** command in global configuration mode. To remove the line from the configuration, use the **no** form of this command.

cs7 address-table replace { **mlr** | **sms** } *table-name url*

no cs7 address-table replace { **mlr** | **sms** } *table-name url*

Syntax Description	mlr	Specifies table type mlr .
	sms	Specifies table type sms .
	<i>table-name</i>	Identifies the existing address table that is to be replaced.
	<i>url</i>	User-assigned local or remote location representing the filename and path from which the file will be replaced.

Defaults None.

Command Modes Global configuration

Command History

Usage Guidelines The replacement does not impact routing until the entire replacement address table is loaded successfully. If an error occurs, the old address table (if present) remains intact. Each time an address table is replaced, the corresponding **load** command is added to the running configuration.

Examples The following command shows how to replace an SMS address table named addrtbl1 with the file at disk0:smsaddrtbl:

```
cs7 address-table replace sms addrtbl1 disk0:smsaddrtbl
```

Related Commands	Command	Description
	load (cs7 sms address-table)	Specifies the file to load on startup.

cs7 as

To define an application server (AS), use the **cs7 as** command in global configuration mode. To inactivate an AS and delete the AS definition from configuration, use the **no** form of this command.

cs7 [**instance** *instance-number*] **as** *as-name* { **m3ua** | **sua** | **sgmp** }

no cs7 [**instance** *instance-number*] **as** *as-name* { **m3ua** | **sua** | **sgmp** }

Syntax Description

instance	(Optional) Associates an application server (AS) with a defined instance.
<i>instance-number</i>	Instance number. The valid range is 0 to 7. The default instance is 0.
<i>as-name</i>	A unique name that identifies an AS for configuration and monitoring.
m3ua	Indicates an M3UA AS.
sua	Indicates an SUA AS.
sgmp	Indicates an SGMP AS.

Defaults

None.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)IRA	This command was introduced.
12.2(33)IRD	The sgmp keyword was introduced.

Usage Guidelines

The as-name may be up to 12 characters long. The first character must be alphabetic. The AS name cannot duplicate an AS route name and cannot match the following reserved keywords: **m3ua**, **sua**, **all**, **operational**, **active**, **statistics**, **bindings**, or **detail**.

You must configure the ASPs before you configure the AS.

You must specify both a routing key and at least one ASP in as submode. An incomplete AS definition will be deleted.

You cannot delete an AS that is currently defined in an AS route. You must first remove this AS from the AS route.

This command is not instance related and cannot be specified with the **instance** keyword.

Issuing the **cs7 as** command enables cs7 as submode. In this submode for M3UA and SUA ASs, you can configure the routing key, ASP, traffic-mode AS parameters, and QoS class. You cannot modify the parameters of an active AS.

In the AS submode for SGMP, you can only configure the **cs7 mated-sg**, **shutdown**, and **routing-key rcontext** commands. SGMP is a common channel and SGMP AS configuration requires a routing-context value. The routing-context value can be any value that does not conflict with other routing-keys. Mated ITPs must use same SGMP routing key. You cannot modify the parameters of an active AS.

When an AS is not active, the ASPs associated with the AS are also not active for this routing context. This will generate a Notify message.

Examples

The following example shows how to configure an M3UA AS named BLUE:

```
cs7 as BLUE m3ua
```

The following example shows how to configure the AS named BLUE for SUA use:

```
cs7 as BLUE sua
```

The following example shows how to configure the instance 0 AS named provence for SGMP use:

```
cs7 instance 0 as provence sgmp
```

Related Commands

Command	Description
asp	Associates ASPs to an AS.
burst-recovery-timeout	Specifies the amount of time allowed for an association to recover from a burst of traffic due to failover.
cs7 asp	Defines an ASP.
cs7 m3ua	Specifies the local port number for M3UA.
cs7 mtp3 tuning rx-congestion-threshold	Enables multiple instances of a variant and network indicator combination.
cs7 sua	Specifies the local port number for SUA.
qos-class (cs7 as)	Configures a QoS class for the packets sent to the ASPs in this AS.
recovery-timeout	Specifies the recovery timeout value.
show cs7 as	Displays AS and routing key information.
cs7 sgmp	Enables SGMP offloading.
cs7 mated-sg	Configure a connection to a mated SG.
routing-key (cs7 as)	Describes a set of SS7 parameters and parameter values that uniquely define the range of signaling traffic to be handled by a particular AS.

cs7 asp

To specify an application server process and enable cs7 asp submode, use the **cs7 asp** command in global configuration mode. To delete an ASP definition from the configuration, use the **no** form of this command.

cs7 asp *asp-name* *remote-port* [*local-port*] [**m3ua** | **sua**]

no cs7 asp *asp-name* *remote-port* [*local-port*] [**m3ua** | **sua**]

Syntax Description

<i>asp-name</i>	A unique name that identifies an ASP for configuration and monitoring. This name may be up to 12 characters long. The first character must be alphabetic. The ASP name cannot match a reserved keyword (such as m3ua , sua , all , operational , active , statistics , bindings , or detail).
<i>remote-port</i>	Remote port number of the ASP. Valid range is 0 to 65535. This argument is used for validation. The SCTP connection requests from the ASP must come in with this remote port number. If two ASPs are configured with the same remote IP address, then the remote port and the local port are used to differentiate between the two ASPs. If a remote port of 0 is configured, the ASP matches on any remote port (providing <i>remote-ip</i> and <i>local-port</i> match). The remote IP, remote port, and local port combination must be unique for each configured ASP.
<i>local-port</i>	Local port number of the ITP.
m3ua	(Optional) Indicates an M3UA ASP. This value must match the protocol of the specified local port.
sua	(Optional) Indicates an SUA ASP. This value must match the protocol of the specified local port.

Defaults

None.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)IRA	This command was introduced.

Usage Guidelines

The **cs7 asp** command defines an ASP and enables cs7 asp submode. The remote IP address and remote port number combination must be unique for each configured ASP. An SCTP association for an ASP will fail if the ASP is not associated with an AS. An ASP may be associated with multiple ASes.

You can modify the remote port, local port, and protocol of a previously configured ASP. If you enter a valid remote port, local port, and protocol combination, the ASP is updated if its SCTP association is down. You cannot change both the local port and protocol of an ASP that is defined in an AS.

The **no cs7 asp** command deletes this ASP definition from the configuration. If an association is up with this ASP, you must first shut down the ASP and remove the ASP from all CS7 AS definitions before this command can be deleted from the configuration.

In cs7 asp submode, you can disable the ASP by entering the **shutdown** or **block** command. New SCTP associations are rejected when the ASP is in shutdown mode.

You cannot delete an ASP that is currently configured in an AS. You must first remove the ASP from the AS configuration.

You must specify at least one remote IP address in cs7 asp submode or the incomplete ASP definition will be deleted.

This command is not instance related and cannot be specified with the **instance** keyword.

Examples

The following example shows how to configure an M3UA ASP named ASP1 with remote port number 5000 and local port number 5000:

```
cs7 m3ua 5000
  local-ip 1.1.1.1
!
cs7 asp ASP1 5000 5000 m3ua
  remote-ip 2.2.2.2
```

Related Commands

Command	Description
assoc-retransmit (cs7 asp)	Configures the maximum number of consecutive retransmissions for the association.
block	Allows a new SCTP association to be established but prevents the ASP from going into the active state.
bundling (cs7 asp)	Specifies the maximum amount of time, in milliseconds, that SCTP will wait for messages for bundling.
cs7 as	Defines an application server.
cs7 qos class	Defines a CS7 QoS class.
cumulative-sack (cs7 asp)	Specifies the cumulative selective acknowledgment timeout value, in milliseconds.
keepalive (cs7 asp)	Specifies the keepalive interval, in milliseconds.
match any (cs7 asp)	Assigns a QoS class number to all inbound traffic.
match si (cs7 asp)	Assign a QoS class number to any inbound packet that has a specific service indicator.
path-retransmit (cs7 asp)	Specifies the maximum number of path retransmissions on a remote address for the association.
qos-class (cs7 asp)	Defines a QoS class for the packets sent to this ASP.
remote-ip (cs7 asp)	Configures a remote IP address to associate incoming packets from an ASP to a configured ASP.
retransmit-timeout (cs7 asp)	Specifies the minimum retransmission timeout value for the association.
show cs7 asp	Displays ASP information.
shutdown (cs7 asp)	Disables an ASP without deleting the configuration.
tx-queue-depth (cs7 asp)	Specifies the maximum transmit queue depth for the association.

cs7 audit

To validate and audit the consistency of the content in the files of the line card and main processor, including MLR or GWS configuration files, GWS table files, and MLR address table files, use the **cs7 audit** command in global configuration mode. To disable the feature, use the **no shutdown** command.

```
cs7 audit [timer [timer-minutes]] [gws[sync]][mlr[sync]]
```

```
no cs7 audit [timer [timer-minutes]] [gws[sync]][mlr[sync]]
```

Syntax Description

timer	Signifies the use of the audit interval timer.
<i>timer-minutes</i>	Length of time between audits. The default is 60 minutes.
gws	Enables an audit for GWS. The default is disabled.
mlr	Enables an audit for MLR. The default is disabled.
sync	Matches the SUP and LC configuration.

Defaults

This command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXF	This command was introduced.
12.4(15)SW1	
12.2(33)IRA	

Usage Guidelines

If the audit discovers that the line card has a different configuration from the supervisor engine, the configurations synchronize again from the supervisor to the line card.

Examples

The following example shows how to configure a GWS audit:

```
cs7 audit gws
```

Related Commands

Command	Description
show cs7 audit status	Shows the latest audit begin time, end time, and status.

cs7 billing account

To configure and identify a billing account and enter the cs7 billing account configuration submode, use the **cs7 billing account** command in global configuration mode. To remove an account, use the **no** form of this command.

cs7 [*instance instance*] **billing account** *billing-account-name*

no cs7 [*instance instance*] **billing account** *billing-account-name*

Syntax Description	billing account	The representation of a billable entity.
	<i>billing-account-name</i>	A unique name that identifies an billing account for configuration and accounting.
Defaults	None	
Command Modes	Global configuration	
Command History	Release	Modification
	12.4(15)SW4	This command was introduced.
	12.2(33)IRD	
Usage Guidelines	A billing account contains information that matches billing accounting criteria. You can specify the detailed criteria in the config-accnt-entry submode after typing this command.	
Examples	The following command shows how to configure a billing account named Alpha for the instance 0: <pre>cs7 instance 0 billing account Alpha</pre>	
Related Commands	Command	Description
	cs7 billing pc-table	Configures a pc-table for the billing account.
	cs7 billing options	Configures options for billing.
	cs7 billing load	Specifies the billing configuration file to load.

cs7 billing load

To load a configuration file for a billing account, use the **cs7 billing load** command in global configuration mode. To disable the loading, use the **no** form of this command.

cs7 billing load *location* [**execute**]

no cs7 billing load *location* [**execute**]

Syntax Description

<i>location</i>	The URL or disc location of the configuration file.
execute	(Optional) Immediately loads the configuration file on the ITP.

Defaults

The configuration file from the URL or disc location will load onto the ITP during the next system reboot.

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)SW4	This command was introduced.
12.2(33)IRD	

Usage Guidelines

Use this command to configure the file loading URL or disc location for a cs7 billing configuration file.

Examples

The following command shows how to load a configuration from the disc location `disk0:itp_billing`. The file loads during the next reboot of the ITP:

```
cs7 billing load disk0:itp_billing
```

Related Commands

Command	Description
cs7 billing pc-table	Configures a pc-table for the billing account.
cs7 billing options	Configures options for billing.
cs7 billing load	Specifies the billing configuration file to load.

cs7 billing options

To configure user options for the billing account and enter the billing option configuration submode, use the **cs7 billing options** command in global configuration mode. To disable the loading, use the **no** form of this command.

cs7 billing options {*rx-interval seconds* | *rx-per-tx times* | **backstore** *order url* | **bak-file-num** *num*}

no cs7 billing options {*rx-interval seconds* | *rx-per-tx times* | **backstore** *order url* | **bak-file-num** *num*}

Syntax Description

<i>seconds</i>	Seconds of interval for a time of data collection (30-86400).
<i>times</i>	Times of data collection in a data storage interval (3-1024).
<i>order</i>	Order of trying current back storage among all back storages (0-1).
<i>url</i>	The URL location of the back storage file.
<i>num</i>	The backup file number in the data saving destination (1-1024).

Defaults

The default interval for times of data collection is 300 seconds. The default interval for a time of data collection is 5. The default backup file number in the data saving destination is 1.

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)SW4	This command was introduced.
12.2(33)IRD	

Usage Guidelines

This command also enters the cs7 billing option configuration submode.

Examples

The following example configure user options for the billing account and enters the cs7 billing option configuration submode. It also sets the times of data collection at a data storage interval of 12 and a data collection interval of 300 seconds:

```
(config)#cs7 billing options
(config-optns-entry)#rx-per-tx 12
(config-optns-entry)#rx-interval 300
```

Related Commands

cs7 billing pc-table

To configure a point code table used for billing criteria, use the **cs7 billing pc-table** command in global configuration mode. To remove the point code table, use the **no** form of this command.

cs7 [*instance instance-number*] **billing pc-table** *pctbl_name* {**mtp3** | **sccp** | **sms_sccp**}

no **cs7** [*instance instance-number*] **billing pc-table** *pctbl_name* {**mtp3** | **sccp** | **sms_sccp**}

Syntax Description

<i>pctbl_name</i>	Name of the pc table.
mtp3	The first of two protocols you can specify for the pc table.
sccp	The second of two protocols you can specify for pc table.
sms_sccp	The third of three protocols you can specify for pc table.
<i>pctbl_name</i>	Name of the pc table associated with this entry.

Defaults

None.

Command Modes

Global configuration mode

Command History

Release	Modification
12.4(15)SW4 12.2(33)IRD	This command was introduced.
12.4(15)SW6 12.2(33)IRF	The keyword sms_sccp was introduced.

Usage Guidelines

This command enters pc-table configuration submode, which allows you to add table entries. You can associate a pc table with one or more configured billing account entries.

Examples

The following example shows how to configure a billing pc table named *PCTBL_02* with the SCCP protocol on instance 0:

```
cs7 instance 0 billing pc-table PCTBL_02 sccp
```

The following example shows how to configure a billing pc table named *PCTBL_01* with the SMS protocol on instance 0:

```
cs7 instance 0 billing pc-table PCTBL_01 sms_sccp
```

Related Commands

Command	Description
cs7 billing options	Configures options for billing.

Command	Description
cs7 billing load	Specifies the billing configuration file to load.
cs7 billing account	Configures a billing account.

cs7 capability-pc

To configure the capability point code for ITP and its mated node, use the **cs7 capability-pc** command in global configuration mode. To remove the capability point code, use the **no** form of this command.

cs7 [**instance** *instance-number*] **capability-pc** *zone.region.sp*

no cs7 [**instance** *instance-number*] **capability-pc** *zone.region.sp*

Syntax Description	instance	(Optional) Configures the capability point code for a specified instance of the ITP and its mated node.
	<i>instance-number</i>	Instance number. The valid range is 0 to 7. The default instance is 0.
	<i>zone.region.sp</i>	Capability point code.

Defaults The default instance is 0.

Command Modes Global configuration

Command History	Release	Modification
	12.4(15)SW1	This command was introduced.
	12.2(33)IRA	

Usage Guidelines The ITP supports configuring up to 200 capability point codes for each instance. A capability point code must be configured according to the existing point code format. The capability point code functions like an alias for a mated pair of ITPs. For example, for redundancy, a capability point code is assigned to a mated pair of ITPs that share a GTT database. In this case, all SCCP messages are directed to a single “capable” point code and either ITP can handle the processing.

Examples The following example shows excerpts from two separate ITP configurations. Both ITPs are assigned the same capability point code.

```
hostname itpa
cs7 multi-instance
cs7 instance 0 variant itu
cs7 instance 0 point-code 5.100.2
cs7 instance 0 capability-pc 5.100.12
```

```
hostname itpb
cs7 multi-instance
cs7 instance 0 variant itu
cs7 instance 0 point-code 5.100.3
cs7 instance 0 capability-pc 5.100.12
```

Related Commands	Command	Description
	cs7 pmp	Assigns a local point code to an instance.
	cs7 variant	Specifies the variant for an instance.
	cs7 mtp3 tuning rx-congestion-threshold	Enables multiple instances of a variant and network indicator combination.
	show cs7	Displays the ITP basic configuration, including the point code and capability point code.

cs7 clli

A Common Language Location (CLLI) code is an 11-character standardized geographic identifier that uniquely identifies the geographic location of telecommunication equipment. To define a CLLI code for an ITP, use the **cs7 clli** command in global configuration mode. To remove the definition, use the **no** form of this command.

cs7 clli *line*

no clli *line*

Syntax Description	<i>line</i>	A text string used to define a common language location code for the ITP. The string can be from 1 to 11 alphanumeric characters long.

Defaults	None.

Command Modes	Global configuration

Command History	Release	Modification
	12.2(18)IXF	This command was introduced.
	12.4(15)SW1	
	12.2(33)IRA	

Usage Guidelines	The CLLI <i>line</i> value is included on traps that apply to the SS7 resources on the ITP. The value is also used by network management stations. Complete listings of geographical and geopolitical codes can be found in the BR 751-401-xxx series and BR 751-100-055, respectively. This command is not instance related and cannot be specified with the instance keyword.

Examples	The following example shows how to define a common language location code for the ITP: <pre>cs7 clli QSWYNJPIDS5</pre>

Related Commands	Command	Description
	show running config	Displays the contents of the currently running configuration file.

cs7 dcs

A DCS (data collection server) node represents an endpoint that receives a proprietary probeless monitoring protocol (PMP). The protocol relies on UDP and carries copies of sent or received ITP MSUs.

To specify the name for a DCS node and enter cs7 dcs submode, use the **cs7 dcs** command in global configuration mode. To remove the name, use the **no** form of this command.

cs7 dcs *name*

no cs7 dcs *name*

Syntax Description	<i>name</i>	Identifies a name to be associated with this DCS. The name is specified as an alphanumeric string with a maximum of 12 characters.

Defaults	None.

Command Modes	Global configuration

Command History	Release	Modification
	12.4(15)SW3 12.2(33)IRC	This command was introduced.

Usage Guidelines	The DCS node name must be unique among all DCS endpoints. A DCS node represents a probeless monitoring protocol (PMP) endpoint and is uniquely identified by name, IP address, and port number. Each DCS node may contain up to two IP address and port combinations.

Examples	The following example shows how to create a DCS node named dcs1:

```
cs7 pmp
cs7 pmp hold-queue 64 128
cs7 pmp congestion-timer 30
!
cs7 multi-instance
cs7 instance 0 variant ANSI
cs7 instance 0 network-name ANSI
cs7 instance 0 point-code 6.0.1
cs7 instance 0 secondary-pc 6.0.2
cs7 instance 0 capability-pc 6.0.3
cs7 instance 0 description ANSI:6.0.1

cs7 instance 2 variant ITU
cs7 instance 2 network-name ITU
cs7 instance 2 point-code 6.2.1
cs7 instance 2 secondary-pc 6.2.2
cs7 instance 2 capability-pc 6.2.3
cs7 instance 2 description ITU:6.2.1
```

```

!
cs7 dcs dcs1
  remote-ip 209.165.200.225 33500
  local-ip 209.165.200.250 33500
  ping-interval 0
  no shutdown
!
cs7 dcs-group pmpGroup1
  dcs dcs1 0
!
cs7 instance 0 linkset 1.M2PA.6 1.0.1
  pmp
  dcs-group pmpGroup1 all
  accounting
  link 0 sctp 172.18.16.24 209.165.200.490 3000 3000
    context 12
  link 1 sctp 209.165.200.490 209.165.200.270 3001 draft2
    context 13
  link 2 sctp 209.165.200.290 3002 3002
    context 14
  link 3 sctp 209.165.200.490 3003 3003
    context 15

```

Related Commands

Command	Description
cs7 dcs-group	Identifies a name to be associated with a DCS group.
cs7 pmp	Turns probeless monitoring on for all linksets and ASes.
cs7 pmp hold-queue	Sets the integer range of PMP hold queue thresholds.
show cs7 pmp	Displays errors and information about the PMP.
cs7 pmp congestion-timer	Sets the integer range of the PMP congestion timer.
show cs7 dcs-group	Displays information about the DCS group.
show cs7 dcs	Displays information about the DCS node.

cs7 dcs-group

A DCS group is a collection of DCS nodes. To identify a name to be associated with a DCS group, use the **cs7 dcs-group** command in global configuration mode. To remove the name, use the **no** form of this command.

cs7 dcs-group *name*

no cs7 dcs-group *name*

Syntax Description

<i>name</i>	Identifies a name to be associated with this DCS group. The name is specified as an alphanumeric string with a maximum of 12 characters.

Defaults

None.

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)SW3	This command was introduced.
12.2(33)IRC	

Usage Guidelines

A DCS group represents a group of one or more DCS endpoints. Each DCS group may contain up to eight DCS nodes. The DCS group name must be unique among all DCS groups. You cannot delete a DCS group that is referenced by a linkset or AS.

Examples

The following example shows how to create a DCS group named pmpGroup1:

```
cs7 pmp
cs7 pmp hold-queue 64 128
cs7 pmp congestion-timer 30
!
cs7 multi-instance
cs7 instance 0 variant ANSI
cs7 instance 0 network-name ANSI
cs7 instance 0 point-code 6.0.1
cs7 instance 0 secondary-pc 6.0.2
cs7 instance 0 capability-pc 6.0.3
cs7 instance 0 description ANSI:6.0.1

cs7 instance 2 variant ITU
cs7 instance 2 network-name ITU
cs7 instance 2 point-code 6.2.1
cs7 instance 2 secondary-pc 6.2.2
cs7 instance 2 capability-pc 6.2.3
cs7 instance 2 description ITU:6.2.1
!
cs7 dcs dcs1
  remote-ip 209.165.200.225 33500
```

```

local-ip 209.165.200.250 33500
ping-interval 0
no shutdown
!
cs7 dcs-group pmpGroup1
    dcs dcs1 0
!
cs7 instance 0 linkset 1.M2PA.6 1.0.1
    pmp
    dcs-group pmpGroup1 all
    accounting
    link 0 sctp 172.18.16.24 209.165.200.490 3000 3000
        context 12
    link 1 sctp 209.165.200.490 209.165.200.270 3001 draft2
        context 13
    link 2 sctp 209.165.200.290 3002 3002
        context 14
    link 3 sctp 209.165.200.490 3003 3003
        context 15

```

Related Commands

Command	Description
cs7 dcs-group	Identifies a name to be associated with a DCS group.
cs7 pmp	Turns probeless monitoring on for all linksets and ASes.
cs7 pmp hold-queue	Sets the integer range of PMP hold queue thresholds.
cs 7 dcs	Identifies a name to be associated with a DCS node.
cs7 pmp congestion-timer	Sets the integer range of the PMP congestion timer.
show cs7 pmp	Displays errors and information about the PMP.
show cs7 dcs-group	Displays information about the DCS group.
show cs7 dcs	Displays information about the DCS node.

cs7 description

To specify a description of the ITP to be used by the administrator or the network management stations, use the **cs7 description** command in global configuration mode. To remove the text string, use the **no** form of this command.

cs7 [*instance instance-number*] **description** *line*

no cs7 [*instance instance-number*] **description** *line*

Syntax Description

instance	(Optional) Specifies a description of an instance.
<i>instance-number</i>	Instance number. The valid range is 0 to 7. The default instance is 0.
<i>line</i>	Text string description of the ITP. Length can be from 1 to 254 alphanumeric characters.

Defaults

The default instance is 0.

Command Modes

Global configuration

Command History

Release	Modification
	This command was introduced.

Usage Guidelines

The **cs7 description** command provides extra data to help service the point code. This command is not instance related and cannot be specified with the **instance** keyword.

Examples

The following examples show how to include text in a **cs7 description** command:

```
cs7 description "Houston 1.2.1 Primary contact Mike Workhard at 111-222-3456"
```

```
cs7 instance 1 description "Houston 1.2.1 Primary contact Mike Workhard at 111-222-3456"
```

Related Commands

Command	Description
show running config	Displays the contents of the currently running configuration file.

cs7 display-name

The **cs7 display-name** command assigns a descriptive name to an ITP instance. The name is included on traps that apply to the SS7 resources on the ITP instance and is displayed with such information on the NMS.

To define a display name, use the **cs7 display-name** command in global configuration mode. To remove the definition, use the **no** form of this command.

cs7 [*instance instance-number*] **display-name** *line*

no cs7 [*instance instance-number*] **display-name** *line*

Syntax Description

instance	(Optional) Assigns a descriptive name to an ITP instance.
<i>instance-number</i>	Instance number. The valid range is 0 to 7. The default instance is 0.
<i>line</i>	Text string description or the ITP point code formatted as an ASCII string in dotted decimal format. Length can be 30 characters.

Defaults

The default value of *line* is the point code formatted as an ASCII string in the format defined by the **cs7 point-code format** command.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXF	This command was introduced.
12.4(15)SW1	
12.2(33)IRA	

Usage Guidelines

The display name is included on traps that apply to the SS7 resources on the router. The display name is included with information that is sent to the NMS.

Examples

The following examples show how to configure the display name for the ITP:

```
cs7 display-name West-Chicago
```

```
cs7 instance 1 display-name West-Chicago
```

Related Commands

Command	Description
show cs7	Displays the ITP basic configuration, including the point code and capability point code.

cs7 distribute-sccp-sequenced

To enable the ITP to override in-sequence delivery of SSCP traffic, use the **cs7 distribute-sccp-sequenced** command in global configuration mode. To remove the configuration, use the **no** form of this command.

cs7 [*instance instance-number*] **distribute-sccp-sequenced**

no cs7 [*instance instance-number*] **distribute-sccp-sequenced**

Syntax Description	instance	(Optional) Specifies an instance if multiple instances exist. If you have configured the ITP with the multi-instance command, you must use the instance keyword to specify the particular instance. A single instance does not require this keyword.
	<i>instance-number</i>	(Optional) Number of the particular instance. Valid range is 0 to 7. The default instance is 0.

Defaults SSCP traffic is delivered in sequence.

Command Modes Global configuration

Command History	Release	Modification
		This command was introduced.

Usage Guidelines Although some high-level SS7 protocols require in-sequence delivery of packets, other high-level SS7 protocols, such as SCCP and TCAP, do not. When **cs7 distribute-sccp-sequenced** is enabled, the ITP overrides the in-sequence delivery of SCCP traffic.

Examples The following examples show how to enable the **cs7 distribute-sccp-sequenced** command:

```
cs7 distribute-sccp-sequenced
```

or

```
cs7 instance 1 distribute-sccp-sequenced
```

Related Commands	Command	Description
	cs7 mtp3 tuning rx-congestion-threshold	Enables multiple instances of a variant and network indicator combination.
	show cs7	Displays the ITP basic configuration, including the point code and capability point code.

cs7 distribute-sccp-unsequenced

To enable the ITP to determine how to forward packets when in-sequence delivery is not required, use the **cs7 distribute-sccp-unsequenced** command in global configuration mode. To remove the configuration, use the **no** form of this command.

cs7 [*instance instance-number*] **distribute-sccp-unsequenced**

no cs7 [*instance instance-number*] **distribute-sccp-unsequenced**

Syntax Description

instance	(Optional) Specifies on an instance how to forward packets when in-sequence delivery is not required.
<i>instance-number</i>	Instance number. The valid range is 0 to 7. The default instance is 0.

Defaults

Distributed links are included in round-robin selection.

Command Modes

Global configuration

Command History

Release	Modification
	This command was introduced.

Usage Guidelines

Although some high-level SS7 protocols require in-sequence delivery of packets, other high-level SS7 protocols, such as SCCP and TCAP, do not. When **cs7 distribute-sccp-unsequenced** is enabled, the Cisco ITP examines the packet header and determines whether or not that protocol requires in-sequence delivery. If in-sequence delivery is not required, the SLS field value is ignored and the Cisco ITP makes a round-robin selection of the link or ASP on which to forward the packet.

Examples

The following examples show how to enable the **cs7 distribute-sccp-unsequenced** command:

```
cs7 distribute-sccp-unsequenced
```

```
cs7 instance 1 distribute-sccp-unsequenced
```

Related Commands

Command	Description
cs7 mtp3 tuning rx-congestion-threshold	Enables multiple instances of a variant and network indicator combination.
show cs7	Displays the ITP basic configuration, including the point code and capability point code.

cs7 fast-restart

To enable MTP3 fast restart, use the **cs7 fast-restart** command in global configuration mode. To remove the configuration, use the **no** form of this command.

cs7 [*instance instance-number*] **fast-restart**

no cs7 [*instance instance-number*] **fast-restart**

Syntax Description	instance	(Optional) Enables MTP3 fast restart on an instance.
	<i>instance-number</i>	Instance number. The valid range is 0 to 7. The default instance is 0.

Defaults	Fast restart is disabled.

Command Modes	Global configuration

Command History	Release	Modification
		This command was introduced.

Usage Guidelines	When an SP restarts, it normally waits to receive a TRA from each of its adjacent nodes before it marks the links available for passing user traffic. If TRAs are not received from each of the adjacent nodes, the SP eventually times out (30 seconds by default) and starts passing user traffic.

The **cs7 fast-restart** command bypasses this timeout so that the SP does not need to wait for TRAs from the adjacent nodes.

Examples	The following examples show how to enable fast restart:

```
cs7 fast-restart
```

```
cs7 instance 2 fast-restart
```

Related Commands	Command	Description
	cs7 mtp3 tuning rx-congestion-threshold	Enables multiple instances of a variant and network indicator combination.
	show cs7	Displays the ITP basic configuration, including the point code and capability point code.

cs7 fisu-audit-interval

To enable sending FISU messages evenly across the links and specify its time interval, use the **cs7 fisu-audit-interval** command in cs7 configuration mode. To disable this feature, use the **no** form of the command.

cs7 fisu-audit-interval *fisuauditinterval*

no cs7 fisu-audit-interval *fisuauditinterval*

Syntax Description	<i>fisuauditinterval</i> FISU rate audit interval value in seconds. Range is 1 to 25.

Defaults	The <i>fisuauditinterval</i> value is 1.

Command Modes	cs7 configuration

Command History	Release	Modification
	12.2(33)IRH	This command was introduced.

Usage Guidelines	To send the FISU messages evenly across the links configured inside the ITP on the basis of a configured time interval, use the cs7 fisu-audit-interval command in cs7 configuration mode.

Examples	The following example shows how to configure a FISU audit interval of 10 seconds:

```
cs7 fisu-audit-interval 10
```

**Note**

In CS7 group, manual configuration of **cs7 instance dest-instance pc-conversion default orig-instance [no-route]** must not be done at the alternate node if it is already synced from the manager node.

cs7 gtt address-conversion

To configure a global title address conversion table, use the **cs7 gtt address-conversion** command in global configuration mode. To remove the definition, use the **no** form of this command.

cs7 [**instance** *instance-number*] **gtt address-conversion** *table-name*

no cs7 [**instance** *instance-number*] **gtt address-conversion** *table-name*

Syntax Description

instance	(Optional) Configures a global title address conversion table on an instance.
<i>instance-number</i>	Instance number. The valid range is 0 to 7. The default instance is 0.
<i>table-name</i>	Global title address conversion table name. The table name may be 1 to 12 characters long.

Defaults

The default instance is 0.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)SW	This command was introduced.
12.2(33)IRA	

Usage Guidelines

This command specifies a GTT address conversion table name and enables cs7 gtt address conversion table submenu. The address conversion tables are used to specify mappings such as E.212 - E.214 address conversion. After you have defined a GTT address conversion table, you can apply the table on a GTT-selector basis.

Examples

The following command shows how to specify a global title address conversion table named conv1:

```
cs7 gtt address-conversion conv1
```

The following command shows how to specify a global title address conversion table named conv1 for instance 1:

```
cs7 instance 2 gtt address-conversion conv1
```

Related Commands

Command	Description
cs7 mtp3 tuning rx-congestion-threshold	Enables multiple instances of a variant and network indicator combination.
show cs7 gtt address-conversion	Displays CS7 GTT address conversion entries.
update (cs7 gtt address conversion)	Adds, removes, or changes a GTT address conversion entry.

cs7 gtt application-group

To configure a GTT application group and enter the CS7 GTT application group submode, use the **cs7 gtt application-group** command in global configuration mode. To remove the configuration, use the **no** form of this command.

cs7 [*instance instance-number*] **gtt application-group** *name*

no **cs7** [*instance instance-number*] **gtt application-group** *name*

Syntax Description

instance	(Optional) Configures a GTT application group on an instance.
<i>instance-number</i>	Instance number. The valid range is 0 to 7. The default instance is 0.
<i>name</i>	Name of the application group.

Defaults

The default instance is 0.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)SW	This command was introduced.
12.2(33)IRA	

Usage Guidelines

The application group must be defined before you can define the GTA subcommands that use it.

ITP supports performing GTT on two instances for the same MSU. For example, instance 0 can have a GTT application group that specifies the local PC of another instance and the RI set to route on the GT. If this method is used, the MSU may perform a GTT lookup in instance 0 and then translate to the local PC of instance 1. Afterward, the MSU is again translated in instance 1 to its final destination.

Examples

The following example shows how to configure an application group named group1:

```
cs7 gtt application-group group1
```

The following example shows how to configure an application group named group1 on instance 3:

```
cs7 instance 3 gtt application-group group1
```

Related Commands

Command	Description
cs7 mtp3 tuning rx-congestion-threshold	Enables multiple instances of a variant and network indicator combination.
gta app-grp	Translates a GTA to a GTT application group.

Command	Description
multiplicity	Specifies a method for selecting destinations in the application group.
show cs7 gtt application-group	Displays CS7 GTT application group entries.
show cs7 gtt consistency	Displays GTT point codes that do not have routes provisioned for them.
show cs7 gtt gta	Displays CS7 GTT GTA entries.

cs7 gtt concern-pclist

To configure a GTT concerned point code list, use the **cs7 gtt concern-pclist** command in global configuration mode. To remove a point code from an existing concerned point code list, use the **no** form of this command. To delete the concerned point code list, remove all point codes from the list.

cs7 [**instance** *instance-number*] **gtt concern-pclist** *list-name cpc*

no cs7 [**instance** *instance-number*] **gtt concern-pclist** *list-name cpc*

Syntax Description

<i>cpc</i>	Concerned point code, in the form <i>zone.region.sp</i> .
instance	(Optional) Configures a GTT concerned point code list on an instance.
<i>instance-number</i>	Instance number. The valid range is 0 to 7. The default instance is 0.
<i>list-name</i>	Name of the concerned point code list.

Defaults

The default instance is 0.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)SW	This command was introduced.
12.2(33)IRA	

Usage Guidelines

To create a new concerned point code list with one point code, the list name must be unique. Use the following syntax: **cs7 gtt concern-pclist** *listname cpc*

To add a new point code to an existing list, the point code specified must be unique for the list. Use the following syntax: **cs7 gtt concern-pclist** *existinglistname newcpc*

To remove a point code from an existing concerned point code list, the point code must exist. Use the following syntax: **cs7 gtt concern-pclist** *existinglistname cpc*

To delete the concerned point code list, remove all point codes from the list. You cannot delete the last point code in a list if it is referenced by a MAP entry.

Examples

The following example shows how to create a new concerned point code list named mylist with the point code 5.100.5:

```
cs7 gtt concern-pclist mylist 5.100.5
```

The following example shows how to create a new concerned point code list on instance 2 named mylist with the point code 5.100.5:

```
cs7 instance 2 gtt concern-pclist mylist 5.100.5
```

Related Commands	Command	Description
	cs7 mtp3 tuning rx-congestion-threshold	Enables multiple instances of a variant and network indicator combination.
	show cs7 gtt concern-pclist	Displays a CS7 GTT concerned point code list.
	show cs7 gtt map	Displays CS7 GTT MAP entries.

cs7 gtt load

Upon ITP reload, to specify the URL location from which the GTT database is loaded, use the **cs7 gtt load** command in global configuration mode.

cs7 [**instance** *instance-number*] **gtt load** *url* [**execute**]

Syntax Description

<i>url</i>	Path and filename for the GTT load file.
execute	Executes the load immediately.
instance	(Optional) Specifies the URL location from which, on ITP reload, the GTT database for a specified instance will be loaded.
<i>instance-number</i>	Instance number. The valid range is 0 to 7. The default instance is 0.

Defaults

The default instance is 0.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)SW	This command was introduced.
12.2(33)IRA	

Examples

The following example shows, when the ITP is reloaded, how to load the GTT database from a file named gttdata.txt in flash memory:

```
cs7 gtt load flash:gttdata.txt
```

The following example shows, when the ITP is reloaded, how to load the GTT database for instance 4 from a file named gttdata.txt in flash memory:

```
cs7 instance 4 gtt load flash:gttdata.txt
```

Related Commands

Command	Description
cs7 mtp3 tuning rx-congestion-threshold	Enables multiple instances of a variant and network indicator combination.
cs7 save billing-cfg	Saves the CS7 GTT table to a file.

cs7 gtt map

To configure a global title mated application (MAP) entry, use the **cs7 gtt map** command in global configuration mode. To remove the configuration, use the **no** form of this command.

cs7 [**instance** *instance-number*] **gtt map** *ppc pssn* [*flags*] *mult* [*bpc*] [*bssn*]

no cs7 gtt map [**instance** *instance-number*]



Note

You cannot delete any map entry that references another map entry. You must first change all entries that reference it to **sol** before you can delete the entry with the **no cs7 gtt map** command.

Syntax Description

instance	(Optional) Configures a global title mated application (MAP) entry for an instance.
<i>instance-number</i>	Instance number. The valid range is 0 to 7. The default instance is 0.
<i>ppc</i>	Primary SS7 point code, in the form <i>zone.region.sp</i> .
<i>pssn</i>	Primary subsystem number.
<i>flags</i>	One of the following flags: adj —Marks <i>ppc/pssn</i> as adjacent. csplist name —Specifies a concerned point code list name. rrc —Reroutes if congested.
<i>mult</i>	The entry in the MAP table may be modified to work in one of three multiplicities or modes: solitary —Uses a single PC (no alternate if PC and/or SSN is not available). share —Shares load equally across the primary PC/SSN and backup PC/SSN. dominant —Always translates to primary PC/SSN if available, and only translates to backup if primary is unavailable.
<i>bpc</i>	Backup point code, in the form <i>zone.region.sp</i> .
<i>bssn</i>	Backup subsystem number. Valid range is 2 to 255.

Defaults

None.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)SW	This command was introduced.
12.2(33)IRA	

Usage Guidelines

A GTT MAP entry has two main purposes. First, the SCCP application uses it internally to track point code and SSN states such as congestion and availability. Second, it is used to define backups or alternates for a particular PC/SSN combination. An entry in the GTA table that contains a PC and SSN has a corresponding entry in the MAP table. The following rules apply to these entries:

- A backup point code and subsystem must be specified if the mode (multiplicity) is shared or dominant.
- A backup point code and subsystem cannot be specified if the mode (multiplicity) is solitary.
- A PC/SSN entry cannot be deleted if it is being used as a backup by another PC/SSN entry.
- A PC/SSN entry cannot be deleted if it is referenced by an entry in the GTA table.
- The primary and backup point codes cannot be identical.
- A maximum of 9 subsystems for each point code is allowed.
- The PC cannot be equal to the node's own PC.

When a CS7 node changes the RI of a message requiring GTT to "Route on Subsystem," SCRC must look in the GTT MAP table to see if the subsystem is available and to determine which method to use to route the message. ITU-T Q.714 section 5.1 describes the following routing modes:

- **Solitary mode**

The destination subsystem or next translation node is chosen from the one single SCCP node. When that node or its SCCP fails, the SCCP management notifies the SCCP routing control; the traffic toward the **solitary** nodes is discarded or returned if return-option is set.

- Replicated service in **dominant mode**

The next translation node or destination subsystem can be chosen from two SCCP nodes. Traffic toward a specific subdomain (characterized by ranges of global titles) is normally sent to the SCCP of a primary node. When the primary node is inaccessible, the SCCP management notifies the routing control and this traffic is routed to the SCCP of a backup node. As soon as the primary node becomes accessible again, the traffic is again routed to it.

- Replicated service in dynamically load **shared mode**

The next translation node or destination subsystem is chosen from two SCCP nodes. The traffic is dynamically distributed to the next two nodes by the traffic-sending node. The next pair of SCCP nodes receiving the traffic back up each other. If one of the nodes becomes inaccessible, the SCCP management notifies the routing control and the traffic is routed to the other one. As soon as the previously inaccessible node becomes accessible again, the traffic is dynamically distributed to those two nodes again.

In the ANSI domain, GR-82 describes the requirement to support eight different destinations, each having a relative cost, rather than supporting only a primary and secondary node.

Examples

The following example shows how to configure a solitary mated application for instance 2 with PC=1.10.1 and SSN=20:

```
cs7 instance 2 gtt map 1.10.1 20 sol
```

The following example shows how to configure a primary mated application with PC=1.20.1 and SSN=250. The backup is PC=2.20.2 SSN=20 operating in dominant mode.

```
cs7 gtt map 1.20.1 250 dom 2.20.2 250
```

The following example shows how to configure a primary mated application with PC=1.30.1 and SSN=250. The backup is PC=2.30.2 SSN=250 operating in shared mode.

```
cs7 gtt map 1.30.1 250 share 2.30.2 250
```

Related Commands

Command	Description
cs7 gtt map sp	Changes the state of a point code in the MAP table.
cs7 gtt map ss	Changes the state of a subsystem in the MAP table.
cs7 mtp3 tuning rx-congestion-threshold	Enables multiple instances of a variant and network indicator combination.
show cs7 gtt consistency	Displays GTT point codes that do not have routes provisioned for them.
show cs7 gtt map	Displays CS7 GTT MAP entries.

cs7 gtt map sp

To change the state of a point code in the map table, use the **cs7 gtt map** privileged EXEC command.

cs7 [*instance instance-number*] **gtt map sp** {**available** | **prohibited**} *point-code*

Syntax Description	available	Overrides the current state of the point code and sets it to available.
	instance	(Optional) Changes the state of a point code in the map table for an instance.
	<i>instance-number</i>	Instance number. The valid range is 0 to 7. The default instance is 0.
	prohibited	Overrides the current state of the point code and sets it to prohibited.
	<i>point-code</i>	Remote SP point code.

Defaults The default instance is 0.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.4(11)SW 12.2(33)IRA	This command was introduced.

Usage Guidelines Use this command when it becomes necessary (for example, for maintenance purposes) to prevent GTT translated messages from being sent to a point code in the map table.



Note This command is not applied to xUA DPC.

Examples The following example shows how to set the state of the remote point code 2.3.4 in the map table to prohibited:

```
cs7 gtt map sp prohibited 2.3.4
```

The following example shows how to set the state of the remote point code 2.3.4 in the map table for instance 2 to prohibited:

```
cs7 instance 2 gtt map sp prohibited 2.3.4
```

Related Commands	Command	Description
	cs7 gtt map ss	Changes the state of a subsystem in the map table.
	cs7 mtp3 tuning rx-congestion-threshold	Enables multiple instances of a variant and network indicator combination.
	show cs7 gtt map	Displays CS7 GTT MAP entries.

cs7 gtt map ss

To change the state of a subsystem in the map table, use the **cs7 gtt map ss** privileged EXEC command.

```
cs7 [instance instance-number] gtt map ss {available | prohibited | ignore-sst | accept-sst}
    point-code ssn
```

Syntax Description	
instance	(Optional) Changes the state of a subsystem in the map table for an instance.
<i>instance-number</i>	Instance number. The valid range is 0 to 7. The default instance is 0.
accept-sst	Processes subsystem test messages received for the affected point code and subsystem.
available	Overrides the current state of the subsystem and sets it to available.
ignore-sst	Ignores subsystem test messages received for the affected point code and subsystem.
prohibited	Overrides the current state of the subsystem and sets it to prohibited.
<i>point-code</i>	Remote SP point code.
<i>ssn</i>	Subsystem number.

Defaults The default instance is 0.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.4(11)SW	This command was introduced.
	12.2(33)IRA	

Usage Guidelines When the ITP receives a subsystem prohibited message from the network, it changes the state of the subsystem to “prohibited” and starts sending subsystem test messages to the node that sent the message. It continues to send test messages until it receives a subsystem available message.

With the **cs7 gtt map ss** command, you can manually change the subsystem state to prohibited. Because you are performing a manual operation on the ITP, the ITP cannot send a subsystem test message (as it normally would) because it does not have a point code to send the message to.



Note This command is not applied to xUA DPC.

Examples The following example shows how to set the state of the remote point code 2.3.4 in the map table to prohibited:

```
cs7 gtt map ss prohibited 2.3.4 10
```

The following example shows how to set the state of the remote point code 2.3.4 in the map table to prohibited for instance 1:

```
cs7 instance 1 gtt map ss prohibited 2.3.4 10
```

Related Commands

Command	Description
cs7 gtt map ss	Changes the state of a subsystem in the map table.
cs7 mtp3 tuning rx-congestion-threshold	Enables multiple instances of a variant and network indicator combination.
show cs7 gtt map	Displays CS7 GTT MAP entries.

cs7 gtt replace-db

To replace the entire contents of the GTT database, use the **cs7 gtt replace-db** privileged EXEC command.

cs7 [**instance** *instance-number*] **gtt replace-db** *url*

Syntax Description

instance	(Optional) Replaces the entire contents of the GTT database for an instance.
<i>instance-number</i>	Instance number. The valid range is 0 to 7. The default instance is 0.
<i>url</i>	URL of replacement contents.

Defaults

The default instance is 0.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(11)SW	This command was introduced.
12.2(33)IRA	

Usage Guidelines

GTT database replacement is non-disruptive as of Cisco IOS release 12.2(18)IXA, 12.4(11)SW, and 12.2(33)IRA.

Examples

The following example shows how to replace the GTT database with a file named gttdata.txt in flash memory:

```
cs7 gtt replace-db flash:gttdata.txt
```

The following example shows how to replace the GTT database with a file named gttdata.txt in flash memory for instance 1:

```
cs7 instance 1 gtt replace-db flash:gttdata.txt
```

Related Commands

Command	Description
cs7 mtp3 tuning rx-congestion-threshold	Enables multiple instances of a variant and network indicator combination.
show cs7 gtt map	Displays CS7 GTT MAP entries.

cs7 gtt selector

To create and configure a GTT selector and enter the submode for modifying the attributes of an existing selector, use the **cs7 instance gtt selector** command in global configuration mode. To delete a selector, use the **no** form of this command.

cs7 [**instance** *instance-number*] **gtt selector** *selector* **tt** *tt* [**gti** *gti*] [**np** *np*] [**nai** *nai*]

no **cs7** *instance-number* **gtt selector** *selector*

Syntax Description

instance	(Optional) Creates and configures a GTT selector for an instance.
<i>instance-number</i>	Instance number. The valid range is 0 to 7. The default instance is 0.
<i>selector</i>	Name of the GTT selector. The name must be unique and no longer than 12 characters.
tt	Specifies a translation type.
<i>tt</i>	Translation type. In the Called Party field of the GTT message, the SSP sets the TT to indicate which GTT table the STP should use. The TT is a 1-byte field that usually maps to a specific service. Valid numbers range from 0 to 255.
gti	Specifies a global title indicator.
<i>gti</i>	(Optional) Global title indicator. Valid numbers are 2 (primarily used in the ANSI domain) or 4 (used in the ITU domain).
np	Specifies a numbering plan value.
<i>np</i>	(Optional) Numbering plan value. Valid range is 0 to 15.
nai	Specifies a nature of address indicator.
<i>nai</i>	(Optional) Nature of address indicator. Required for GTI 4. Optional for GTI 2. Valid range is 0 to 127.

Defaults

The default instance is 0.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The following rules apply to creating a GTT selector:

- NP and NAI cannot be specified if the variant is ANSI.
- GTI can be specified only if the variant is ITU.
- NP and NAI must be specified if GTI=4.

- For ITU nodes, GTI must be 2 or 4.
- For ANSI nodes, GTI must be 2.

The **cs7 gtt selector** *selector* command exits global configuration mode and enters cs7 gtt selector mode. This mode is used to modify attributes of a selector or to update global title addresses (GTAs) of a selector.

Examples

The following example shows how to configure for instance 2 a selector named itp_gtt with tt=0, gti=4, np=1, and nai=3:

```
cs7 instance 2 gtt selector itp_gtt 0 4 1 3
```

The following example shows how to configure a selector named itp_gtt with tt=0, gti=4, np=1, and nai=3:

```
cs7 gtt selector itp_gtt 0 4 1 3
```

Related Commands

Command	Description
cs7 mtp3 tuning rx-congestion-threshold	Enables multiple instances of a variant and network indicator combination.
show cs7 gtt selector	Displays CS7 GTT selectors.

cs7 gws action-set

To define gateway screening action sets, use the **cs7 gws action-set** command in global configuration mode. To remove the specification, use the **no** form of this command.

```
cs7 [instance instance-number] gws action-set action-set-name {allow | block [sccp-error error]| mlr
{ruleset ruleset-name | group result-group-name} [logging {silent | file [verbose] | console [verbose] | file
[verbose] console [verbose]}}] [pam pam-name]
```

```
no cs7 gws action-set action-set-name
```

Syntax Description

instance	(Optional) Specifies an instance.
<i>instance-number</i>	Instance number.
<i>action-set-name</i>	Name of the action set. Valid names may contain no more than 12 characters.
allow	Allows the message for further processing.
block	Blocks (rejects) the message.
mlr	Routes the MSU using MLR.
ruleset	Specifies a ruleset.
<i>ruleset-name</i>	Name of the ruleset.
group	Specifies a result group.
<i>result-group-name</i>	Name of the result group.
logging	(Optional) Enables logging.
silent	Screens messages without any logging.
file	Copies the log to a file.
verbose	(Optional) Prints packets up to 40 bytes to the file or displays them on the console along with other parameters.
console	Displays the log on the console.
sccp-error <i>error</i>	Configures block to send a UDTS to the originator of the SCCP packet. The UDT must also have return-on-error set and a return cause configured to return UDTS with an unqualified return cause. This keyword is used only for incoming packets.
pam	This keyword indicates a PAM table is part of the GWS action.
<i>pam-name</i>	Name used to specify the particular PAM table.

Defaults

The default logging type is **silent**.

Command Modes

Global configuration

Command History

Usage Guidelines

An action set cannot be deleted if it is referenced by other entries.
Action sets are independent of CS7 variants.

You can configure **block** with **scep-error** in MLR rules and address table entries.

Examples

The following example shows how to define the action sets allowed-ver and blocked-ver:

```
cs7 gws action-set allowed-ver allow
cs7 gws action-set blocked-ver block
```

The following example shows how to define GWS action sets for the PAM tables named pam1, pam2, and pam3:

```
cs7 instance 0 gws action-set action-set1 mlr group test pam pam1
cs7 instance 0 gws action-set action-set2 mlr ruleset test pam pam2
cs7 instance 0 gws action-set action-set2 allow pam pam3
```

Related Commands

Command	Description
show cs7 gws action-set	Displays ITP gateway screening action-set information.
cs7 pam	Identifies a packet address modification (PAM) table and enters the CS7 PAM submode.
cgpa (cs7 pam)	Configures one cgpa entry in the PAM table.
cdpa (cs7 pam)	Configures one cdpa entry in the PAM table.
opc	Configures an opc entry in the PAM table.
dpc	Configures a dpc entry in the PAM table.
modify-failure (pam)	Specifies the desired action when the PAM table packet modification fails.
gta asname	Creates or modifies a GTA entry that translates to an M3UA or SUA application server name. The GTA entry may include a PAM table.

cs7 gws as

To configure a GWS AS screening table, use the **cs7 gws as** command in global configuration mode. To remove the configuration, use the **no** form of this command.

cs7 [**instance** *instance-number*] **gws as** {**name** *as-name* | **default**}

no cs7 [**instance** *instance-number*] **gws as** {**name** *as-name* | **default**}

Syntax Description

instance	Specifies an instance.
<i>instance-number</i>	Instance number. The valid range is 0 to 7. The default instance is 0.
name	Specifies an AS name.
<i>as-name</i>	AS name.
default	Default screening for all ASes.

Defaults

The default instance is 0.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The GWS AS can be defined before or after the CS7 AS is defined.

The **cs7 gws as** command enables gws as configuration mode.

Examples

The following example shows how to configure an AS table for gateway screening. The AS name is as2.

```
cs7 instance 0 gws as name as2
  outbound result action ALLOW
!
```

The following example shows how to configure an AS table for gateway screening. The AS name is default.

```
cs7 instance 0 gws as default
  inbound logging type block file console verbose result table SIO0
  outbound result action BLOCK
!
```

Related Commands

Command	Description
show cs7 gws as	Displays ITP gateway screening information for the AS.

cs7 gws linkset

To specify a linkset table for gateway screening, use the **cs7 gws linkset** command in global configuration mode. To remove the configuration, use the **no** form of this command.

cs7 [*instance instance-number*] **gws linkset** { **name** *ls-name* | **default** }

no cs7 [*instance instance-number*] **gws linkset** { **name** *ls-name* | **default** }

Syntax Description

instance	Specifies an instance.
<i>instance-number</i>	Instance number. The valid range is 0 to 7. The default instance is 0.
name	Specifies a linkset.
<i>ls-name</i>	Linkset name.
default	Specifies the default screening for all linksets.

Defaults

Logging is silent.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The GWS linkset can be defined before or after the CS7 linkset is defined.
The **cs7 gws linkset** command enables gws linkset configuration mode.

Examples

The following example shows how to configure a GWS linkset screening table for the linkset `to_morehead1` and specify the inbound and outbound results:

```
cs7 instance 1 gws linkset name to_morehead1
  inbound result table OPCTTC1
  outbound result action BLOCK
```

Related Commands

Command	Description
show cs7 gws linkset	Displays ITP gateway screening information for the linkset.

cs7 gws replace

To replace the running GWS configuration file or existing GWS tables with ones from a local or remote file, use the **cs7 gws replace** EXEC command.

cs7 [**instance** *instance-number*] **gws replace** *url*

Syntax Description

instance	(Optional) Specifies an instance.
<i>instance-number</i>	Instance number.
<i>url</i>	Location where the file is to be saved.

Defaults

None.

Command Modes

EXEC

Command History

Usage Guidelines

Cisco ITP does not need to be reloaded to replace the running configuration.

Examples

The following example shows how to substitute a new GWS configuration for an older configuration:

```
cs7 gws-table replace xxx disk0:gws-replace
```

Related Commands

Command	Description
cs7 gws-table replace	Replaces a single GWS table with the table configuration file specified by the URL.
cs7 gws load	Loads a GWS configuration, including GWS tables, from a specified remote or local file during a Cisco ITP restart or reload.
show cs7 gws table	Displays the GWS table entries.

cs7 gws-table replace

To replace a single GWS table with the table configuration file specified by the URL, use the **cs7 gws-table replace EXEC** command.

cs7 [*instance instance-number*] **gws-table replace** *table-name url*

Syntax Description

instance	(Optional) Specifies an instance.
<i>instance-number</i>	Instance number.
<i>table-name</i>	Name of the new GWS table.
<i>url</i>	Location where the file is to be saved.

Defaults

None.

Command Modes

EXEC

Command History

Usage Guidelines

Cisco ITP does not need to be reloaded to replace the GWS table.

Examples

The following example shows how to substitute a new GWS table for an older one:

```
cs7 gws-table replace disk0:gws-replace
```

Related Commands

Command	Description
cs7 gws load	Loads a GWS configuration, including GWS tables, from a specified remote or local file during a Cisco ITP restart or reload.
cs7 gws replace	Replaces the running GWS configuration file or existing GWS tables with ones from a local or remote file.
show cs7 gws table	Displays the GWS table entries.

cs7 gws load

To load a GWS configuration, including GWS tables, from a specified remote or local file during a Cisco ITP restart or reload, use the **cs7 gws load** command in global configuration mode.

cs7 [**instance** *instance-number*] **gws load** [*url*]

Syntax Description

instance	(Optional) Specifies an instance.
<i>instance-number</i>	Instance number.
<i>url</i>	Location where file is to be saved.

Defaults

None.

Command Modes

Global configuration

Command History

Usage Guidelines

Entering the **load** command does not initiate the restart or reload needed to trigger the actual load operation. It configures the load operation to occur when a restart or reload occurs.

If the load operation fails, the system generates an error message with the probable cause of the problem. Syntax errors in the loaded file can cause the load operation to fail.

Examples

The following example shows how to load a GWS configuration:

```
cs7 gws load disk0:gws-config
```

Related Commands

Command	Description
cs7 gws-table replace	Replaces a single GWS table with the table configuration file specified by the URL.
cs7 gws replace	Replaces the running GWS configuration file or existing GWS tables with ones from a local or remote file.
show cs7 gws config	Displays the whole configuration of GWS, including global action sets, linksets, global table entries, tables, and table entries.
show cs7 gws table	Displays the GWS table entries.

cs7 gws table

To configure gateway screening tables, use the **cs7 gws table** command in global configuration mode. To remove the table, use the **no** form of this command.

cs7 [*instance instance-number*] **gws table** *name* **type** *table-type* [**action** {**allowed** | **blocked**}]

no **cs7** [*instance instance-number*] **gws table** *name*

Syntax Description																																	
instance	Specifies an instance.																																
<i>instance-number</i>	Instance number. The valid range is 0 to 7. The default instance is 0.																																
<i>name</i>	Name of the table.																																
type	Specifies a gateway screening table type.																																
<i>table-type</i>	Gateway screening table type. Valid types are: <table> <tr> <td>aff-dest</td><td>Affected Dest Table</td></tr> <tr> <td>aff-pc-ssn</td><td>SCCP Aff. PC-SSN Table</td></tr> <tr> <td>cdpa-gta-prefix</td><td>CdPA GTA Prefix Table</td></tr> <tr> <td>cdpa-gta-range</td><td>CdPA GTA Range Table</td></tr> <tr> <td>cdpa-pc-ssn</td><td>CdPA PC-SSN Table</td></tr> <tr> <td>cdpa-selector</td><td>CdPA Selector Table</td></tr> <tr> <td>cgpa-gta-prefix</td><td>CgPA GTA Prefix Table</td></tr> <tr> <td>cgpa-gta-range</td><td>CgPA GTA Range Table</td></tr> <tr> <td>cgpa-pc-ssn</td><td>CgPA PC-SSN Table</td></tr> <tr> <td>cgpa-selector</td><td>CgPA Selector Table</td></tr> <tr> <td>dpc</td><td>DPC Table</td></tr> <tr> <td>isup-msg-type</td><td>ISUP Msg Type Table</td></tr> <tr> <td>mtp-msg-type</td><td>MTP Msg Type Table</td></tr> <tr> <td>opc</td><td>OPC Table</td></tr> <tr> <td>sccp-msg-hdr</td><td>SCCP Msg Hdr Table</td></tr> <tr> <td>sio</td><td>SIO Table</td></tr> </table>	aff-dest	Affected Dest Table	aff-pc-ssn	SCCP Aff. PC-SSN Table	cdpa-gta-prefix	CdPA GTA Prefix Table	cdpa-gta-range	CdPA GTA Range Table	cdpa-pc-ssn	CdPA PC-SSN Table	cdpa-selector	CdPA Selector Table	cgpa-gta-prefix	CgPA GTA Prefix Table	cgpa-gta-range	CgPA GTA Range Table	cgpa-pc-ssn	CgPA PC-SSN Table	cgpa-selector	CgPA Selector Table	dpc	DPC Table	isup-msg-type	ISUP Msg Type Table	mtp-msg-type	MTP Msg Type Table	opc	OPC Table	sccp-msg-hdr	SCCP Msg Hdr Table	sio	SIO Table
aff-dest	Affected Dest Table																																
aff-pc-ssn	SCCP Aff. PC-SSN Table																																
cdpa-gta-prefix	CdPA GTA Prefix Table																																
cdpa-gta-range	CdPA GTA Range Table																																
cdpa-pc-ssn	CdPA PC-SSN Table																																
cdpa-selector	CdPA Selector Table																																
cgpa-gta-prefix	CgPA GTA Prefix Table																																
cgpa-gta-range	CgPA GTA Range Table																																
cgpa-pc-ssn	CgPA PC-SSN Table																																
cgpa-selector	CgPA Selector Table																																
dpc	DPC Table																																
isup-msg-type	ISUP Msg Type Table																																
mtp-msg-type	MTP Msg Type Table																																
opc	OPC Table																																
sccp-msg-hdr	SCCP Msg Hdr Table																																
sio	SIO Table																																
action	(Optional) Specifies the action for a screening match.																																
allowed	Allows the message.																																
blocked	Blocks the message.																																

Defaults If no **action** is specified, the default is **allowed**.

Command Modes Global configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

To be deleted, a table must have no entries and must not be referenced by any other entries.

The **cs7 gws table** command enables gws table configuration mode for the table type specified.

Examples

The following example shows how to configure a gateway screening table named allowed-dpc-1. The table type is **dpc** and the action is **allowed**.

```
cs7 instance 0 gws table allowed-dpc-1 type dpc action allowed
```

Related Commands

Command	Description
show cs7 gws table	Displays GWS table information.

cs7 host

To map a hostname to a point code, use the **cs7 host** command in global configuration mode. To remove all point code mappings for a name, use the **no cs7 host hostname** form of this command. To remove only one point code from a name mapping, use the **no cs7 host hostname point-code** form of this command.

```
cs7 host hostname [additional] {point-code [point-code ...]} | {point-code:instance-number  
[point-code:instance-number...]}
```

```
no cs7 host hostname [additional] {point-code [point-code ...]} | {point-code:instance-number  
[point-code:instance-number...]}
```

Syntax Description	additional	Appends an additional point code.
	<i>hostname</i>	Name of the SS7 node.
	<i>instance-number</i>	When the multiple instances feature is enabled, specifies the instance number.
	<i>point-code</i>	Point code to be mapped.

Defaults	None.

Command Modes	Global configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	You can map multiple point codes to the same hostname. This feature allows a node that is part of multiple instances to have the same name in all instances. However, a point code <i>cannot</i> be mapped to multiple names.

The optional **additional** keyword must be used when assigning an additional point code to a hostname. If you do not specify **additional**, an existing mapping of point codes to the name is replaced with the new configuration.

When the multiple instance feature is enabled, include the instance number.

To display the mapping of hostnames to point codes, use the **show hosts** command. If a point code represents a node (no clusters, networks, or summarized routes) and a name for the point code is configured, the name is displayed instead of the point code. Otherwise, the numeric point code is displayed.

You can specify a name instead of a point code in the **show cs7** and **ping cs7** commands. However, configuration statements require a numeric point code.

Examples

The following configuration includes an example of the **cs7 host** command:

```
cs7 multi-instance
cs7 instance 0 variant ITU
cs7 instance 0 point-code format 14
cs7 instance 1 variant ANSI
cs7 instance 1 network-name ansi

cs7 host red 1.1.1:1 1234:0
cs7 host green 5121:0
!
cs7 instance 0 route-table
  update route 5221 16383 linkset one
  update route 5121 16383 linkset one
  update route 5120 16376 linkset one
  update route 1234 16383 linkset one
!
cs7 instance 1 route-table
  update route 1.1.1 255.255.255 linkset two
!
cs7 instance 0 linkset one 666
!
cs7 instance 1 linkset two 3.3.3
!
```

Related Commands

Command	Description
cs7 pmp	Assigns a local point code to an instance.
cs7 variant	Specifies the variant for an instance.
cs7 mtp3 tuning rx-congestion-threshold	Enables multiple instances of a variant and network indicator combination.
show cs7	Displays the ITP basic configuration, including the point code and capability point code.
show hosts	Displays information about a host.

cs7 ignore-sccp-pcconv

To configure instance conversion to ignore the SCCP point code (PC), use the **cs7 ignore-sccp-pcconv** command in global configuration mode. To remove the configuration, use the **no** form of this command.

cs7 [*instance instance-number*] **ignore-sccp-pcconv** *point-code*

no [*instance instance-number*] **ignore-sccp-pcconv** *point-code*

<i>instance-number</i>	Specifies the instance number.
<i>point-code</i>	Point code to be mapped.

Defaults

None.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXH1	This command was introduced.
12.4(15)SW5	
12.2(33)IRE	

Usage Guidelines

When Cisco ITP is performing instance conversion, it tries to instance convert MTP3 PC and SCCP PCs. If Cisco ITP is doing MTP3 routing, there is no info for the SCCP PC and it produces an error. This command prevents that error when the CxPA PC does not have a PC conversion item configured for it.

Without the **cs7 ignore-sccp-pcconv** command configured, the Cisco ITP blocks the traffic because it is unable to convert the SCCP layer PC. No alias is defined for the SCCP layer PC.

With the **cs7 ignore-sccp-pcconv** command configured, the Cisco ITP does not attempt to convert the SCCP layer PC to the alias PC anymore. The traffic is routed normally.

Examples

The following command shows how to configure the Cisco ITP to ignore the PC conversion failure in SCCP layer if the packet goes from y to x.

```
cs7 instance [x] ignore-sccp-pcconv [y]
```

cs7 inhibit

To inhibit a link, use the **cs7 inhibit** user EXEC command with the linkset name and the link number. To reverse the inhibit, use the **cs7 uninhibit** command.

cs7 inhibit *linkset link*

cs7 uninhibit *linkset link*

Syntax Description	<i>linkset</i>	Linkset name.
	<i>link</i>	Link.

Defaults	None.

Command Modes	User EXEC

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	Use the inhibit command when you need to make or keep a signaling link unavailable to user-generated signaling traffic (for example, for maintenance). Inhibiting a link is allowed only if the action does not cause any previously accessible destinations to become inaccessible at either end of the signaling link.
	A signaling traffic management command, inhibit does not cause any link status changes at Level 2. In particular, a signaling link that was active and in service before being inhibited will remain so, and will be able to transmit and receive maintenance and test messages.

Examples	The following command shows how to inhibit link 0 on the linkset named tony:
	<code>cs7 inhibit tony 0</code>

Related Commands	Command	Description
	shutdown (cs7 link)	Disables a link or linkset.
	cs7 uninhibit	Puts the link or linkset back in service.

cs7 large-msu-support

To configure large MSU support for all M2PA links in a CS7 instance, use the **cs7 instance large-msu-support** command in global configuration mode. To disable the support, use the **no** form of this command.

cs7 instance *instance-number* **large-msu-support**

no cs7 instance *instance-number* **large-msu-support**

Syntax Description

<i>instance-number</i>	Instance number.

Defaults

M2PA restricts the outgoing packet size to 273 bytes.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXH	This command was introduced.
12.4(15)SW3	
12.2(33)IRC	

Usage Guidelines

This command allows an instance to carry MSU sizes of up to 4096 bytes instead of the default maximum of 273 bytes. SCTP segmentation and reassembly is used for the MSUs that are greater than the 1500 bytes and carried by the M2PA link, because M2PA runs over IP networks with a maximum MSU size of 1500 bytes.

Examples

The following example shows large MSU is supported on all the M2PA links in that CS7 instance:

```
cs7 instance 0 large-msu-support
```

Related Commands

Command	Description
cs7 linkset	Specifies a linkset and enters cs7 linkset submode.

cs7 linkset

To specify a linkset and enter cs7 linkset submode, use the **cs7 linkset** command in global configuration mode. To disable the specification, use the **no** form of this command.

cs7 [**instance** *instance-number*] **linkset** *ls-name* *adj-pc* [**local-pc** [*pc*]]

no cs7 [**instance** *instance-number*] **linkset** *ls-name* *adj-pc*

Syntax Description

instance	(Optional) Specifies a linkset for an instance.
<i>instance-number</i>	Instance number. The valid range is 0 to 7. The default instance is 0.
<i>ls-name</i>	Name of the linkset. (Linkset names are case-specific.)
<i>adj-pc</i>	Point code of the adjacent signaling point.
local-pc	(Optional) Specifies another point code, which functions as a second linkset between the ITP and the adjacent node.
<i>pc</i>	Can be the ITP's primary or secondary point code. By default, it is the primary point code.

Defaults

The specified local pc is the ITP's primary point code.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

You must specify the SS7 variant and the point code before you can configure linksets.

When you remove a linkset from the configuration with the **no cs7 linkset** command, a few seconds elapse before the system responds. This delay ensures that all previous shutdown-related activity has completed for the linkset.



Note

To avoid overloading the CPU, we recommend that you shut down interfaces that are configured but not provisioned as part of a linkset.

With the optional multiple linkset feature, you can configure two linksets to an adjacent node, each having 16 links, for a total of 32 links. To configure the linksets, use the optional keyword **local-pc**. This local PC must be either the ITP's primary PC (configured with the **cs7 point-code** command) or the ITP's secondary PC, configured with the **cs7 secondary-pc** command. (By default, it is the primary PC.)

When a linkset is created using the **cs7 linkset** command, a route table entry is automatically created for destination *adj-pc*. Because this entry is the direct linkset to this destination, it is assigned the highest priority of 1.

When two linksets to the adjacent node are created, they are automatically entered in the route table as a combined route to the adjacent node. Traffic going to the adjacent node is divided between the two linksets based on the signaling link selector (SLS).

When you issue the **cs7 linkset** command, you enter cs7 linkset submode. In this submode, you have access to commands that allow you to further configure linksets.

Linkset names are case-specific.

Examples

The following example shows how to configure a single a linkset named linkset1 with an adjacent node at point code 2.2.2.:

```
cs7 linkset linkset1 2.2.2
```

The following example shows how to configure two linksets to the adjacent node 2.2.2.

Linkset1 specifies the adjacent signaling point 2.2.2 and the ITP's primary point code 1.1.1.

Linkset2 specifies the adjacent signaling point 2.2.2 and the ITP's secondary point code 1.1.2.

```
cs7 linkset linkset1 2.2.2 local-pc 1.1.1
cs7 linkset linkset2 2.2.2 local-pc 1.1.2
```

The following example shows how to configure two linksets on instance 1 to the adjacent node 2.2.2.

Linkset1 specifies the adjacent signaling point 2.2.2 and the ITP's primary point code 1.1.1.

Linkset2 specifies the adjacent signaling point 2.2.2 and the ITP's secondary point code 1.1.2.

```
cs7 instance 1 linkset linkset1 2.2.2 local-pc 1.1.1
cs7 instance 1 linkset linkset2 2.2.2 local-pc 1.1.2
```

Related Commands

Command	Description
cs7 mtp3 tuning rx-congestion-threshold	Enables multiple instances of a variant and network indicator combination.
show cs7 linkset	Displays ITP linkset information.

cs7 local-peer

To specify the local peer and, optionally, configure M2PA/SCTP offload, use the **cs7 local-peer** command in global configuration mode. To remove the local peer from the ITP configuration, use the **no** form of this command.

cs7 local-peer *port-number* [**offload**] [*line-card-slot-number*] [*bay-number*]

no local-peer *port-number* [**offload**] [*line-card-slot-number*] [*bay-number*]

Syntax Description

<i>port-number</i>	Port number of the local peer. Range is 1024 to 49151.
offload	Configures local peer for M2PA/SCTP offload onto a line card.
<i>line-card-slot-number</i>	Line card slot number. Valid range is 0 to 16.

Defaults

None.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.
12.2(25)IRA	Extended the range of the <i>bay-number</i> argument for use with SAMI processors.

Usage Guidelines

This command is not instance related and cannot be specified with the **instance** keyword.

When you issue the **cs7 local-peer** command, you enter cs7 local peer submode. In this submode, you can configure a local IP address for an instance.

The range for *bay-number* (3 to 8) reflects the labeling of the SAMI card processors. It is consistent with other SAMI applications, as well as the faceplate numbering for the console connections.

Examples

The following example shows how to offload M2PA/SCTP onto the SAMI card in slot 2, processor 3:

```
cs7 local-peer 7000 offload 2 3
```

The following example shows how to specify a local peer with a local port number of 7000:

```
cs7 local-peer 7000
```

The following example shows how to offload M2PA/SCTP onto the line card in slot 2, bay 0:

```
cs7 local-peer 7000 offload 2 0
```

Related Commands

Command	Description
local-ip (cs7 dcs)	Assigns an IP address to the local peer.
show cs7 m2pa	Displays ITP M2PA statistics.
show cs7 sami ip	Displays an ITP SAMI configuration.

cs7 local-sccp-addr-ind

To customize the setting of the national use field within SCCP management calling and called party addresses, use the **cs7 local-sccp-addr-ind** command in global configuration mode. To remove the configuration, use the **no** form of this command.

cs7 [*instance instance-number*] **local-sccp-addr-ind** {**national** | **international**}

no cs7 [*instance instance-number*] **local-sccp-addr-ind** {**national** | **international**}

Syntax Description

instance	(Optional) Specifies on an instance how to set the value of the national indicator value within SCCP management calling and called addresses.
<i>instance-number</i>	Instance number. The valid range is 0 to 7. The default instance is 0.
national	Sets the address indicator field to '1'b to indicate national format.
international	Sets the address indicator field to '0'b to indicate international format.

Defaults

The default value for instances configured with the ANSI variant is national ('1'b value), and the default for all other variants is international ('0'b value).

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

Bit 8 of the address indicator field within the SCCP calling and called address parameters is reserved for use by national specifications. (The ANSI variant, for example, sets this indicator to '1'b to indicate that the SCCP addresses are in a national format.) SCCP processing of the addresses is not affected by the setting of this indicator, but some STP and SCP implementations perform validity checking on the indicator.

The configuration of this command only affects the construction of SCCP management address fields.

Examples

In the following example, the default instance (instance 0) is configured with the China variant and the address indicator field is set to national. Instance 1 is configured with the ANSI variant and the address indicator field is set to international.

```
cs7 variant china
cs7 local-sccp-addr-ind national

cs7 instance 1 ansi
cs7 instance 1 local-sccp-addr-ind international
```


Related Commands

Command	Description
cs7 mtp3 tuning rx-congestion-threshold	Enables multiple instances of a variant and network indicator combination.
cs7 variant	Configures the MTP3 and SCCP standard specification to use.

cs7 log

To enable the ITP to log events, errors, and traces, use the **cs7 log** command in global configuration mode. To disable logging, use the **no** form of this command.

cs7 log *type* { **checkpoint** *seconds destination* | **size** *entries* | **verbose** }

no cs7 log *type*

Syntax Description

<i>type</i>	Specifies the type of log. Valid types are: gtt Log related to global title translation errors. gws-nontest Enhanced gateway screening logging in nontest mode. gws-test Enhanced gateway screening logging in test mode.
checkpoint	Enables automatic archiving of a log to a remote or local destination at a specified interval.
<i>seconds</i>	Archiving interval in seconds. The valid range is 60 to 86400 seconds.
<i>destination</i>	Specifies the location where the log is stored. Valid destinations are: cs7: path to store log flash: path to store log ftp: path to store log null: path to store log nvr: path to store log nvram: path to store log rcp: path to store log system: path to store log tftp: path to store log
size	Specifies the maximum number of entries in the log.
<i>entries</i>	Maximum number of entries in the log. The valid range is 0 to 100,000 entries. The default is 0. When the limit is reached, new entries overwrite existing entries, starting from the first entry.
verbose	Enables verbose output of log entries.

Defaults

Logging is off. The default log size is 0.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The log is saved to an internal file. The filename is created internally and comprises the log type and the timestamp indicating when the checkpoint occurred.

Examples

The following example shows how to archive a GWS log every hour and send the log to the destination directory tftp://10.1.1.2/logs:

```
cs7 log gws-test checkpoint 3600 tftp://10.1.1.2/logs
```

The following example shows how to specify the maximum number of entries in the circular log. When the current number of entries exceeds 10000, the first entry is overwritten.

```
cs7 log gws-test size 10000
```

The following example shows how to specify the checkpoint DIRECTORY. The filename is created automatically and contains the timestamp when the checkpoint occurred.

```
cs7 log gws-test checkpoint 10000 tftp://bizarre/rosebud/
```

Related Commands

Command	Description
show cs7 log	Displays the current log.

cs7 log checkpoint

To enable automatic archiving of a log to a remote or local destination at a specified interval of time, use the **cs7 log checkpoint** command in global configuration mode. To disable the checkpoint operation, use the **no** form of this command.

cs7 log type checkpoint secs destination

no cs7 log type checkpoint secs destination

Syntax Description

<i>type</i>	Specifies the type of log.
<i>secs</i>	Specifies the interval in seconds.
<i>destination</i>	Path and filename of the log archive destination.

Defaults

Log checkpointing is off.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Examples

The following example shows how to archive the GTT log every hour and send the log to the destination tftp://10.1.1.2/logs with the filename gtt and the date and timestamp:

```
cs7 log gtt checkpoint 3600 tftp://10.1.1.2/logs/
```

Related Commands

Command	Description
cs7 log	Enables the ITP to log events, errors, and traces.
cs7 save log	Saves a log to a file.
show cs7 log	Displays the current log.

cs7 m3ua

To specify the local port number for M3UA and enter m3ua submode, use the **cs7 m3ua** command in global configuration mode. To delete the M3UA configuration (if there are no configured M3UA ASes or ASPs), use the **no** form of this command.

cs7 m3ua *port-number* [**offload**] [*line-card-slot-number*] [*bay-number*]

no m3ua *port-number* [**offload**] [*line-card-slot-number*] [*bay-number*]

Syntax Description

<i>port-number</i>	Port number of the local peer. Range is 1024 to 49151. The M3UA well-known port is 2905.
offload	(Optional) Configures the local peer for M2PA/SCTP offload onto a line card. Offloading applies only to the 7600 platform.
<i>line-card-slot-number</i>	(Optional) Line card slot number. Valid range is 0 to 16.

Defaults

None.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.
12.2(25)IRA	Extends the range of the bay-number argument for use with SAMI processors.

Usage Guidelines

The range for *bay-number* (3 to 8) reflects the labeling of the SAMI card processors. It is consistent with other SAMI applications, as well as the faceplate numbering for the console connections.

M3UA uses SCTP to communicate with application server processes (ASPs). The **offload** keyword enables the ITP to offload M3UA SCTP message processing to the line card. If you are configuring M3UA SCTP offload, the **local-ip** *ip-address* must be an IP address that was already configured on the line card to which you are offloading this M3UA instance. When offload is enabled, only a single IP route is allowed for each destination.

If offloaded, a specific M3UA instance can run on only one line card, but different offloaded M3UA instances can run on different line cards or on the same line card. If you offload M3UA or SUA to a line card, that line card cannot also be used for M2PA offload.

Issuing the **cs7 m3ua** command enables cs7 m3ua submode.

The **cs7 m3ua** command cannot be specified with the **instance** keyword.

The M3UA configuration must be removed before the variant or local point code can be removed.

Examples

The following example shows how to specify a local port number of 2000 for M3UA:

```
cs7 m3ua 2000 offload 2 0
local-ip 10.10.10.7
```

The following example shows how to offload two different instances of M3UA processing to the line card in slot 5, bay 0 and another instance to the line card in slot 6, bay 0:

```
cs7 m3ua 3000 offload 5 0
local-ip 10.10.10.8
!
cs7 m3ua 3500 offload 5 0
local-ip 10.10.10.8
!
cs7 m3ua 4000 offload 6 0
local-ip 10.10.10.9
```

Related Commands

Command	Description
local-ip (CS7 M3UA)	Configures up to four local IP addresses that will receive M3UA packets.
show cs7 asp	Displays ASP information.
show cs7 m3ua	Displays M3UA node information.

cs7 m3ua extended-upu

To enable M3UA extended UPU (User Part Unavailable) operation, use the **cs7 m3ua extended-upu** command in global configuration mode. To remove the statement from the configuration, use the **no** form of this command.

cs7 m3ua extended-upu

no cs7 m3ua extended-upu

Syntax Description This command has no arguments or keywords.

Defaults None.

Command Modes Global configuration

Command History	Release	Modification
	12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.

Usage Guidelines By default, the ITP sends response-mode UPU messages when a received message has a DPC equal to a locally managed ITP PC (including M3UA and SUA AS PCs) that is available, and the service indicator (SI) within the received message is not supported or not available.

With **cs7 m3ua extended-upu** configured, the ITP also sends UPU messages in the following cases. (Note that the destination M3UA AS PC must still be available.)

- If the M3UA AS goes down or becomes inactive, send UPU message to the OPC in the AS routing key with unavailability cause = inaccessible remote user.
- If the M3UA AS is inactive or down and matches a received MSU, send UPU message to the OPC in the MSU with unavailability cause = inaccessible remote user.
- If an ISUP or TUP MSU is received and matches no routing key, send UPU message to the OPC in the MSU with unavailability cause = unequipped remote user.
- If an M3UA AS with OPC configured and SI configured for ISUP or TUP becomes inactive, send UPU message to the OPC in the AS routing key.

Extended UPU is not allowed if any M3UA AS has a CIC range configured. Conversely, CIC range configuration is not allowed if extended UPU is enabled.

In all cases, UPU is rate-limited to no more than 1 per second per SI value.

Examples The following example shows how to enable M3UA extended UPU operation:

```
cs7 m3ua extended-upu
```

cs7 mated-sg

To configure a connection to a mated SG, use the **cs7 mated-sg** command in global configuration mode. To remove the mate definition from the configuration, use the **no** form of this command.

cs7 mated-sg *name remote-port* [*local-port*] [**passive**]

no cs7 mated-sg *name remote-port* [*local-port*] [**passive**]

Syntax Description

<i>name</i>	Name of the mated SG. The mated-SG name is a unique name used to identify the mate for configuration and monitoring. This name may be up to 12 characters long. The first character must be alphabetic. The mate name cannot match a reserved keyword (such as m3ua , sua , all , operational , active , statistics , bindings , or detail).
<i>remote-port</i>	Remote port number of the mate, in the range 1024 to 65535. This argument is used for validation. The SCTP connection requests from the mate must come in with this remote port number.
<i>local-port</i>	(Optional) Local port number for SGMP link offloaded to line card
passive	(Optional) Does not attempt to initiate the connection to the mate.

Defaults

None.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.
12.2(33)IRD	The <i>local-port</i> argument was introduced.

Usage Guidelines

The Signaling Gateway Mate Protocol (SGMP) is used to establish an association to the mated SG with an equivalent SG configuration.

The **cs7 mated-sg** command allows you to define the mated SG and enables cs7 mated-sg configuration submode. Only one mate can be defined on a SG. The mate uses the SGMP local port.

The **no** form of the **cs7 mated-sg** command deletes the mate definition from configuration. You must remove the mate from all **cs7 asroute** definitions before this command can be deleted from the configuration.

This command is not instance related and cannot be specified with the **instance** keyword.

Examples

The following example shows how to specify a mated SG named mate2 at remote port 5000 with the **passive** keyword:


```
cs7 mated-sg mate2 5000 passive
```

Related Commands

Command	Description
cs7 as	Defines an AS.
cs7 sgmp	Specifies the local port number for SGMP and enters cs7 sgmp submode.
remote-ip (cs7 mated-sg)	Configures a remote IP address to associate incoming packets from the mate.
show cs7 mated-sg	Displays mated-SG information.

cs7 max-dynamic-routes

To specify the maximum number of dynamic routes, use the **cs7 max-dynamic routes** command in global configuration mode. To restore the default maximum number of dynamic routes, use the **no** form of this command.

cs7 max-dynamic-routes *number*

no cs7 max-dynamic-routes *number*

Syntax Description	<i>number</i>	Maximum number of dynamic routes that can be created. The range is 100 to 2000. The default number is 1000.

Defaults	1000 dynamic routes

Command Modes	Global configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	This command is not instance related and cannot be specified with the instance keyword.

Examples	The following example shows how to specify a maximum of 500 dynamic routes: <code>cs7 max-dynamic-routes 500</code>

Related Commands	Command	Description
	show cs7 route	Displays the ITP routing table.

cs7 mlr address-table

To define a table of addresses to use when searching with the previously specified routing parameter, use the **cs7 mlr address-table** command in global configuration mode. To remove the definition, use the **no** form of this command.

cs7 [**instance** *instance-number*] **mlr address-table** *table-name*

no [**instance** *instance-number*] **cs7 mlr address-table** *table-name*

Syntax Description

instance	(Optional) Specifies the ITP network instance in which the MLR table is valid.
<i>instance-number</i>	Instance number. The valid range is 0 to 7. The default instance is 0.
<i>table-name</i>	Identifies a name to be associated with this multilayer result table. The name must be unique among all multilayer routing tables. The name is specified as a character string with a maximum of 12 characters.

Defaults

The default instance is 0.

Command Modes

Global configuration

Command History

Release	Modification
12.2(21)SW	This command was introduced.

Usage Guidelines

The MLR address table contains addresses and destinations that more than one rule may reference. If a table is required in more than one instance, then it must be defined in each appropriate instance. If the instance is not specified, then the table may be used only for the default network instance, 0.

Both DSMR (SMS MO Proxy) and MLR can reference MLR address tables.

The **cs7 mlr address-table** command enables cs7 mlr address-table configuration mode.

Examples

The following example shows how to define a table of addresses named VSMSC-ADDRS:

```
cs7 mlr address-table VSMSC-ADDRS
```

Related Commands

Command	Description
addr (cs7 mlr address-table)	Specifies an MLR address within the MLR address table.
show cs7 mlr address-table	Displays addresses matched within the CS7 MLR address table.

cs7 mlr load

To load an MLR configuration, including MLR tables, from a specified remote or local file during a Cisco ITP restart or reload, use the **cs7 mlr load** privileged EXEC command.

cs7 [**instance** *instance-number*] **mlr load** *url*

Syntax Description

instance	(Optional) Specifies an instance.
<i>instance-number</i>	Instance number.
<i>url</i>	Location where the file is to be saved.

Defaults

None.

Command Modes

Privileged EXEC

Command History

Usage Guidelines

Entering the **load** command does not initiate the restart or reload needed to trigger the actual load operation. It configures the load operation to occur when a restart or reload occurs.

If the load operation fails, the system generates an error message with the probable cause of the problem. Syntax errors in the loaded file can cause the load operation to fail.

Examples

The following example shows how to load an MLR configuration:

```
cs7 mlr load disk0:mlr-config
```

Related Commands

Command	Description
cs7 save mlr	Saves a general MLR configuration to a separate file.
cs7 mlr replace	Replaces the running configuration file with a file specified by the URL.

cs7 mlr modify-profile

To specify an MLR modify profile, use the **cs7 mlr modify-profile** configuration command. To remove the specification, use the **no** form of this command.

A modification profile specifies SCCP and MAP address modification rules for messages that are routed by a configured set of MLR rules. For each profile, you must configure the instance, a unique profile name, the protocol, and optional operation. Multiple profiles can be created for each instance. Only one profile may be assigned to a specific rule.

MLR supports CgPA and CdPA modification for all GSM-MAP and ANSI-41 operations, provided that the protocol and operation of the associated rule and modify-profile are compatible.

```
cs7 [instance instance] mlr modify-profile profile-name {gsm-map [operation-name] | ansi-41}
```

```
no cs7 [instance instance] mlr modify-profile profile-name {gsm-map [operation-name] | ansi-41}
```

Syntax Description

instance	(Optional) Specifies an instance.
<i>instance-number</i>	Instance number.
<i>profile-name</i>	Identifies a name to be associated with this MLR modify-profile. The name must be unique among all CS7 MLR modify-profiles. The name is specified as a character string with a maximum of 12 characters.
gsm-map	Modify-profile is valid for GSM MAP messages.
ansi-41	Modify-profile is valid for ANSI-41 messages.
<i>operation-name</i>	(Optional) Operation for which the modify-profile is valid. The only currently valid operation name is sri-sm , which indicates that the modify-profile will operate only on a GSM-MAP sendRoutingInfoForSM message. If an operation is not specified, then the profile applies to all operations using the configured protocol (for example, GSM MAP or ANSI-41).

Defaults

None.

Command Modes

cs7 mlr modify-profile configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The **cs7 mlr modify-profile** command enters cs7 mlr modify configuration submode.

You can create multiple modify profiles for each instance, but can specify only one profile within a rule.

MLR currently supports modifying only the service center address (orig-smsc) and the calling party address (CgPA) for SRI-SM messages.

The modify-profile is assigned to a rule using the **modify-profile rule** command. If an MLR rule matches, then the modify-profile is applied to messages that are routed using MLR. Address translation is performed only if the matched rule contains a modify-profile.

MLR modify-profile and PAM cannot be configured simultaneously.

Related Commands	Command	Description
	clear cs7 accounting	Specifies a combination trigger based on the combination of the calling party and the called party.
	modify-profile (cs7 mlr ruleset rule)	Specifies SCCP and MAP addresses to modify in messages that are routed with MLR.

cs7 mlr options

To specify MLR global options, use the **cs7 mlr options** command in global configuration mode. To remove the definition, use the **no** form of this command.

cs7 [*instance instance-number*] **mlr options**

no cs7 [*instance instance-number*] **mlr options**

Syntax Description

instance	(Optional) Specifies the IP Transfer Point (ITP) network instance in which the MLR global options are valid.
<i>instance-number</i>	Instance number. The valid range is 0 to 7. The default instance is 0.

Defaults

The default instance is 0.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXB	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The **cs7 mlr options** command enables cs7 mlr options configuration mode.

Examples

The following example shows how to enable global options and, when a packet is routed with MLR, insert the Message Transfer Part (MTP) destination point code (DPC) into the called party (cdpa) point code (pc) if the cdpa is null. This global option applies to the MLR-routed results **pc**, **pcssn**, **gt**, and **asname**.

```
cs7 instance 0 mlr options
  insert-dpc-in-cdpa
```

Related Commands

Command	Description
insert-dpc-in-cdpa	Global option inserts DPC into the cdPA PC for packets that are routed with MLR.
preserve-opc (cs7 mlr ruleset)	Preserves the original originating point code (OPC) when an MLR is selected in this instance.
modify-profile (cs7 mlr ruleset rule)	Specifies SCCP and MAP addresses to modify in messages that are routed with MLR.

cs7 mlr replace

To replace the running MLR configuration file or existing MLR tables with ones from a local or remote file, use the **cs7 mlr replace** EXEC command.

cs7 [**instance** *instance-number*] **mlr replace** *url*

Syntax Description

instance	(Optional) Specifies an instance.
<i>instance-number</i>	Instance number.
<i>url</i>	Location where the file is to be saved.

Defaults

None.

Command Modes

EXEC

Command History

Usage Guidelines

Cisco ITP does not need to be reloaded to replace the running configuration.

Examples

The following example shows how to substitute a new MLR configuration for an older configuration:

```
cs7 mlr replace disk0:mlr-config
```

Related Commands

Command	Description
cs7 mlr load	Replaces a single MLR table with the table configuration file specified by the URL.
cs7 save mlr	Loads a GWS configuration, including GWS tables, from a specified remote or local file during a Cisco ITP restart or reload.

cs7 mlr result

To name a multilayer result group, use the **cs7 mlr result** command in global configuration mode. The result group lists destination resources that process traffic to be routed based on multilayer information.

To delete a multilayer result group, use the **no** form of this command.

```
cs7 [instance instance-number] mlr result result-name [protocol {gsm-map | ansi41}] [mode {wrr | dest-sme-binding}]
```

```
no cs7 [instance instance-number] mlr result result-name [protocol {gsm-map | ansi41}] [mode {wrr | dest-sme-binding}]
```

Syntax Description	
instance	(Optional) Specifies the ITP network instance in which the MLR table is valid. If a table is required in more than one instance, then it must be defined in each appropriate instance. If an instance is not specified, then the table may only be used for the default network instance 0.
<i>instance-number</i>	Instance number. The valid range is 0 to 7. The default instance is 0.
<i>result-name</i>	Identifies a name to be associated with this multilayer result table. The name must be unique among all multilayer routing tables. The name is specified as a character string with a maximum of 12 characters.
protocol	Used only by SMS-MO Proxy (DSMR). It is included in MLR result group configuration in case a DSMR result references an MLR result group. It is not used by MLR.
gsm-map	Protocol used by SMS-MO Proxy (DSMR) for the results in this result group.
ansi41	Protocol used by SMS-MO Proxy (DSMR) for the results in this result group. The protocol is ANSI-41/IS-41.
mode	Algorithm used by this result group. If mode is not configured, then the mode defaults to WRR.
wrr	Weighted round-robin algorithm is used by this result group to select a result.
dest-sme-binding	Dynamic B-address binding algorithm is used by this result group to select a result. This mode uses a weighted distribution algorithm that binds a set of B-addresses to the same available result.

Defaults

The default instance is 0.

The default mode is WRR.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The result group lists the appropriate destination resources and the mechanism used to select a single destination for a given packet. State information is determined for each possible destination. Only available destinations are considered for routing. Note, however, that the distribution algorithms consider GT results to be always available. Ensure that the proper GT configuration is in place and available for GT routing.

MLR provides the following result group distributions modes:

- **Weighted round-robin (WRR)**

This distribution algorithm properly balances SMS workload to servers of varying capacity. Each server within a result group (application group or multilayer result table) is assigned a server weight from 0 to 10. The value of 0 indicates that the server is a backup, and should be used only when all of the servers in the group with a nonzero weight have failed. Congested resources are used only if no available, noncongested destinations exist.

- **Dynamic B-address binding**

This mode uses a hashing algorithm based on the message's B-address to determine which result (SMSC) a message is to be routed to for delivery. The algorithm selects the same result (SMSC) each time based on the B-address to prevent out-of-order messaging. SMSCs with greater capacity are configured as such using the result's **weight** keyword. The results (SMSCs) are inserted into the result group using the **order** keyword. If an unplanned SMSC outage occurs (in other words, if a result is unavailable), then these messages destined for the unavailable SMSC are rerouted to the remaining SMSCs. Note that an SMSC outage does not affect the mapping for available SMSCs. This algorithm handles routing of alphanumeric B-addresses, as well as numeric B-addresses.

SMS MO Proxy sms-mo messages can use MLR result groups with WRR or dest-sme-binding mode. This ITP enhancement was introduced to simplify configuration because both SMS MO Proxy and MLR dest-sme-binding result groups must be identically configured in an SMS MO Proxy solution. However, DMSR does not currently support **asname** command results within an SMS result group. DMSR can reference only those MLR groups that contain no **asname** results.

Examples

The following example shows how to identify a multilayer result group named vas-grp:

```
cs7 mlr result vas-grp
  asname voting-as1 weight 1
  asname voting-as2 weight 1
  pc 3.3.1 weight 0
  pc 3.3.2 weight 0
  pc 3.3.3 weight 0
```

The following example shows how to identify a multilayer result group named MLR-BINDING:

```
cs7 instance 0 mlr result MLR-BINDING mode dest-sme-binding
  pc 5.5.3 order 10 weight 20
  pc 1.5.6 order 20 weight 40
  asname AS1 order 30 weight 15
  pc 5.5.6 order 40 weight 60
```

Related Commands	Command	Description
	asname (cs7 mlr result)	Specifies a particular destination M3UA or SUA application server.
	pc (cs7 mlr result)	Specifies the destination point code.
	gt (cs7 mlr result)	Specifies an outbound global title destination from within a result group.
	response-timer (cs7 sms profile parms)	Specifies the processing to perform on a packet matching the specified trigger and rule.
	show cs7 mlr configuration	Displays the result to select from an SMS result group for the specified dest-sme address.
	show cs7 mlr result	Specifies a multilayer result group.

cs7 mlr ruleset

To specify sets of rules to process traffic-matching triggers defined in a multilayer routing table, use the **cs7 mlr ruleset** command in global configuration mode. To remove the rules, provided that no defined MLR triggers are using the ruleset, use the **no** form of this command.

```
cs7 [instance instance-number] mlr ruleset result-name [protocol {gsm-map | ansi-41}]
[event-trace]
```

```
no cs7[instance instance-number] mlr ruleset result-name [protocol {gsm-map | ansi-41}]
[event-trace]
```

instance	(Optional) ITP network instance in which the MLR table is valid. If a table is required in more than one instance, then it must be defined in each appropriate instance. If an instance is not specified, then the table may only be used for the default network instance 0.
<i>instance-number</i>	An integer value in the range 0 to 7. The default instance is 0.
<i>result-name</i>	Identifies a name to be associated with this multilayer ruleset table. The name must be unique among all multilayer ruleset tables. The name is specified as a character string with a maximum of 12 characters.
protocol	(Optional) Specifies an application layer protocol filter for this ruleset.
gsm-map	(Optional) Uses GSM MAP ¹ as the application layer protocol filter within the ruleset. For networks with mixed application layer protocols, the filter should not be specified so that all protocol operations on the rule statement are allowed.
ansi-41	Uses ANSI-41 ² or IS-41 as the application layer protocol filter within the ruleset. For networks with mixed application layer protocols, the filter should not be specified so that all protocol operations on the rule statement are allowed.

1. GSM 09.02: "Digital cellular telecommunications system (Phase 2+); Mobile Application Part (MAP) Specification", ETSI, document TS 100 974 V7.3.0.
2. TIA/EIA-41-D, Cellular Radiotelecommunications Intersystem Operations, December 1997 SMS flows 3-373.

Defaults

The default instance is 0.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

This command enables cs7 mlr ruleset configuration submode. The command configures rules that customize message routing. When issued, the command enters cs7 mlr set configuration submode. In this submode, the **rule** command is valid.

Examples

The following example shows how to create a ruleset named ruleset-5:

```
cs7 mlr ruleset ruleset-5
rule 10 sms-mo
    dest-sme 1234
    result group vas-grp
rule 20 sms-mo
    dest-sme 5678
    result group vas-grp
```

Related Commands

Command	Description
rule (cs7 mlr ruleset)	Specifies the rules for a routing trigger within a multilayer ruleset table and enables cs7 mlr ruleset rule configuration mode.
show cs7 mlr ruleset	Displays information about the CS7 MLR ruleset.
trigger cdpa (cs7 mlr table)	Specifies the routing key, or trigger, for a multilayer SMS routing table and indicates that the routing trigger is located in the SCCP called party address (CdPA) field of the incoming MSU.
trigger cgpa (cs7 mlr table)	Specifies the routing key, or trigger, for a multilayer SMS routing table and indicates that the routing trigger is located in the SCCP calling party address (CdPA) field of the incoming MSU.

cs7 mlr table

To specify the name of the multilayer SMS routing table and enable cs7 mlr table mode, use the **cs7 mlr table** command in global configuration mode. To disable the multilayer SMS routing feature, use the **no** form of this command.

cs7 [*instance instance-number*] **mlr table** *name*

no cs7 [*instance instance-number*] **mlr table** *name*

Syntax Description	instance	(Optional) ITP network instance in which the MLR table is valid. If a table is required in more than one instance, then it must be defined in each appropriate instance. If instance is not specified, then the table may only be used for the default network instance 0.
	<i>instance-number</i>	Instance number. An integer value in the range 0 to 7. The default instance is 0
	<i>name</i>	Identifies a name to be associated with this multilayer routing table. The name must be unique among all multilayer routing tables. The name is specified as a character string with a maximum of 12 characters.

Defaults The default instance is 0.

Command Modes Global configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines This command enables cs7 mlr table mode.
In the current release, only a single multilayer routing table is allowed.

Examples The following example shows how to specify a CS7 MLR routing table named SMS-TABLE:

```
cs7 mlr table SMS-TABLE
trigger cdpa gt 9991117770 ruleset ruleset-5
cgpa gt 9991116 ruleset ruleset-5
```

The following example shows how to specify a CS7 MLR routing table named SMS-TABLE and that the MLR table is valid in instance 2:

```
cs7 instance 2 mlr table SMS-TABLE
```

Related Commands	Command	Description
	rule (cs7 mlr ruleset)	Specifies the rules for a routing trigger within a multilayer ruleset table and enables cs7 mlr ruleset rule configuration mode.
	show cs7 mlr ruleset	Displays information about the CS7 MLR ruleset.
	trigger cdpa (cs7 mlr table)	Specifies the routing key, or trigger, for a multilayer SMS routing table and indicates that the routing trigger is located in the SCCP called party address (CdPA) field of the incoming MSU.
	trigger cgpa (cs7 mlr table)	Specifies the routing key, or trigger, for a multilayer SMS routing table and indicates that the routing trigger is located in the SCCP calling party address (CdPA) field of the incoming MSU.

cs7 msu-rates notification-interval

To configure a notification interval for MSU rate notifications, use the **cs7 msu-rates notification-interval** command in global configuration mode. To remove the configuration, use the **no** form of this command.

cs7 msu-rates notification-interval *seconds*

no cs7 msu-rates notification-interval *seconds*

Syntax Description	<i>seconds</i> Interval for notifications. Range is from 60 to 3600 seconds. The default is 900 seconds.											
Defaults	900 seconds											
Command Modes	Global configuration											
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>12.2(18)IXA</td><td rowspan="3">This command was introduced.</td></tr><tr><td>12.4(11)SW</td></tr><tr><td>12.2(33)IRA</td></tr></table>		Release	Modification	12.2(18)IXA	This command was introduced.	12.4(11)SW	12.2(33)IRA				
Release	Modification											
12.2(18)IXA	This command was introduced.											
12.4(11)SW												
12.2(33)IRA												
Usage Guidelines	Use the cs7 msu-rates notification-interval command to prevent excessive generation of notifications.											
Examples	The following example shows how to specify a notification interval of 60 seconds: <pre>cs7 msu-rates notification-interval 60</pre>											
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>cs7 msu-rates sample-interval</td><td>Configures the sample interval over which MSU rates are calculated.</td></tr><tr><td>cs7 msu-rates threshold-default</td><td>Configures the global MSU rate threshold ranges and defaults for all processors in the ITP platform.</td></tr><tr><td>cs7 msu-rates threshold-proc</td><td>Configures MSU rate threshold ranges for a specific processor, overriding the global thresholds.</td></tr><tr><td>show cs7 msu-rates</td><td>Displays information about configured SS7 MSU rates.</td></tr></table>		Command	Description	cs7 msu-rates sample-interval	Configures the sample interval over which MSU rates are calculated.	cs7 msu-rates threshold-default	Configures the global MSU rate threshold ranges and defaults for all processors in the ITP platform.	cs7 msu-rates threshold-proc	Configures MSU rate threshold ranges for a specific processor, overriding the global thresholds.	show cs7 msu-rates	Displays information about configured SS7 MSU rates.
Command	Description											
cs7 msu-rates sample-interval	Configures the sample interval over which MSU rates are calculated.											
cs7 msu-rates threshold-default	Configures the global MSU rate threshold ranges and defaults for all processors in the ITP platform.											
cs7 msu-rates threshold-proc	Configures MSU rate threshold ranges for a specific processor, overriding the global thresholds.											
show cs7 msu-rates	Displays information about configured SS7 MSU rates.											

cs7 msu-rates sample-interval

To configure the interval over which MSU rates are calculated, use the **cs7 msu-rates sample-interval** command in global configuration mode. To remove the configuration, use the **no** form of this command.

cs7 msu-rates sample-interval *seconds*

no cs7 msu-rates sample-interval *seconds*

Syntax Description	<i>seconds</i>	Sample interval. Range is from 1 to 60 seconds. The default is 5 seconds.

Defaults	5 seconds

Command Modes	Global configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples	The following example shows how to specify a sample interval of 10 seconds: <pre>cs7 msu-rates sample-interval 10</pre>

Related Commands	Command	Description
	cs7 msu-rates notification-interval	Configures the notification interval used to prevent excessive generation of notifications.
	cs7 msu-rates threshold-default	Configures the global MSU rate threshold ranges and defaults for all processors in the ITP platform.
	cs7 msu-rates threshold-proc	Configures MSU rate threshold ranges for a specific processor, overriding the global thresholds.
	show cs7 msu-rates	Displays information about configured SS7 MSU rates.

cs7 msu-rates threshold-default

To configure the global MSU rate threshold defaults for all processors on the ITP platform, use the **cs7 msu-rates threshold-default** command in global configuration mode. To remove the configuration, use the **no** form of this command.

cs7 msu-rates threshold-default *acceptable warning overloaded*

no cs7 msu-rates threshold-default *acceptable warning overloaded*

Syntax Description

<i>acceptable</i>	Threshold value, in MSUs per second, that indicates an acceptable rate of traffic. This value must be less than both the <i>warning</i> and <i>overloaded</i> values. Range is from 100 to 999999.
<i>warning</i>	Threshold value, in MSUs per second, that indicates a rate of traffic that may impact the device. This value must be greater than the <i>acceptable</i> value and less than the <i>overloaded</i> value. Range is from 100 to 999999.
<i>overloaded</i>	Threshold value, in MSUs per second, that indicates a rate of traffic that impacts operation of the device. This value must be greater than both the <i>acceptable</i> and <i>warning</i> values. Range is from 100 to 999999.

Defaults

This command establishes the default MSU rate threshold values for all processors on the platform.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

Use the **cs7 msu-rates threshold-default** command to establish global thresholds for the acceptable, warning, and overloaded MSU rates of traffic for all processors in the ITP platform. After you establish these global thresholds, you can override them on specific processors with the **cs7 msu-rates threshold-proc** command.

Examples

The examples in this section are intended only to describe the command parameters. They do not represent recommended configurations.

In the following example for a Cisco 7513 ITP platform, the first line defines global thresholds for acceptable, warning, and overloaded MSU rates for all FlexWANs in the ITP platform. Lines 4 and 5 set the threshold values for the Route Processors.

```
cs7 msu-rates threshold-default 2000 3000 6000
cs7 msu-rates sample-interval 1
cs7 msu-rates notification-interval 60
```

```
cs7 msu-rates threshold-proc 6 5000 6000 12000
cs7 msu-rates threshold-proc 7 5000 6000 12000
snmp-server enable traps cs7 msu-rates
```

Related Commands

Command	Description
cs7 msu-rates notification-interval	Configures the notification interval used to prevent excessive generation of notifications.
cs7 msu-rates sample-interval	Configures the sample interval over which MSU rates are calculated.
cs7 msu-rates threshold-proc	Configures MSU rate threshold ranges for a specific processor, overriding the global thresholds.
show cs7 msu-rates	Displays information about configured SS7 MSU rates.

cs7 msu-rates threshold-proc

To override previously defined global MSU rate thresholds and configure the MSU rate thresholds for a specific processor, use the **cs7 msu-rates threshold-proc** command in global configuration mode. To remove the configuration, use the **no** form of this command.

cs7 msu-rates threshold-proc [*slot* [*bay*]] *acceptable* *warning* *overloaded*

no cs7 msu-rates threshold-proc [*slot* [*bay*]] *acceptable* *warning* *overloaded*

Syntax Description	
<i>slot</i>	(Optional) Slot that contains the processor. This keyword applies only to those ITP platforms that support multiple processors.
<i>bay</i>	(Optional) Bay that contains the processor. This keyword applies only to those ITP platforms that support multiple processors.
<i>acceptable</i>	Threshold value in MSUs per second that defines, for the specified processor, an acceptable rate of traffic. This value must be less than both the <i>warning</i> and <i>overloaded</i> values. Range is from 100 to 999999.
<i>warning</i>	Threshold value in MSUs per second that defines, for the specified processor, a rate of traffic that may impact the device. This value must be greater than the <i>acceptable</i> value and less than the <i>overloaded</i> value. Range is from 100 to 999999.
<i>overloaded</i>	Threshold value in MSUs per second that defines, for the specified processor, a rate of traffic that impacts operation of the device. This value must be greater than both the <i>acceptable</i> and <i>warning</i> values. Range is from 100 to 999999.

Defaults The default MSU rate threshold values were globally configured for all processors on the platform with the **cs7 msu-rate threshold-default** command. The **cs7 msu-rate threshold-proc** command overrides those defaults for specified processors.

Command Modes Global configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines You use the **cs7 msu-rates threshold-proc** command to override, for a specified processor, the global thresholds that you previously defined for all processors with the **cs7 msu-rates threshold-default** command. The **cs7 msu-rates threshold-proc** command defines the threshold MSU rates for acceptable, warning, and overloaded rates of traffic on a specific processor in the ITP.

Examples

The examples in this section are intended only to describe the command parameters. They do not represent recommended configurations.

In the following example for a Cisco 7513 ITP platform, the first line defines global thresholds for acceptable, warning, and overloaded MSU rates for all FlexWANs in the ITP platform. Lines 4 and 5 set the threshold values for the Route Processors.

```
cs7 msu-rates threshold-default 2000 3000 6000
cs7 msu-rates sample-interval 1
cs7 msu-rates notification-interval 60
cs7 msu-rates threshold-proc 6 5000 6000 12000
cs7 msu-rates threshold-proc 7 5000 6000 12000
snmp-server enable traps cs7 msu-rates
```

Related Commands

Command	Description
cs7 msu-rates notification-interval	Configures the notification interval used to prevent excessive generation of notifications.
cs7 msu-rates sample-interval	Configures the sample interval over which MSU rates are calculated.
cs7 msu-rates threshold-default	Configures the global MSU rate threshold ranges and defaults for all processors in the ITP platform.
show cs7 msu-rates	Displays information about configured SS7 MSU rates.

cs7 mtp3 crd

Circular route detection occurs when an MSU flows through an SS7 network and traverses a path that takes it back to the originating point code. CRD recognizes the behavior and disables the route.

To turn on circular route detection, use the **cs7 mtp3 crd** command in global configuration mode. To turn off the feature, use the **no** form of this command.

cs7 mtp3 crd

no cs7 mtp3 crd

Syntax Description

This command has no arguments or keywords.

Defaults

For the ANSI variant, CRD is on. For all other variants, CRD is off.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXG	This command was introduced.
12.4(15)SW2	
12.2(33)IRB	

Usage Guidelines

The following restrictions apply to this command:

- If the ITP has a mate and one or more C-link linksets are already configured, then these linksets must be identified in the configuration for correct operation of OPC verification.
- Because both CRD and OPC verification are on by default for ANSI, you must turn off CRD before making any changes to a C-link linkset configuration.
- The CRD default for all other variants is off, but if CRD is turned on in the configuration, you need to turn it off before changing the C-link linkset configuration.
- If CRD is on for either ANSI or another variant, then C-links may fail due to dropped link test messages.

For ITU and similar variant national options, you must configure multiple congestion levels before enabling CRD.

Examples

The following example shows how to enable CRD:

```
cs7 mtp3 crd
```

Related Commands	Command	Description
	show cs7 route	Displays the ITP routing table.
	cs7 mtp3 timer	Configures MTP3 management timers including the loop detection timer.

cs7 mtp3 event-history

To specify the maximum number of events to store in memory, use the **cs7 mtp3 event-history** command in global configuration mode. To return to the default number of events to store (512), use the **no** form of this command.

cs7 [**instance** *instance-number*] **mtp3 event-history** *number*

no cs7 [**instance** *instance-number*] **mtp3 event-history**

Syntax Description	instance	(Optional) Specifies the maximum number of events to store in memory for an instance.
	instance-number	Instance number. The valid range is 0 to 7. The default instance is 0.
	number	Maximum number of events to log in memory. Valid range is 0 to 5000. The default number is 512. Setting the number to 0 removes all saved events and discontinues event logging.

Defaults 512 events are logged.

Command Modes Global configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines Because events are continuously logged in round-robin fashion, new events will overwrite the old ones when the maximum value is reached.

Examples The following example shows how to set the maximum number of events to be logged at 1024:

```
cs7 mtp3 event history 1024
```

The following example shows how to set the maximum number of events to be logged to 1024 for instance 2:

```
cs7 instance 2 mtp3 event history 1024
```


Related Commands	Command	Description
	cs7 mtp3 tuning rx-congestion-threshold	Enables multiple instances of a variant and network indicator combination.
	show cs7 mtp3 event-history	Displays logged events exchanged among the three MTP components (traffic, link, and route management).

cs7 mtp3 timer

To configure the ITP MTP3 management timers globally, use the **cs7 mtp3 timer** command in global configuration mode. To reset a timer to its default value, use the **no** form of this command.

```
cs7 [instance instance-number] mtp3 timer {retry msec | slt-t1 msec | slt-t2 msec | t01 msec | t02 msec | t03 msec | t04 msec | t05 msec | t6 msec | t8 msec | t10 msec | t11 msec | t12 msec | t13 msec | t14 msec | t15 msec | t16 msec | t17 msec | t18 msec | t19 msec | t20 msec | t21 msec | t22 msec | t23 msec | t24 msec | t25 msec | t26 msec | t28 msec | t29 msec | t30 msec | t32 msec | tc msec} | loop msec
```

```
no cs7 [instance instance-number] mtp3 timer {retry | slt-t1 | slt-t2 | t01 | t02 | t03 | t04 | t05 | t6 | t8 | t10 | t11 | t12 | t13 | t14 | t15 | t16 | t17 | t18 | t19 | t20 | t21 | t22 | t23 | t24 | t25 | t26 | t28 | t29 | t30 | t32 | tc msec} | loop msec
```



Note

Ranges are defined by ANSI, ITU, or TTC. MTP3 timer values for the China variant are the same as ITU. When used, the MTP3 timer values for TTC match ITU.

Syntax Description

instance	(Optional) Configures the ITP MTP3 management timers globally on an instance.
<i>instance-number</i>	Instance number. An integer value in the range 0 to 7.
retry msec	(ANSI, ITU) Link activation retry timer. (ANSI, ITU) Range of <i>msec</i> is 60000 to 90000 milliseconds. Default is 60000 milliseconds.
slt-t1 msec	(ANSI, ITU) Link test acknowledgment timer. (ANSI, ITU) ITU Range of <i>msec</i> is 4000 to 12000 milliseconds. Default is 8000 milliseconds.
slt-t2 msec	(ANSI, ITU) Interval timer for sending test messages. (ANSI, ITU) Range of <i>msec</i> is 30000 to 90000 milliseconds. (ANSI, ITU) Default is 60000 milliseconds.
t01 msec	(ANSI, ITU, TTC) Delays to avoid message missequencing. (ANSI, ITU, TTC) Range of <i>msec</i> is 500 to 1200 milliseconds. (ANSI, ITU, TTC) Default is 800 milliseconds.
t02 msec	(ANSI, ITU, TTC) Waits for changeover acknowledgment. (ANSI, ITU, TTC) Range of <i>msec</i> is 700 to 2000 milliseconds. (ANSI, ITU, TTC) Default is 1400 milliseconds.
t03 msec	(ANSI, ITU, TTC) Delays to avoid missequencing in changeback. (ANSI, ITU, TTC) Range of <i>msec</i> is 500 to 1200 milliseconds. (ANSI, ITU, TTC) Default is 800 milliseconds.
t04 msec	(ANSI, ITU, TTC) Waits for changeback acknowledgment (first attempt). (ANSI, ITU, TTC) Range of <i>msec</i> is 500 to 1200 milliseconds. (ANSI, ITU, TTC) Default is 800 milliseconds.
t05 msec	(ANSI, ITU) Waits for changeback acknowledgment (second attempt). (ANSI, ITU) Range of <i>msec</i> is 500 to 1200 milliseconds. (ANSI, ITU) Default is 800 milliseconds.

t06 msec	(ANSI, ITU, TTC) Delays to avoid message missequencing on controlled rerouting. (ANSI, ITU, TTC) Range of <i>msec</i> is 500 to 1200 milliseconds. (ANSI, ITU, TTC) Default is 800 milliseconds.
t08 msec	(ANSI, ITU, TTC) Transfer-prohibited inhibited timer. (ANSI, ITU, TTC) Range of <i>msec</i> is 800 to 1200 milliseconds. (ANSI, ITU, TTC) Default is 1000 milliseconds.
t10 msec	(ANSI, ITU, TTC) Waits to repeat signaling-route-set-test message. (ANSI, ITU, TTC) Range of <i>msec</i> is 30000 to 60000 milliseconds. (ANSI, ITU, TTC) Default is 45000 milliseconds.
t11 msec	(ANSI, ITU) Transfer-restricted timer. (ANSI, ITU) Range of <i>msec</i> is 30000 to 90000 milliseconds. (ANSI, ITU) Default is 60000 milliseconds.
t12 msec	(ANSI, ITU) Waits for uninhibited acknowledgment. (ANSI, ITU) Range of <i>msec</i> is 800 to 1500 milliseconds. (ANSI, ITU) Default is 1150 milliseconds.
t13 msec	(ANSI, ITU) Waits for force uninhibited. (ANSI, ITU) Range of <i>msec</i> is 800 to 1500 milliseconds. (ANSI, ITU) Default is 1150 milliseconds.
t14 msec	(ANSI, ITU) Waits for inhibition acknowledgment. (ANSI, ITU) Range of <i>msec</i> is 2000 to 3000 milliseconds. (ANSI, ITU) Default is 2500 milliseconds.
t15 msec	(ANSI) Waits to repeat signaling-route-set-congestion test. (ITU, TTC) Waits to start route-set-congestion test. (ANSI, ITU, TTC) Range of <i>msec</i> is 2000 to 3000 milliseconds. (ANSI, ITU, TTC) Default is 2500 milliseconds.
t16 msec	(ANSI, ITU, TTC) Waits for route-set-congestion update. (ANSI, ITU, TTC) Range of <i>msec</i> is 1400 to 2000 milliseconds. (ANSI, ITU, TTC) Default is 1700 milliseconds.
t17 msec	(ANSI, ITU) Delays to avoid oscillation of alignment failure and link restart. (ANSI, ITU) Range of <i>msec</i> is 800 to 1500 milliseconds. (ANSI, ITU) Default is 1150 milliseconds.
t18 msec	(ANSI) Repeats TFR once by response method. (ANSI) Range of <i>msec</i> is 2000 to 20000 milliseconds. (ANSI) Default is 11000 milliseconds. (ITU) MTP restarts for supervising link and link set activation. (ITU) Range of <i>msec</i> is 1000 to 31000 milliseconds. (ITU) Default is 30000 milliseconds.
t19 msec	(ANSI) Failed link craft referral timer. (ANSI) Range of <i>msec</i> is 480000 to 600000 milliseconds. (ANSI) Default is 540000. (ITU) Supervision timer during MTP restart. (ITU) Range of <i>msec</i> is 67000 to 69000 milliseconds. (ITU) Default is 68000 milliseconds.

t20 msec	(ANSI) Waits to repeat local inhibit test. (ANSI) Range of <i>msec</i> is 90000 to 120000 milliseconds. (ANSI) Default is 105000 milliseconds. (ITU) MTP restart timer at the signaling point whose MTP restarts. (ITU) Range of <i>msec</i> is 1000 to 61000 milliseconds. (ITU) Default is 60000 milliseconds.
t21 msec	(ANSI) Waits to repeat remote inhibit test. (ANSI) Range of <i>msec</i> is 90000 to 120000 milliseconds. (ANSI) Default is 105000 milliseconds. (ITU) MTP restart timer at signaling point adjacent to one whose MTP restarts. (ITU) Range of <i>msec</i> is 63000 to 65000 milliseconds. (ITU) Default is 64000 milliseconds.
t22 msec	(ANSI) Timer at restarting SP waiting for signaling links to become available. (ANSI) Range of <i>msec</i> is 36000 to 60000 milliseconds. (ANSI) Default is 30000 milliseconds. (ITU) Local inhibit test timer. (ITU) Range of <i>msec</i> is 180000 to 360000 milliseconds. (ITU) Default is 300000 milliseconds.
t23 msec	(ANSI) Timer at restarting SP with transfer function, started after T22, waiting to broadcast all traffic restart allowed messages. (ANSI) Range of <i>msec</i> is 9000 to 60000 milliseconds. (ANSI) Default is 30000 milliseconds. (ITU) Remote inhibit test timer. (ITU) Range of <i>msec</i> is 180000 to 360000 milliseconds. (ITU) Default is 300000 milliseconds.
t24 msec	(ANSI) Timer at restarting SP with transfer function, started after T23, waiting to broadcast all traffic restart allowed messages. (ANSI) Range of <i>msec</i> is 9000 to 60000 milliseconds. (ANSI) Default is 30000 milliseconds. (ITU) Stabilizing timer after removal of local processor outage, used in LPO latching to RPO. (ITU) Only valid value for <i>msec</i> is 500 milliseconds. (ITU) Default is 500 milliseconds.
t25 msec	(ANSI) Timer at SP adjacent to restarting SP waiting for traffic restart allowed message. (ANSI) Range of <i>msec</i> is 30000 to 35000 milliseconds. (ANSI) Default is 30000 milliseconds.
t26 msec	(ANSI) Timer at restarting SP waiting to repeat traffic restart waiting message. (ANSI) Range of <i>msec</i> is 12000 to 15000 milliseconds. (ANSI) Default is 12000 milliseconds.
t28 msec	(ANSI) Timer at SP adjacent to restarting SP waiting for traffic restart waiting message. (ANSI) Range of <i>msec</i> is 3000 to 35000 milliseconds. (ANSI) Default is 30000 milliseconds.

t29 msec	(ANSI) Timer started when TRA sent in response to unexpected TRA or TRW. (ANSI) Range of <i>msec</i> is 60000 to 65000 milliseconds. (ANSI) Default is 63000 milliseconds.
t30 msec	(ANSI) Timer to limit sending TFPs and TFRs in response to unexpected TRA and TRW. (ANSI) Range of <i>msec</i> is 30000 to 35000 milliseconds. (ANSI) Default is 33000 milliseconds.
t32 msec	(ANSI) Link oscillation timer - Procedure A. Range of <i>msec</i> is 60000 to 120000 milliseconds. Default is 60000 milliseconds.
tc msec	(TTC) Congestion test timer. Range of <i>msec</i> is 3000 to 30000. Default is 3000 milliseconds.
tloop msec	Loop detection timer. The timer value is in the range 10000 to 20000 milliseconds. The default value is 10000 milliseconds.

Defaults

See Syntax Description.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.
12.2(18)IXG 12.4(15)SW2 12.2(33)IRB	The tloop keyword was added.

Usage Guidelines

MTP3 timers can be defined at three levels: global, linkset, and link.

All global-, linkset-, and link-specific timers can be defined at the global level. These values serve as defaults and are propagated down to the lower levels.

All linkset- and link-specific timers can be defined at the linkset level. These values serve as defaults for the linkset and all links defined within that linkset. Any values defined here override any global values.

All timers defined at the link level apply to the link and override any values for that timer defined at either the linkset or global level.

Examples

The following example shows how to set the ITP MTP3 T6 timer to 1000 milliseconds:

```
cs7 mtp3 timer t6 1000
```

The following example shows how to set the ITP MTP3 T6 timer to 1000 milliseconds:

```
cs7 mtp3 timer t6 1000
```

Related Commands	Command	Description
	cs7 mtp3 tuning rx-congestion-threshold	Enables multiple instances of a variant and network indicator combination.
	link-timer	Configures timers for a link.
	show cs7 mtp3 timers	Displays the values of the MTP3 timers.
	timer (cs7 linkset)	Configures timers for a linkset (and, optionally, timers for links on the linkset).
	cs7 mtp3 crd	Turns on circular route detection.

cs7 mtp3 tuning

To specify MTP3 performance tuning parameters, use the **cs7 mtp3 tuning** command in global configuration mode. To return to the default MTP3 tuning parameters, use the **no** form of this command.

cs7 mtp3 tuning {**buffered-packet-threshold** *bufferedPaks* | **rx-congestion-threshold** *queuedPaks*}

no cs7 mtp3 tuning {**buffered-packet-threshold** *bufferedPaks* | **rx-congestion-threshold** *queuedPaks*}

Syntax Description	buffered-packet-threshold <i>bufferedPaks</i>	Number of packets buffered at MTP3 for changeover/changeback after which packets begin being dropped. The range is 1000 to 80000 buffered packets per ITP. The default is 20000 buffered packets for each ITP.
	rx-congestion-threshold <i>queuedPaks</i>	Percentage of the maximum number of packets on the MTP3 link's interface input queue at which the link is declared to be congested. The range is 0 to 100. The default percentage is 50.

Defaults

The default buffered-packet threshold is 20000 packets for each ITP.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Examples

The following example shows how to set the buffered-packet threshold to 1000 and the rx-congestion threshold to 50 percent:

```
cs7 mtp3 tuning buffered-packets-threshold 1000 rx-congestion-threshold 50
```

Related Commands

Command	Description
cs7 mtp3 timer	Configures MTP3 timers.
cs7 mtp3 tuning rx-congestion-threshold	Enables multiple instances of a variant and network indicator combination.
show cs7 mtp3 timers	Displays the values of the MTP3 timers.

cs7 mtp3 tuning rx-congestion-threshold

To specify the value of the rx-queue-depth, use the **cs7 mtp3 tuning rx-congestion-threshold** command in global configuration mode. To return to the default rx-queue-depth, use the **no** form of this command.

cs7 mtp3 tuning rx-congestion-threshold {mtp2-link | mtp2-hsl-link | m2pa-link | atm-hsl-link}
rx-queue-depth

Syntax Description

<i>rx-queue-depth</i>	The configurable number of packets that the congestion onset threshold and the congestion abatement threshold are based on (20-20000).
mtp2-link	Specifies the rx-queue-depth is for all serial links.
mtp2-hsl-link	Specifies the rx-queue-depth is for all Q.703 links.
m2pa-link	Specifies the rx-queue-depth is for all M2PA links.
atm-hsl-link	Specifies the rx-queue-depth is for all ATM HSL links.

Defaults

The defaults for the *rx-queue-depth* are listed below:

serial link	500 packets
Q.703	5000 packets
M2PA	1000 packets
ATM HSL	1000 packets

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)SW5	This command was introduced.
12.2(33)IRE	

Usage Guidelines

The congestion onset threshold is defined as 50% of the rx-queue-depth, and the congestion abate threshold is defined as 30% of the rx-queue-depth.

Examples

You can display information on the following link types with the **show-running config** command:

The following example shows the *rx-queue-depth* configured at 10,000 for a serial link:

```
cs7 mtp3 tuning rx-congestion-threshold mtp2-link 10000
```

The following example shows the *rx-queue-depth* configured at 10,000 for a Q.703 link:

```
cs7 mtp3 tuning rx-congestion-threshold mtp2-hsl-link 10000
```

The following example shows the *rx-queue-depth* configured at 10,000 for a M2PA link:


```
cs7 mtp3 tuning rx-congestion-threshold m2pa-link 10000
```

The following example shows the *rx-queue-depth* configured at 10,000 for an ATM HSL link:

```
cs7 mtp3 tuning rx-congestion-threshold atm-hsl-link 10000
```

Related Commands

Command	Description
show cs7 m2pa	Displays M2PA link information including congestion.
show cs7 mtp2	Displays Q.703 link information including congestion.
show cs7 hsl congestion	Displays ATM HSL link information including congestion.

cs7 multi-instance

To enable multiple instances of a variant and network indicator combination, use the **cs7 multi-instance** command in global configuration mode. To disable multiple instances, use the **no** form of this command.

cs7 multi-instance

no cs7 multi-instance

Syntax Description This command has no arguments or keywords.

Defaults None.

Command Modes Global configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

Use the **cs7 multi-instance** command to enable multiple variants and network indicator combinations to run concurrently on one ITP. Up to eight instances can be configured.

The multiple instance feature cannot be enabled until the default instance is first assigned a variant.

Examples

The following example shows how to enable the configuration of multiple variant and network indicator “instances”:

```
cs7 multi-instance
```

Related Commands

Command	Description
cs7 local-sccp-addr-ind	Customizes the setting of the national use field within SCCP management calling and called party addresses.
cs7 variant	Indicates which of the SS7 variations the ITP is running on an instance.

cs7 national-options

To configure national options, use the **cs7 national-options** command in global configuration mode. To remove national options, use the **no** form of this command.

cs7 [*instance instance-number*] **national-options** { **tfr** | **multiple-congestion** | **route-set-congestion-test** | **combined-linkset-loadsharing** }

no cs7 [*instance instance-number*] **national-options**

Syntax Description	instance	(Optional) Configures national options on an instance.
	<i>instance-number</i>	Instance number. An integer value in the range 0 to 7.
	tfr	(Applies to ITU and China SS7 variants.) Sends Transfer Restricted Messages.
	multiple-congestion	(Applies to ITU and China SS7 variants.) Uses multiple congestion levels.
	route-set-congestion-test	(Applies to TTC SS7 variant.) Enables route set congestion test (RSCT).
	combined-linkset-loadsharing	(Applies to TTC SS7 variant.) Allows ITPs with the TTC variant to use the enhanced loadsharing algorithm.

Defaults None.

Command Modes Global configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines The national options apply to the variants as follows:

- **TFR:** ITU and China SS7 variants
- **multiple-congestion:** ITU and China SS7 variants
- **route-set-congestion-test:** TTC SS7 variant
- **combined-linkset-loadsharing:** TTC SS7 variant

Before Release 12.2(25)SW1, all SS7 variants used an enhanced loadsharing algorithm for distributing messages across the available links within a linkset and combined linkset. (This algorithm allows for efficient load balancing when an unequal number of available links exists in the two linksets that comprise the combined linkset.) In Release 12.2(25)SW1, the TTC variant reverted to using the A/B

linkset selection bit that exists as part of the SLS in the MSU routing label. To allow ITPs configured with the TTC variant to use the enhanced loadsharing algorithm, specify the **combined-linkset-loadsharing** keyword.

To display national options, use the **show running config** command.

Refer to Q.704 section 11.2.4 for multiple-congestion, and Q.704 section 13.4 for TFR.

Examples

The following example shows how to configure the national options to send transfer restricted messages:

```
cs7 national-options TFR
```

Related Commands

Command	Description
cs7 mtp3 tuning rx-congestion-threshold	Enables multiple instances of a variant and network indicator combination.
cs7 variant	Specifies which of the SS7 variations the router is running.
encapsulation mtp2	Specifies MTP2 encapsulation.
mtp2-timer	Configures MTP2 encapsulation timers.
show cs7 mtp2	Displays ITP MTP2 status.

cs7 network-indicator

To configure the network indicator, use the **cs7 network-indicator** command in global configuration mode. To return to the default, use the **no** form of this command.

cs7 [*instance instance-number*] **network-indicator** {**international** | **national** | **reserved** | **spare**}

no cs7 [*instance instance-number*] **network-indicator**

Syntax Description

instance	(Optional) Configures the network indicator on an instance.
<i>instance-number</i>	Instance number. An integer value in the range 0 to 7.
international	International network.
national	National network.
reserved	Reserved for national use.
spare	Reserved for international use.

Defaults

National network

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Examples

The following example shows how to configure the network indicator to international:

```
cs7 network-indicator international
```

The following example shows how to configure the network indicator to international on instance 3:

```
cs7 instance 3 network-indicator international
```

Related Commands

Command	Description
cs7 mtp3 tuning rx-congestion-threshold	Enables multiple instances of a variant and network indicator combination.
cs7 variant	Specifies which of the SS7 variations (ANSI or ITU) the router is running.
encapsulation mtp2	Specifies MTP2 encapsulation.
mtp2-timer	Configures MTP2 encapsulation timers.
show cs7 mtp2	Displays ITP MTP2 status.

cs7 network-name

To specify a network name for a signaling point, use the **cs7 network-name** command in global configuration mode. To remove the name, use the **no** form of this command.

cs7 [**instance** *instance-number*] **network-name** *network-name*

no cs7 [**instance** *instance-number*] **network-name** *network-name*

Syntax Description	instance	(Optional) Specifies a network name for a signaling point on an instance.
	instance-number	Instance number. An integer value in the range 0 to 7.
	network-name	Network name. Valid names are text strings up to 19 characters long.
Defaults	None.	
Command Modes	Global configuration	
Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	
Usage Guidelines	The network name allows network management to group signaling points by network. The network name is not required for instance 0. For all other instances, the name must be specified after the variant and before all other commands for the instance.	
Examples	The following example shows how to specify the network name hr:	
	cs7 network-name hr	
	The following example shows how to specify the network name hr for instance 2:	
	cs7 instance 2 network-name hr	
Related Commands	Command	Description
	cs7 mtp3 tuning rx-congestion-threshold	Enables multiple instances of a variant and network indicator combination.

cs7 nso

To enable ITP Nonstop Operation (NSO), use the **cs7 nso** command in global configuration mode. To disable ITP NSO, use the **no** form of this command.

cs7 nso

no cs7 nso

Syntax Description This command has no arguments or keywords.

Defaults None.

Command Modes Global configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines Issuing the **no cs7 nso** command reloads the standby Route Processor, if it is present. Reloading occurs because the ITP protocols on the standby Route Processor must revert to the state required for RPR+ operation. This state is the default for ITP if the redundancy mode is SSO and NSO is not configured.

Examples The following example shows how to enable NSO:

```
cs7 nso
```

Related Commands	Command	Description
	show cs7 nso	Displays NSO information.

cs7 offload mtp3

To enable MTP3 offload (line card to line card forwarding of MSUs), use the **cs7 offload mtp3** command in global configuration mode. To remove the configuration, use the **no** form of this command.

cs7 offload mtp3

no cs7 offload mtp3

Syntax Description

This command has no arguments or keywords.

Defaults

MTP3 offload is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The **cs7 offload mtp3** command activates MTP3 offload on all line cards.

MTP3 offload and the Instance Translation feature are mutually exclusive. MTP3 offload cannot be enabled if the Instance Translation feature has been configured, and the Instance Translation feature cannot be enabled if MTP3 offload has been configured.

The **cs7 offload mtp3** command takes effect when the ITP is reloaded.

Examples

The following example shows how to enable the ITP to forward MSUs between line cards without involving the Route Processor:

```
cs7 offload mtp3
```

Related Commands

Command	Description
show cs7	Displays the ITP basic configuration and indicates if MTP3 offload is enabled.

cs7 offload mtp3 restart

To enable the ITP software to reload IOS microcode on a line card on which MTP3 offload has been permanently disabled by the MTP3 offload feature (due to excessive errors), use the **cs7 offload mtp3 restart** privileged EXEC command. Because the command can only be issued for a physical slot, it reloads both bays (CPUs) on the FlexWAN.

cs7 offload mtp3 slot restart

Syntax Description	<i>slot</i> Line card slot number.				
Defaults	None.				
Command Modes	Privileged EXEC				
Usage Guidelines	When this command is issued, the ITP performs an immediate microcode reload on the specified line card by simulating an online insertion and removal (OIR) of the line card. This command should be used only when a particular line card has been permanently disabled by the MTP3 offload feature, due to excessive errors. In most error situations, the MTP3 offload feature automatically performs error recovery. However, if successive recovery attempts do not eliminate the error conditions, all links on the line card are deactivated, and the MTP3 offload feature is disabled on that line card.				
 Note	To perform an OIR of a line card, you must first execute the no power enable module <i>module_slot_number</i> CLI command.				
Examples	Assuming the line card in slot 0 is marked as permanently disabled, the following example shows how to load IOS microcode on the line card in slot 0: <pre>cs7 offload mtp3 0 restart</pre>				
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>show cs7 offload</td><td>Displays the current status of MTP3 offload on each line card.</td></tr></table>	Command	Description	show cs7 offload	Displays the current status of MTP3 offload on each line card.
Command	Description				
show cs7 offload	Displays the current status of MTP3 offload on each line card.				

cs7 paklog

To configure the ITP Packet Logging facility, use the **cs7 paklog** command in global configuration mode. To remove the configuration, use the **no** form of this command.

cs7 paklog *dest-ip* **dest-port** *dest-port* [**severity** *severity*] [**facility** *facility*] [**src-port** *src-port*] [**hostname** *hostname*]

no cs7 paklog *dest-ip* **dest-port** *dest-port* [**severity** *severity*] [**facility** *facility*] [**src-port** *src-port*] [**hostname** *hostname*]

Syntax Description		
<i>dest-ip</i>		Destination IP address of the syslog receiving host.
dest-port <i>dest-port</i>		Indicates the destination IP port of the remote syslog receiving port. Valid range is port number 1 to 65535.
severity <i>severity</i>		(Optional) Specifies the severity of the message. Valid range is 0 to 7. If no severity is specified, the default is severity level 7, debug level severity.
facility <i>facility</i>		(Optional) Specifies the facility for the message. Valid range is 0 to 23. If no facility is specified, the default facility is 16, "local use 0."
src-port <i>src-port</i>		(Optional) Specifies the source IP port of the UDP syslog message. Valid range is port number 1 to 65535. If no source IP port is specified, the default source port 10000 is assigned.
hostname <i>hostname</i>		(Optional) Specifies a hostname to be sent in the syslog message. If no hostname is specified, the local ITP host name is assigned.

Defaults

If no severity is specified, the default is severity level 7, debug level severity.
 If no facility is specified, the default facility is 16, "local use 0."
 If no source IP port is specified, the default source port 10000 is assigned.
 If no hostname is specified, the local ITP host name is assigned.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The ITP Packet Logging facility uses the BSD Syslog protocol (RFC 3164) to send selected MSUs to a user-selected monitoring tool via the UDP connectionless protocol (RFC 768). Cisco does not provide monitoring tools specifically for receiving and decoding messages sent by the facility. You must obtain a suitable tool for receiving syslog messages.

Under normal conditions, using the ITP Packet Logging facility does not impact system performance. However, if packet logging is configured incorrectly, system performance can be diminished during periods of high traffic.

Examples

The following example shows how to specify a CS7 access list. The access list permits packets to be logged, specifies the destination IP address and port number of the host that will receive the packets, and specifies the source IP port of the UDP syslog message.

```
cs7 paklog 64.102.85.109 dest-port 514

access-list 2700 instance 0 permit all

debug cs7 mtp3 paklog 2700
```

Related Commands

Command	Description
access-list	Defines a Cisco ITP access list.

cs7 pam

To identify a packet address modification (PAM) table and enter the CS7 PAM submode, use the **cs7 instance pam** command in global configuration mode. To remove the identify of the PAM table, use the **no** form of this command.

cs7 instance *instance-number* **pam** *pam-name*

no cs7 instance *instance-number* **pam** *pam-name*

Syntax Description

pam	The keyword that indicates a PAM table identity is being set.
<i>pam-name</i>	The identifying name of the PAM table. The name is specified as an alpha-numeric character string with a maximum of 12 characters.

Defaults

None.

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)SW5	This command was introduced.
12.2(33)IRE	

Usage Guidelines

MLR modify-profile and PAM cannot be configured simultaneously.

Examples

The following example shows a PAM table named alpha in instance 1:

```
cs7 instance 1 pam alpha
```

Related Commands

Command	Description
cgpa (cs7 pam)	Configures one cgpa entry in the PAM table.
cdpa (cs7 pam)	Configures one cdpa entry in the PAM table.
opc	Configures an opc entry in the PAM table.
dpc	Configures a dpc entry in the PAM table.
modify-failure (pam)	Specifies the desired action when the PAM table packet modification fails.
cs7 gws action-set	Defines gateway screening action sets that may include a PAM table.
gta asname	Creates or modifies a GTA entry that translates to an M3UA or SUA application server name. The GTA entry may include a PAM table.

cs7 pc-conversion

To configure instance translation, use the **cs7 instance pc-conversion** command in global configuration mode. To remove the instance translation virtual link, use the **no** form of this command.

cs7 instance *instance-number* **pc-conversion** *pc* **alias-pc** *alias-instance* *alias-pc*

no cs7 instance *instance-number* **pc-conversion** *pc* **alias-pc** *alias-instance* *alias-pc*

Syntax Description

<i>instance-number</i>	Instance number of the real point code. The valid range is 0 to 7.
<i>pc</i>	CS7 point code. This point code must already exist in the instance's routing table.
alias-pc	Maps the alias point code to the real point code.
<i>alias-instance</i>	Instance number of the alias point code. The valid range is 0 to 7.
<i>alias-pc</i>	Alias point code. This point code must not already exist in the alias instance's routing table.

Defaults

None.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

Instance translation is the conversion of packets between two instances on the ITP, which creates a virtual link between the instance of the real point code and the instance of the alias point code.

This command configures a mapping between *pc* in instance *instance-number* and *alias-pc* in *alias-instance*. If an MSU arrives destined for *alias-pc* in instance *alias-instance*, the ITP sends it to instance *instance* and converts the DPC to *pc*.

Examples

The following example shows how to map the alias point code to the real point code:

```
cs7 instance 0 pc-conversion 1.1.1 alias-pc 1 2.2.5
cs7 instance 1 pc-conversion 1.1.1 alias-pc 0 1.1.3
```

Related Commands

Command	Description
show cs7 virtual-linkset	Displays information about virtual linksets, including link utilization and associated measurements.
show cs7 pc-conversion	Displays the status of the instance translation.

cs7 pc-conversion default

Default conversion sends any MSUs with unknown point codes (PCs) in one instance to another instance. Also, any PCs in the MSU that require conversion but do not have an alias point code assigned to them are unchanged in the new instance.

To configure the default conversion, use the **cs7 instance pc-conversion default** command in global configuration mode. To disable default conversion, use the **no** form of this command.

cs7 instance *dest-instance* **pc-conversion default** *orig-instance* [**no-route**]

no cs7 instance *dest-instance* **pc-conversion default** *orig-instance* [**no-route**]

Syntax Description	
<i>dest-instance</i>	Indicates the instance where the MSUs are sent. Valid range is 0 to 7.
<i>orig-instance</i>	Indicates the instance where the MSUs originate. Valid range is 0 to 7.
no-route	Allows messages to be converted to the new instance without conversion statements being configured for the source point code addressing. If this keyword is specified, unknown point codes are not sent to another instance. However, any PCs in MSUs that require conversion but do not have an alias point code assigned are unchanged in the new instance. This design helps prevent alias point codes for the source point code (OPC or CGPA PC) being entered when an MSU is converted to a new instance. Because this keyword does not enter a summary route between instances, fewer restrictions apply to its use.

Defaults

Any MSUs with unknown point codes in one instance are sent to another instance.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

This command performs the following actions:

- Enters a summary route for mask length 0 in *orig-instance* that goes over the virtual linkset to *dest-instance*. Any MSUs routed in *orig-instance* that do not match other routes are sent to *dest-instance*. The command does not enter this summary route if the **no-route** keyword is specified.
- Enters a default conversion for point codes between *orig-instance* and *dest-instance*. If point code conversion between the two instances is required, and the point code does not match a specified PC conversion or the ITP's point code, then the point code is unchanged in the new instance and conversion still succeeds.

If you configure default conversion from instance 0 to instance 1, you must configure explicit conversion from instance 1 to instance 0 if you want destinations in instance 0 to allow traffic to be routed from instance 1 to instance 0.

If you configure default routing from one instance to another, we recommend that you also use the **cs7 instance summary-routing-exception** command. For example, instance 0 has a full point code entry for 4.4.4 and has default conversion configured from instance 0 to instance 1:

- If summary-routing-exception is not configured, when 4.4.4 becomes unavailable, the ITP sends MSUs destined for 4.4.4 to instance 1.
- If summary-routing-exception is configured for instance 0, when 4.4.4 becomes unavailable, the ITP sends TFPs for 4.4.4 and does *not* try to route MSUs destined for 4.4.4 to instance 1.

Examples

The following example shows how to send MSUs with unknown point codes in instance 0 to instance 1:

```
cs7 instance 1 pc-conversion default 0
```

The following example shows how to enable the **no-route** keyword for a default conversion. With the **no-route** keyword, you can specify more than one instance for the default conversion.

```
cs7 instance 0 pc-conversion default 1 no-route
cs7 instance 0 pc-conversion default 2 no-route
```

Related Commands

Command	Description
cs7 summary-routing-exception	Disables the use of summary/cluster routes (for the purpose of routing MSU) for an instance.
show cs7 pc-conversion	Displays the status of the instance translation.

cs7 pmp

The probeless monitoring protocol (PMP) is a proprietary ITP UDP protocol that allows copying sent or received ITP MSUs and sending them to a data collection server (DCS).

To turn probeless monitoring on for all linksets and ASes, use the **cs7 pmp** command in global configuration mode. To turn off probeless monitoring, use the **no** form of this command.

cs7 pmp

no cs7 pmp

Syntax Description

This command has no arguments or keywords.

Defaults

Probeless monitoring is off.

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)SW3	This command was introduced.
12.2(33)IRC	

Usage Guidelines

When this command is off (the default), it disables copying at a system level and overrides all provisioned linkset and AS PMP settings. You need to manually enable probeless monitoring at the system level to activate all subtending linkset and AS PMP settings. Table 8 defines this behavior.

Table 28 Global Probeless Monitoring Behavior for Linkset and AS PMP Settings

CS7 PMP	Linkset/AS PMP	Result
On	On	On
On	Off	Off
Off	On or Off	Off

Examples

The following example shows a configuration with the **cs7 pmp** command turned on globally:

```
no ip cef
no ip finger
no ip domain-lookup
!
cs7 variant itu
cs7 point-code 5.100.4
cs7 capability-pc 5.100.14
cs7 pmp
```

Related Commands	Command	Description
	cs7 dcs-group	Identifies a name to be associated with a DCS group.
	cs7 pmp hold-queue	Sets the integer range of PMP hold queue thresholds.
	show cs7 pmp	Displays errors and information about the PMP.
	show cs7 dcs-group	Displays information about the DCS group.
	show cs7 dcs	Displays information about the DCS node.

cs7 pmp congestion-timer

To set the integer range of the PMP congestion timer, use the **cs7 pmp congestion-timer** command in global configuration mode. To remove this configuration and restore the default threshold, use the **no** form of this command.

cs7 pmp congestion-timer *timer*

no cs7 pmp congestion-timer *timer*

Syntax Description

<i>timer</i>	Value of the congestion timer. The valid range is 0 to 60 seconds. The default value is 0.

Defaults

The default congestion timer is 0.

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)SW3	This command was introduced.
12.2(33)IRC	

Usage Guidelines

This command is used with the **cs7 pmp hold-queue command** to control the congestion of PMP packets. The ending of PMP congestion is delayed based on a configurable timer ranging from 0 to 60 seconds. When PMP packets in the hold queue hit the congestion onset threshold, ITP starts a congestion timer. Before the timer expires, the receiving side of the PMP is disabled. When the timer expires, the congestion status is checked based on the queue length against the abate threshold.

Examples

The following configuration excerpt provides an example of the **cs7 pmp congestion-timer** command turned on globally with a *timer* value of 60 seconds:

```
cs7 pmp congestion-timer 60
```

Related Commands

Command	Description
cs7 dcs-group	Identifies a name to be associated with a DCS group.
cs 7 dcs	Identifies a name to be associated with a DCS node.
cs7 pmp	Turns probeless monitoring on for all linksets and ASes.
cs7 pmp hold-queue	Sets the integer range of PMP hold queue thresholds.
show cs7 pmp	Displays errors and information about the PMP.
show cs7 dcs-group	Displays information about the DCS group.
show cs7 dcs	Displays information about the DCS node.

cs7 pmp hold-queue

To set the integer range of PMP hold queue thresholds, use the **cs7 pmp hold-queue** command in global configuration mode. To remove this configuration and restore the default thresholds, use the **no** form of this command.

cs7 pmp hold-queue *abate-threshold onset-threshold*

no cs7 pmp hold-queue *abate-threshold onset-threshold*

Syntax Description

<i>abate-threshold</i>	Value of the abate threshold. The valid range is 64 to 256. The default value is 128.
<i>onset-threshold</i>	Value of the onset threshold. The valid range is 128 to 512. The default value is 256.

Defaults

The default abate threshold is 128 and the default onset threshold is 256.

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)SW3	This command was introduced.
12.2(33)IRC	

Usage Guidelines

This command is used to control the congestion of PMP packets. When PMP packets in the hold queue hit the congestion onset threshold, ITP starts a congestion timer. Before the timer expires, the receiving side of the PMP is disabled. When the timer expires, the congestion status is checked based on the queue length against the abate threshold.

Examples

The following configuration excerpt provides an example of the **cs7 pmp hold-queue** command turned on globally with an *abate-threshold* value of 256 and an *onset-threshold* value of 512:

```
cs7 pmp hold-queue 256 512
```

Related Commands

Command	Description
cs7 pmp	Turns probeless monitoring on for all linksets and ASes.
cs7 pmp congestion-timer	Sets the integer range of the PMP congestion timer.
cs7 ds-group	Identifies a name to be associated with a DCS group.
cs7 ds	Identifies a name to be associated with a DCS node.

cs7 point-code

Each ITP must have a unique local point code that is used to send management messages to adjacent signaling points. To assign a local point code, use the **cs7 point-code** command in global configuration mode. To remove the point code from the instance configuration, use the **no** form of this command.

cs7 [*instance instance-number*] **point-code** *point-code*

no cs7 [*instance instance-number*] **point-code** *point-code*

Syntax Description

instance	(Optional) Assigns a local point code to an instance.
<i>instance-number</i>	Instance number. An integer value in the range 0 to 7.
<i>point-code</i>	Local point code for this router. The ANSI point code range is 0.0.0 to 255.255.255. The ITU point code range is 0.0.0 to 7.255.7.

Defaults

None.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

You must specify the SS7 variant before you can specify the local point code.

You must remove all M3UA, SUA, and linkset configurations before you can remove the local point code.

Examples

The following example shows how to set the local point code to 10.44.254:

```
cs7 point-code 10.44.254
```

The following example shows how to set the local point code for instance 1 to 10.44.254:

```
cs7 instance 1 point-code 10.44.254
```

Related Commands

Command	Description
cs7 mtp3 tuning rx-congestion-threshold	Enables multiple instances of a variant and network indicator combination.

Command	Description
cs7 point-code delimiter	Specifies the point code delimiter.
cs7 point-code format	Modifies the standard point code format.

cs7 point-code delimiter

The delimiter that separates the network, cluster, and member components of a point code can be either a dot (.) or a dash (-). To specify the point code delimiter, use the **cs7 point-code delimiter** command in global configuration mode. To return to the default delimiter (dot), use the **default** keyword.

cs7 [*instance instance-number*] **point-code delimiter** { **dash** | **default** }

no cs7 [*instance instance-number*] **point-code delimiter** { **dash** | **default** }

Syntax Description

instance	(Optional) Specifies the point code delimiter for an instance.
<i>instance-number</i>	Instance number. An integer value in the range 0 to 7.
dash	Specifies a dash (-) as the point code delimiter.
default	Returns the delimiter to the default dot (.).

Defaults

The default point code delimiter is a dot (.).

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

You can modify the default point code bit format and the default delimiter at any time during configuration, without first removing links and linksets.

Examples

The following example shows how to set the local point code delimiter to dash:

```
cs7 point-code delimiter dash
```

The following example shows how to set the local point code delimiter to dash for instance 2:

```
cs7 instance 2 point-code delimiter dash
```

Related Commands

Command	Description
cs7 mtp3 tuning rx-congestion-threshold	Enables multiple instances of a variant and network indicator combination.

cs7 point-code format

The format of point codes can be represented according to the ANSI or ITU standard. To modify either standard on an instance, use the **cs7 point-code format** command in global configuration mode. To return to either standard's default, use the **no** form of this command with the **default** keyword.

cs7 [**instance** *instance-number*] **point-code format** { *l-24* [*l-23* [*l-22*]] } [**description** *string*]
[**default**]

no cs7 [**instance** *instance-number*] **point-code format** { *l-24* [*l-23* [*l-22*]] } [**description** *string*]
default

Syntax Description

instance	(Optional) Modifies the point code format on an instance.
<i>instance-number</i>	Instance number. An integer value in the range 0 to 7.
<i>l-24</i>	Number of bits used for the first component of the point code.
<i>l-23</i>	Number of bits used for the second component of the point code.
<i>l-22</i>	Number of bits used for the third component of the point code.
description	Text description follows.
<i>string</i>	Text description.
default	Uses the default format.

Defaults

The ANSI standard for point code representation is 24 bits partitioned into three segments (for network, cluster, and member), with a default representation of 8.8.8.

The ITU standard for point code representation is 14 bits partitioned into three segments (for network, cluster, and member), with a default representation of 3.8.3.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

Before modifying the point code format, you must first specify which standard SS7 variant the ITP is running. To do so, use the [cs7 variant](#) global configuration command.

You can modify the default point code bit format and the default delimiter at any time during configuration, without first removing links and linksets.

Examples

The following example shows how to set the format for the ITU standard to 2.6.6:

```
cs7 point-code format 2 6 6 description network cluster member
```


The following example shows how to set the format for the ITU standard to 2.6.6 on instance 1:

```
cs7 instance 1 point-code format 2 6 6 description network cluster member
```

Related Commands

Command	Description
cs7 mtp3 tuning rx-congestion-threshold	Enables multiple instances of a variant and network indicator combination.
cs7 variant	Indicates which of the SS7 variations (ANSI or ITU) the router is running.

cs7 profile

To define a profile that you can apply to all links in a linkset, use the **cs7 profile** command in global configuration mode. To remove the configuration, use the **no** form of this command.

cs7 profile *name*

no cs7 profile *name*

Syntax Description	<i>name</i>	Profile name.

Defaults	None.

Command Modes	Global configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	The cs7 profile command enables cs7 profile configuration mode. This command is not instance related and cannot be specified with the instance keyword.

Examples	The following example shows how to define a profile named m2parfc. The profile supports M2PA RFC, configures peer-timer and hold-transport settings, and applies to all the links in the linkset named to_nyc.

```
cs7 profile m2parfc
m2pa
 peer-timer t01 15000
 peer-timer t2 9000
 hold-transport
```

```
cs7 linkset to_nyc
 profile timers
```

The following example shows how to define a profile named timers. The profile supports MTP2, configures the t1 and t2 settings, and applies to all the links in the linkset named to_nyc.

```
cs7 profile timers
mtp2
 timer t1 15000
 timer t2 9000
```

```
cs7 linkset to_nyc
 profile timers
```

The following example shows how to define a profile named SAAL. The profile supports HSL, specifies the packet bundling interval and SSCF NNI timers, and applies to all the links in the linkset named to_nyc.

```
cs7 profile SAAL
 hsl
  bundling 10
  sscf-nni t1 10
  sscf-nni t2 150
  sscf-nni t3 100
.
.
cs7 linkset to_nyc
 profile SAAL
```

Related Commands

Command	Description
show cs7 mtp2	Displays ITP MTP2 status.
hsl	Configures CS7 link profile parameters for HSL.
m2pa	Configures CS7 link profile parameters for M2PA.
mtp2-timer	Configures CS7 link profile parameters for MTP2.
variant jt1	Specifies which of the SS7 variations the CS7 profile is running.

cs7 prompt enhanced

To configure the command line interface (CLI) prompt to display the current linkset (and, where applicable, the current link) when you are in linkset configuration mode, use the **cs7 prompt enhanced** command in global configuration mode. To return to the default prompt, use the **no** form of this command.

cs7 prompt enhanced

no cs7 prompt enhanced

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Command Modes	Global configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	The cs7 prompt enhanced command is an optional global configuration command that changes the prompt in linkset configuration mode to display the linkset (and, where applicable, the link) that is currently being configured. This command can help avoid the possibility of inadvertently shutting down the wrong linkset or link.

Examples	The following example shows how to configure the CLI prompt to display the current linkset: <pre>cs7 prompt enhanced</pre>

Related Commands	Command	Description
	show cs7 linkset	Displays ITP linkset information.
	shutdown (cs7 link)	Shuts down a link.
	shutdown (cs7 linkset)	Shuts down a linkset.

cs7 qos class

To configure a CS7 quality of service class, use the **cs7 qos class** command in global configuration mode. To remove the configuration, use the **no** form of this command.

cs7 [**instance** *instance-number*] **qos class** *class*

no **cs7** [**instance** *instance-number*] **qos class** *class*

Syntax Description

instance	(Optional) Specifies an instance.
<i>instance-number</i>	Instance number. An integer value in the range 0 to 7. The default instance is 0.
<i>class</i>	Quality of service class identification number. Valid numbers range from 0 to 7.

Defaults

The default instance is 0.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.

Usage Guidelines

A QoS class must be defined before being used by peer links and by the QoS packet classification methods input linkset, service indicator, and access list.

Examples

The following example shows how to configure QoS class 4:

```
cs7 qos class 4
```

The following example shows how to configure QoS class 4 to instance 2:

```
cs7 instance 2 qos class 4
```

Related Commands

Command	Description
cs7 mtp3 tuning rx-congestion-threshold	Enables multiple instances of a variant and network indicator combination.
gta qos-class	Sets the QoS class for the global title address.
map-version	Enables access list packet classification.

Command	Description
match any (cs7 linkset)	Enables input linkset packet classification.
match si (cs7 linkset)	Enables service indicator packet classification.

cs7 rate-limit

To specify the traffic rate limit to apply instance wide to all application groups that share a specific DPC or AS, use the **cs7 rate limit** command in privileged EXEC command.

```
cs7 [instance instance-number] rate-limit rate {pc pc | asname as-name} [type {sccp | mtp}]
```

```
no cs7 [instance instance id] rate-limit rate {pc pc | asname as-name}
```

Syntax Description	
instance	(Optional) Specifies the rate limit instance.
<i>instance-number</i>	The valid range is 0 to 7. The default instance is 0.
rate-limit	Specifies the traffic-rate limitation.
<i>rate</i>	An integrate value from 1 to 4294967296 MSU/sec.
pc	Indicates that the application groups are determined by a shared DPC.
asname	Indicates that the application groups are determined by a shared AS.
type	(Optional) This optional parameter indicates which type applies to the rate-limit. If type is not configured, then the type defaults to sccp.
sccp	Indicates that the rate limit is only applied to MAP entry instance-wide. This can limit a gtt application group.

Defaults The default type is SCCP.

Command Modes Global configuration

Command History	Release	Modification
	12.4(15)SW4	This command was introduced.
	12.2(33)IRD	

Usage Guidelines This command applies instance wide to all application groups that share a specific DPC or AS. These GTT application group will automatically have the configured rate limit applied.

Examples The following example applies rate limiting to all of the existing GTT application group that are contained in instance 7 and that include AS Alpha as part of the GTT application group. The rate limit is set at 1000 MSUs per second:

```
cs7 instance 7 rate-limit 1000 as Alpha type sccp
```

Related Commands

multiplicity	Specifies a method for selecting a destination in the application group.
cs7 gtt application-group	Specifies a GTT application group.
show cs7 gtt consistency	Displays GTT point codes that do not have routes provisioned for them.
cs7 rate-limit	Limits traffic rate to a specified DPC/AS in an MTP over-flow load-share that uses a GTT application group. Adds or changes a point code and optional subsystem number in the application group
pc (cs7 gtt application group)	Adds or changes a point code and optional subsystem number in the application group.
asname (cs7 gtt application group)	Assigns an M3UA or SUA AS directly to a global title.

cs7 remote-congestion-msgs

To allow remote congestion status console messages, use the **cs7 remote-congestion-msgs** command in global configuration mode. To suppress the messages, use the **no** form of this command.

cs7 [*instance instance-number*] **remote-congestion-msgs**

no cs7 [*instance instance-number*] **remote-congestion-msgs**

Syntax Description

instance	(Optional) Specifies a QoS class for an instance.
<i>instance-number</i>	Instance number. An integer value in the range 0 to 7.

Defaults

Remote congestion status messages are allowed.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Examples

The following example shows how to enable remote congestion status console messages:

```
cs7 remote-congestion-msgs
```

The following example shows how to enable remote congestion status console messages on instance 1:

```
cs7 instance 1 remote-congestion-msgs
```

Related Commands

Command	Description
cs7 mtp3 tuning rx-congestion-threshold	Enables multiple instances of a variant and network indicator combination.

cs7 route-mgmt-sls

To change the way route management signaling link selector (SLS) values are assigned on an instance, use the **cs7 route-mgmt-sls** command in global configuration mode. To return to the default selection method (round-robin), use the **no** form of this command.

cs7 [*instance instance-number*] **route-mgmt-sls** {**destination** | **round-robin** | **value** *number*}

no **cs7** [*instance instance-number*] **route-mgmt-sls**

Syntax Description

instance	(Optional) Changes the way route management signaling link selector (SLS) values are assigned on an instance
<i>instance-number</i>	Instance number. The valid range is 0 to 7. The default instance is 0.
destination	Assigns route management SLS values based on the concerned point code destination.
round-robin	Assigns route management SLS values using the round-robin method. Route management messages are distributed evenly over the available links in the linkset.
value	Assigns route management SLS values to a static value. Route management messages are distributed over the same link within a linkset.
<i>number</i>	Value in the range 0 to 255 (ANSI) or 1 to 15 (ITU).

Defaults

Route management SLS values are assigned using the round-robin method.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

When the ITP originates route management messages, it assigns an SLS value that is used by route management to distribute messages over multiple links in a linkset. When the SLS is assigned using the round-robin method, the route management messages are distributed over the available links in the linkset. This method results in the most efficient use of the available links.

Some SS7 nodes require all route management messages to have an SLS value of zero. If the ITP is connected to an adjacent node with this requirement, use the **cs7 instance route-mgmt-sls value** *number* command. Configuring this command to use a specific value causes route management messages to use the same link within a linkset. This method is not necessarily the most efficient use of the available links in a linkset, but it ensures that route management messages arrive at the adjacent node in the order they were sent.

Alternatively, the ITP has the ability to distribute route management message SLS values based on the concerned point code destination address in the route management message. This method allows the ITP to make more efficient use of the available links in the linkset, while preserving the order of route management messages to an adjacent node.

Examples

The following command shows how to specify an SLS value of zero for route management messages:

```
cs7 route-mgmt-sls value 0
```

The following command shows how to specify an SLS value of zero for route management messages that originate at instance 2:

```
cs7 instance 2 route-mgmt-sls value 0
```

Related Commands

Command	Description
cs7 multi-instance	Enables multiple instances of a variant and network indicator combination.

cs7 route-table

To specify the ITP route table, use the **cs7 route-table** command in global configuration mode. To remove the route table, use the **no** form of this command.

cs7 [*instance instance-number*] **route-table** *rt-name*

no cs7 [*instance instance-number*] **route-table** *rt-name*

Syntax Description

instance	(Optional) Specifies the ITP route table for an instance.
<i>instance-number</i>	Instance number. An integer value in the range 0 to 7.
<i>rt-name</i>	Route table name.

Defaults

A route table named **system** is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

A route table for an instance is identified by its route table name. The ITP configures a route table named **system** by default and uses the table to keep routes to all adjacent signaling points. Additional routes can be added to the route table.

Issuing the **cs7 route-table** command enables cs7 route table configuration mode. From this mode, you can update the route table.



Note

You must specify **system** as the route table name (*rt-name*).

Examples

The following example shows how to create a route table:

```
cs7 route-table system
```

The following example shows how to create a route table for instance 1:

```
cs7 instance 1 route-table system
```

Related Commands

Command	Description
cs7 mtp3 tuning rx-congestion-threshold	Enables multiple instances of a variant and network indicator combination.
update route (route-table)	Updates a route.

cs7 sami module

To enter the submode for the provisioning of ITP on the Cisco 7600 Supervisor Engine on the Cisco Service and Application Module for IP (SAMI), use the **cs7 sami module** command in global configuration mode.

cs7 sami module *slot*

Syntax Description	<i>slot</i>	Line card slot number.

Defaults	None.

Command Modes	Global configuration

Command History	Release	Modification
	12.2(25)IRA	This command was introduced.

Usage Guidelines	This command enters cs7 sami module configuration submode.
	This command is restricted to Cisco IOS Release 12.(25)IRA and later Cisco IOS Release 12.(25)IR releases.

Examples	The following example shows how to provision the SAMI module in slot 2 of the Cisco 7600 supervisor engine:
	<pre>cs7 sami module 2</pre>

Related Commands	Command	Description
	show cs7 sami ip	Verifies the ITP configuration.

cs7 save address-table

To save an address table to a specified location and file, use the **cs7 save address-table** privileged EXEC command. To remove the line from the configuration, use the **no** form of this command.

cs7 save address-table { **mlr** | **sms** } *table-name url*

no cs7 save address-table { **mlr** | **sms** } *table-name url*

Syntax Description	mlr	Specifies the type of table is mlr .
	sms	Specifies the type of table is sms .
	<i>table-name</i>	Identifies the existing address table that is to be replaced.
	<i>url</i>	The user-assigned local or remote location representing the filename and path from which the file will be replaced.

Defaults	None.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	SMS address tables can be stored in either NVRAM on the Cisco IOS platform or in a file that is typically stored in flash memory. NVRAM limitations on some platforms might restrict the number of address entries that can be stored there. In this case, the file storage option (<i>url</i>) is recommended.

Examples	The following command shows how to save an SMS address table named addrtbl1 to disk0:smsaddrtbl: <code>cs7 save address-table sms addrtbl1 disk0:smsaddrtbl</code>

Related Commands	Command	Description
	load (cs7 sms address-table)	Specifies the file to load on startup.

cs7 save billing-cfg

To save the current billing configuration to a specified *url*, use the **cs7 save billing-cfg** command in global configuration mode.

cs7 save billing-cfg *url*

Syntax Description	<i>url</i>	The location of the saved billing configuration file.

Defaults	none.

Command Modes	Global configuration

Command History	

Usage Guidelines	none

Examples	The following example saves a billing configuration file to the disc location <code>disk0:itp_billing.cfg</code>: <pre>cs7 save billing config disk0:itp-billing.cfg</pre>

Related Commands	Command	Description
	cs7 billing account	Configures a billing account.
	cs7 billing pc-table	Configures a pc-table for the billing account.
	cs7 billing options	Configures options for billing.
	cs7 billing load	Specifies the billing configuration file to load.

cs7 save gtt-table

To save the CS7 GTT table to a file, use the **cs7 save gtt-table** privileged EXEC command.

cs7 save gtt-table *url*

Syntax Description	<i>url</i> Location where the file is to be saved.	
Defaults	None.	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	
Usage Guidelines	GTT data is not saved with the write memory command. You must use the cs7 save gtt-table command.	
Examples	The following example shows how to save the GTT table to a file named gttdata.txt in flash memory: cs7 save gtt-table flash:gttdata.txt	
Related Commands	Command	Description
	cs7 gtt load	Specifies the location from which the GTT database is reloaded when the ITP router reboots.

cs7 save gws

To save the CS7 GWS configuration to a file, use the **cs7 save gws** privileged EXEC command.

cs7 [**instance** *instance-number*] **save gws** *url*

Syntax Description	instance	(Optional) Specifies the instance.
	<i>instance-number</i>	Instance number. Valid values range from 0 to 7.
	<i>url</i>	Location where the file is to be saved.

Defaults The default location of general GWS configuration files is cs7:gws-config.

Command Modes Privileged EXEC

Command History

Usage Guidelines GWS configuration information is not saved with the standard Cisco IOS CLI **copy running-config startup-config** or **write memory** command. You must use the **cs7 save gws** command.

After the GWS configuration is saved to the file, any existing GWS configuration statements in the running configuration file are saved to the specified file and removed from the running configuration. To save subsequent changes made to the GWS configuration with the Cisco IOS CLI, you must again use the **cs7 save gws** command.

Examples The following example shows how to save a GWS configuration to a file named gws-config:

```
cs7 save gws disk0:gws-config
```

Related Commands	Command	Description
	cs7 gws-table replace	Replaces a single GWS table with the table configuration file specified by the URL.
	cs7 gws replace	Replaces the running GWS configuration file or existing GWS tables with ones from a local or remote file.
	show cs7 gws config	Displays the whole configuration of GWS, including global action sets, linksets, global table entries, tables, and table entries.

cs7 save gws-table

To save the CS7 GWS table to a file, use the **cs7 save gws-table** privileged EXEC command.

cs7 [**instance** *instance-number*] **save gws-table** *table-name* *url*

Syntax Description	instance	(Optional) Specifies an instance.
	<i>instance-number</i>	Instance number. Valid values range from 0 to 7.
	<i>table-name</i>	Table name. Valid names may not exceed 12 alphanumeric characters.
	<i>url</i>	Location where the file is to be saved.

Defaults The default location of general GWS configuration files is cs7:gws-config. For GWS table files, it is cs7:gws-tables.

Command Modes Privileged EXEC

Command History

Usage Guidelines GWS table information is not saved with the standard Cisco IOS CLI **copy running-config startup-config** or **write memory** command. You must use the **cs7 save gws-table** command.

After the GWS table is saved to the file, any existing GWS configuration statements in the running configuration file are saved to the specified file and removed from the running configuration. To save subsequent changes made to the GWS configuration with the Cisco IOS CLI, you must again use the **cs7 save gws-table** command.

Examples The following example shows how to save the GWS table to a file named gws-dpc0:

```
cs7 save gws-table dpc0 disk0:gws-dpc0
```

Related Commands	Command	Description
	cs7 gws-table replace	Replaces a single GWS table with the table configuration file specified by the URL.
	cs7 gws replace	Replaces the running GWS configuration file or existing GWS tables with ones from a local or remote file.
	show cs7 gws config	Displays the whole configuration of GWS, including global action sets, linksets, global table entries, tables, and table entries.
	show cs7 gws table	Displays the GWS table configuration.

cs7 save log

To save a log to a file, use the **cs7 save log** privileged EXEC command.

cs7 save log *type destination*

Syntax Description

<i>type</i>	Specifies the type of log. Valid types are:
gtt	Errors related to global title translation
gws-nontest	Enhanced gateway screening logs in nontest mode
gws-test	Enhanced gateway screening logs in test mode
<i>destination</i>	Path and filename of the log archive destination. Valid destinations are:
cs7:	URL to saved table
flash:	URL to saved table
ftp:	URL to saved table
null:	URL to saved table
nvr:	URL to saved table
rcp:	URL to saved table
system:	URL to saved table
tftp:	URL to saved table

Defaults

None.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

Saved logs are written in readable text format.

New log entries that occur while the save is in progress are written to a new log file and are not lost.

Examples

The following example shows how to detach the current log from the active log process and save it to tftp://10.1.1.3/logs/gttlog1.txt:

```
cs7 save log gtt tftp://10.1.1.3/logs/gttlog1.txt
```

The following example shows how to detach the current log from the active log process and save it to tftp://10.1.1.3/logs/gws-test-log.txt:

```
cs7 save log gws-test tftp://10.1.1.3/logs/gws-test-log1.txt
```

Related Commands

Command	Description
cs7 log	Enables the ITP to log events, errors, and traces.
show cs7 log	Displays the current log.

cs7 save mlr

To save the CS7 MLR configuration to a file, use the **cs7 save mlr** privileged EXEC command.

cs7 [**instance** *instance-number*] **save mlr** [**all**] *url*

Syntax Description

instance	(Optional) Specifies an instance.
<i>instance-number</i>	Instance number. Valid values range from 0 to 7.
<i>url</i>	Location where the file is to be saved.

Defaults

The default location of general MLR configuration files is cs7:mlr.

Command Modes

Privileged EXEC

Command History

Usage Guidelines

MLR configuration information is not saved with the standard Cisco IOS CLI **copy running-config startup-config** or **write memory** command. You must use the **cs7 save mlr** command.

After the MLR configuration is saved to the file, any existing MLR configuration statements in the running configuration file are saved to the specified file and removed from the running configuration. To save subsequent changes made to the MLR configuration with the Cisco IOS CLI, you must again use the **cs7 save mlr** command.

Examples

The following example shows how to save an MLR configuration to a file named mlr-config:

```
cs7 save mlr all disk0:mlr-config
```

Related Commands

Command	Description
cs7 mlr load	Loads an MLR file.
cs7 mlr replace	Replaces the running configuration file with a file specified by the URL.

cs7 save route-table

To save the CS7 route table to a file, use the **cs7 save route-table** privileged EXEC command.

cs7 save route-table *rt-name url*

Syntax Description	<i>rt-name</i>	Route table name.
	<i>url</i>	Location where the file is to be saved.

Defaults	None.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	Use this command to save an active route table into a file. The newly created file can be used with the load route-table subcommand to populate the route table on ITP startup.

**Note**

All **update route** or **remove route** route-table commands are removed from the system configuration after the save is completed. The commands are removed because they have been applied to the actual route table *before* the save and therefore are included in the saved file.

We recommend that you save the router configuration to nonvolatile memory (NVRAM) after generating a new route-table file because the configuration has changed (update/remove route commands may have been removed from the configuration).

Examples	The following example shows how to save a route table named testtable to flash memory:

```
cs7 save route-table testtable flash:testtable
```

Related Commands	Command	Description
	load (cs7 route table)	Loads route table contents from a URL.
	remove route (route table)	Removes the active MTP3 route table.
	update route (route-table)	Updates a route.

cs7 sccp-allow-pak-conv

To configure the conversion option at instance level between XUDT/XUDTS and UDT/UDTS, use the **cs7 sccp-allow-pak-conv** command in global configuration mode. To remove the configuration, use the no form of this command.

cs7 [**instance** *instance-number*] **sccp-allow-pak-conv** *number*

no cs7 [**instance** *instance-number*] **sccp-allow-pak-conv** *number*

Syntax Description	<i>instance-number</i>	Defines the specific instance. Valid values range from 0 to 7.
	<i>number</i>	1 specifies XUDT/XUDTS to UDT/UDTS conversion while 2 specifies UDT/UDTS to XUDT/XUDTS conversion.
Defaults	None.	
Command Modes	Global configuration	
Command History	Release	Modification
	12.4(15)SW9 12.2(33)IRI	This command was introduced.
Usage Guidelines	To be determined.	
Examples	DE: Please provide an example.	
	cs7 instance 0 sccp-allow-pak-conv 1	
Related Commands	Command	Description

cs7 sccp-class1-loadshare

To configure the loadsharing option for GTT application groups in loadshare/cost mode, use the **cs7 sccp-class1-loadshare** command in global configuration mode. To remove the configuration, use the no form of this command.

```
cs7 [instance instance-number] sccp-class1-loadshare {opc-sls [opc-shift [opc-shift-number] |  
cgpa | sls}
```

```
no cs7 [instance instance-number] sccp-class1-loadshare {opc-sls [opc-shift [opc-shift-number] |  
cgpa | sls}
```

Syntax Description	
instance	(Optional) Configures the secondary point code on an instance.
<i>instance-number</i>	(Optional) Defines the specific instance. Valid values range from 0 to 7.
opc-sls	Extends SLS based ASP binding to OPC-SLS combination based binding. This command applies only to the ITU standard not the ANSI standard.
cgpa	Specifies the SCCP calling party address option.
sls	Specifies the SLS based load sharing option.
opc-shift	(Optional) Shifts the OPC bits that are used.
<i>opc-shift-number</i>	Number of OPC bits that are shifted.

Defaults	SLS based loadsharing applies. The default is 0 for the <i>opc-shift-number</i> argument.

Command Modes	Global configuration

Command History	Release	Modification
	12.2(18)IXH	This command was introduced.
	12.4(15)SW3	
	12.2(33)IRC	

Usage Guidelines	The command applies to Class 1 traffic for all GTT application groups instances configured with loadsharing.

Examples	The following command configure the loadsharing option for GTT application groups in loadshare/cost mode with the SCCP calling party address option: <pre>cs7 instance 1 sccp-class1-loadshare cgpa</pre>

Related Commands	Command	Description
	multiplicity	Specifies a method for selecting a destination in the application group.
	asname (cs7 gtt application group)	Assigns an M3UA or SUA AS directly to a global title.
	pc (cs7 gtt application group)	Adds or changes a point code and optional subsystem number in the application group.

cs7 sccp-class1-wrr

To configure the WRR option for GTT application groups, use the **cs7 sccp-class1-wrr** command in global configuration mode. To remove the configuration, use the no form of this command.

```
cs7 [instance instance-number] sccp-class1-wrr {opc-sls [opc-shift [opc-shift-number] | cgpa-sls | sls]}
```

```
no cs7 [instance instance-number] sccp-class1-wrr {opc-sls [opc-shift [opc-shift-number] | cgpa-sls | sls]}
```

Syntax Description	
instance	(Optional) Configures the secondary point code on an instance.
<i>instance-number</i>	(Optional) Defines the specific instance. Valid values range from 0 to 7.
opc-sls	Applies the command to the ITU standard, but not to the ANSI standard.
opc-shift	(Optional) Shifts the OPC bits that are used.
<i>opc-shift-number</i>	Number of OPC bits that are shifted.
cgpa-sls	Specifies loadsharing based on a combination of CGPA and SLS.
sls	Specifies the SLS based load sharing option.

Defaults SLS based loadsharing applies. The default is 0 for the *opc-shift-number* argument.

Command Modes Global configuration mode

Command History	Release	Modification
	12.4(15)SW4	This command was introduced.
	12.2(33)IRD	

Usage Guidelines The command applies to class 1 traffic for all GTT application groups with WRR in that instance.

Examples The following command configure the loadsharing option for GTT application groups in WRR mode with the SCCP calling party address option:

```
cs7 instance 1 sccp-class1-wrr cgpa-sls
```

Related Commands	Command	Description
	multiplicity	Specifies a method for selecting a destination in the application group.
	asname (cs7 gtt application group)	Assigns an M3UA or SUA AS directly to a global title.
	pc (cs7 gtt application group)	Adds or changes a point code and optional subsystem number in the application group.

cs7 sccp gti-conversion

To configure an SCCP GTI conversion table, use the **cs7 sccp gti-conversion** command in global configuration mode. To remove the definition, use the **no** form of this command.

cs7 sccp gti-conversion *table-name*

no cs7 sccp gti-conversion *table-name*

Syntax Description	<i>table-name</i>	SCCP GTI conversion table name. The table name may be 1 to 12 characters long.

Defaults	None.

Command Modes	Global configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	This command names the GTI conversion table and enables cs7 sccp gti conversion mode.

Examples	The following command shows how to specify an SCCP GTI conversion table named gti-conv1: <code>cs7 sccp gti-conversion conv1</code>

Related Commands	Command	Description
	show cs7 sccp gti-conversion	Displays CS7 GTI conversion tables.
	update (cs7 sccp gti conversion)	Creates or updates an SCCP GTI conversion table entry.

cs7 sccp instance-conversion

To configure or update an SCCP instance conversion entry, use the **cs7 sccp instance-conversion** command in global configuration mode. To remove the definition, use the **no** form of this command.

cs7 sccp instance-conversion in-instance *instance* **out-instance** *instance*

no cs7 sccp instance-conversion in-instance *instance* **out-instance** *instance*

Syntax Description

in-instance	Specifies an input instance for conversion.
<i>instance</i>	Input instance number.
out-instance	Specifies an output instance for conversion.
<i>instance</i>	Output instance number.

Defaults

If no conversion methods are assigned, the GTTs in the MSUs do not change.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

When you configure an SCCP instance conversion entry, you can assign GTI conversion, subsystem mapping, and address conversion tables from one instance to another. You can use one, two, or all three conversion methods. If no conversion methods are assigned, the GTTs in the MSUs do not change.

You can also set message-handling options and specify a national indicator.

Examples

The following example shows how to configure an SCCP instance conversion entry. The entry sets gti-conversion, subsystem mapping, and address conversion tables from instance 0 to instance 1.

```
cs7 sccp instance-conversion in-instance 0 out-instance 1
  set gti-conversion gtitable
  set ssn-conversion ssntable
  set address-conversion gtaddresstable
```

Related Commands

Command	Description
set address-conversion	Specifies the GTT address conversion table to be assigned from one instance to another.
set gti-conversion	Specifies the GTI conversion table to be assigned from one instance to another.
set ssn-conversion	Specifies the SSN conversion table to be assigned from one instance to another.
show cs7 sccp gti-conversion	Displays the SCCP GTI conversion table.
show cs7 sccp instance-conversion	Displays the SCCP instance conversion table.
show cs7 sccp ssn-conversion	Displays the SCCP SSN conversion table.

cs7 sccp ssn-conversion

To create a subsystem mapping table, use the **cs7 sccp ssn-conversion** command in global configuration mode. To delete the table, use the **no** form of this command.

cs7 sccp ssn-conversion *table-name* **in-ssn** *in-ssn* **out-ssn** *out-ssn*

no cs7 sccp ssn-conversion *table-name* **in-ssn** *in-ssn* **out-ssn** *out-ssn*

Syntax Description	<i>table-name</i>	Subsystem table name. The table name may be 1 to 12 characters long.
	in-ssn	Input SSN.
	<i>in-ssn</i>	Valid range 0 to 255.
	out-ssn	Output SSN.
	<i>out-ssn</i>	Valid range 0 to 255.

Defaults None.

Command Modes Global configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines This command creates a subsystem mapping table that specifies input and output SSN values. If the ITP does not find a match in the SSN conversion table, the SSN in the MSU does not change.

If both GTI conversion and subsystem mapping are used, and a GTI conversion specifies a new subsystem for the MSU, the ITP uses the subsystem specified by the GTI conversion, not the subsystem from the SSN conversion table.

Examples The following example shows how to create a subsystem mapping table named ss-conv0:

```
cs7 sccp ssn-conversion ss-conv0 in-ssn 11 out-ssn 13
cs7 sccp ssn-conversion ss-conv0 in-ssn 200 out-ssn 6
```

Related Commands	Command	Description
	set address-conversion	Specifies the address conversion table to be assigned from one instance to another.
	set gti-conversion	Specifies the GTI conversion table to be assigned from one instance to another.

Command	Description
set ssn-conversion	Specifies the subsystem conversion table to be assigned from one instance to another.
show cs7 sccp ssn-conversion	Displays the SSN conversion table.

cs7 sctp crc-type

To create a subsystem mapping table, use the **cs7 sccp ssn-conversion** command in global configuration mode. To delete the table, use the **no** form of this command.

cs7 sccp ssn-conversion *table-name* **in-ssn** *in-ssn* **out-ssn** *out-ssn*

no cs7 sccp ssn-conversion *table-name* **in-ssn** *in-ssn* **out-ssn** *out-ssn*

Syntax Description		
	<i>table-name</i>	Subsystem table name. The table name may be 1 to 12 characters long.
	in-ssn	Input SSN.
	<i>in-ssn</i>	Valid range 0 to 255.
	out-ssn	Output SSN.
	<i>out-ssn</i>	Valid range 0 to 255.

Defaults None.

Command Modes Global configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines This command creates a subsystem mapping table that specifies input and output SSN values. If the ITP does not find a match in the SSN conversion table, the SSN in the MSU does not change.

If both GTI conversion and subsystem mapping are used, and a GTI conversion specifies a new subsystem for the MSU, the ITP uses the subsystem specified by the GTI conversion, not the subsystem from the SSN conversion table.

Examples The following example shows how to create a subsystem mapping table named ss-conv0:

```
cs7 sccp ssn-conversion ss-conv0 in-ssn 11 out-ssn 13
cs7 sccp ssn-conversion ss-conv0 in-ssn 200 out-ssn 6
```

Related Commands	Command	Description
	set address-conversion	Specifies the address conversion table to be assigned from one instance to another.
	set gti-conversion	Specifies the GTI conversion table to be assigned from one instance to another.

cs7 secondary-pc

To configure secondary point codes, use the **cs7 secondary-pc** command in global configuration mode. To remove the configuration, use the **no** form of this command.

cs7 [**instance** *instance-number*] **secondary-pc** *zone.region.sp*

no [**instance** *instance-number*] **secondary-pc** *zone.region.sp*

Syntax Description

instance	(Optional) Configures the secondary point code (PC) on an instance.
<i>instance-number</i>	Instance number. An integer value in the range 0 to 7.
<i>zone.region.sp</i>	Secondary PC identifier.

Defaults

None.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.
12.4(15)SW4 12.2(33)IRD	The ability to configure 40 secondary PCs per chassis was added.

Usage Guidelines

This command is used to configure multiple linksets between the ITP and an adjacent node. To the adjacent node, the ITP appears to be two different nodes: one with the PC configured using the **cs7 point-code** command and one with the PC configured using the **cs7 secondary-pc** command. You may configure a maximum of 40 secondary PCs per chassis.

Examples

The following example shows how to configure a primary, secondary, and capability point code:

```
cs7 point-code 1.1.1
cs7 secondary-pc 1.1.2
cs7 capability-pc 1.1.3
```

Related Commands

Command	Description
cs7 mtp3 tuning rx-congestion-threshold	Enables multiple instances of a variant and network indicator combination.
cs7 linkset	Specifies a linkset.

Command	Description
cs7 point-code	Assigns a local pc.
cs7 capability-pc	Assigns a capability pc.

cs7 sg-event-history

To set the maximum number of events to save in history, use the **cs7 sg-event-history** command in global configuration mode. To [stop saving events?], use the **no** form of this command.

cs7 sg-event-history *number*

no sg-event-history *number*

Syntax Description	<i>number</i>	Maximum number of events to save in AS, ASP, and point code history. The valid range is 1 to 256 events. The default is 16 events.

Defaults	16 events

Command Modes	Global configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples	The following example shows how to save 64 events in history: <code>cs7 sg-event-history 64</code>

cs7 sgmp

To specify the local port number for SGMP and enter cs7 sgmp submode, use the **cs7 sgmp** command in global configuration mode. To delete the SGMP configuration, if no mated SG is configured, use the **no** form of this command.

```
cs7 sgmp local_port [offload] [slot] [bay]
```

```
no cs7 sgmp local_port [offload] [slot] [bay]
```

Syntax Description

<i>local_port</i>	The local port number is a number in the range 1024 to 65535. Only one SGMP local port may be specified. The local port number may not be the same as the configured local port numbers for M2PA, M3UA, or SUA.
offloading	Enables SGMP offload.
<i>slot</i>	Linecard slot number.
<i>bay</i>	Linecard bay number containing the processor.

Defaults

None.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.
12.2(33)IRD	The offload keyword was introduced.

Usage Guidelines

Two SGs can function as a mated pair and exchange necessary state information using the Signaling Gateway Mate Protocol (SGMP). SGMP is used to establish an association to the mated-signaling gateway (with equivalent SG configuration).

The mated-pair SGs are used to loadshare and/or back up each other. The mated SG can be used as a backup point code if an association between this SG and the ASP has failed.

Mated-pair SGs must have equivalent SG configuration, including the same AS and AS route routing-key definitions. However, the local point code of each SG must be unique and must not match the local point code, the capability point code, the secondary point code, any AS point code (DPC), or any AS route point code configured on its mate.

When the SG mate association is active, the SG is informed of AS state changes on the mate in real time. When an AS becomes inactive, subsequent messages are rerouted to the mate if the corresponding AS on the mate is active.

When the AS on the original SG returns to active state, new messages are temporarily queued to allow in-transit messages from the mated SG to arrive at the ASP. Queued messages are released to the ASP when an AS recovery timer expires.

This command is not instance related and cannot be specified with the **instance** keyword.

You cannot configure SGMP offload when non-offloaded SGMP is configured. If non-offload SGMP is configured, you must delete it before configuring the SGMP offload.

Examples

The following example shows how to specify the local port number 5000 for SGMP:

```
cs7 sgmp 5000
```

The following example shows how to specify the local port number 999, SGMP offload, line card slot number 2, and line card bay number 1 :

```
cs7 sgmp 9999 offload 2 1
```

Related Commands

Command	Description
cs7 mated-sg	Specifies the mated SG.
local-ip (cs7)	Configures up to four local IP addresses that will receive SGMP packets.
show cs7 sgmp	Displays SGMP information.

cs7 sls-shift

When the variant is ITU, to shift which signaling link selection (SLS) bits are used for link and linkset selection, use the **cs7 sls-shift** command in global configuration mode. To disable the specification, use the **no** form of this command.

cs7 [*instance instance-number*] **sls-shift** {**0-3**}

no cs7 [*instance instance-number*] **sls-shift**

Syntax Description

instance	Shifts SLS bits on an instance.
<i>instance-number</i>	Instance number. An integer value in the range 0 to 7.
0-3	Indicates a range, from least significant bit (0) to most significant bit (3) of the SLS, to be used for linkset selection within a combined linkset.

Defaults

The default bit is 0 (the equivalent of the **no sls-shift** command).

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

This command is for MTP3 users (SUA/M3UA) who do not have an inbound linkset. The command works the same way as the linkset-specific **sls-shift** command.

This command is valid only when the variant is ITU. It affects MSUs received on the linkset, and changes which bit in the SLS is used for linkset selection. ITU, unlike ANSI, does not perform SLS rotation. If all nodes in the network use the same bit for linkset selection, traffic does not balance evenly.

Examples

The following example shows how to use the most significant bit (3) for linkset selection:

```
cs7 sls-shift 3
```

Related Commands

Command	Description
cs7 linkset	Specifies a linkset.
cs7 mtp3 tuning rx-congestion-threshold	Enables multiple instances of a variant and network indicator combination.
cs7 route-mgmt-sls	Changes the way route management SLS values are assigned.

cs7 sms ansi41

To enable the configuration of ANSI-41 transport-specific parameters, use the **cs7 sms ansi41 EXEC** command. To remove the configuration, use the **no** form of this command.

cs7 sms ansi41 ssn *ssn*

no cs7 sms ansi41 ssn *ssn*

Syntax Description

ssn	Specifies the subsystem number.
<i>ssn</i>	Subsystem number. Valid numbers range from 2 to 255.

Defaults

None.

Command Modes

EXEC

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The **cs7 sms ansi41** command allows ANSI-41 transport-specific parameters to be modified independent of the received inbound message.

Only one SMS transport (that is, GSM MAP or ANSI-41 MAP) may be defined. The definition of the ANSI-41 transport *must* precede the definition for handling inbound ANSI-41 messages configured with the **cs7 sms route-table** command. Conversely, the ANSI-41 transport may not be removed until the handling of all ANSI-41 operations is removed from the CS7 SMS route table.

The **cs7 sms ansi41** command enables cs7 sms ansi41 configuration mode.

Examples

The following example shows how to specify the address for all sourced ANSI-41 dialogs:

```
cs7 sms ansi41 ssn 11
map-source-addr digits 9191111111
```

Related Commands

Command	Description
invoke-timer (cs7 sms ansi41)	Specifies a timer to supervise initiated dialogs that are specific to the ANSI-41 transport.

Command	Description
map-source-addr (cs7 sms ansi41)	Specifies the address for all sourced ANSI-41 dialogs.
show cs7 sms dest-sme-binding	Displays SMS ANSI41 MAP information for a specific subsystem.

cs7 sms gsm-map

To enable the configuration of GSM transport-specific parameters, use the **cs7 sms gsm-map** command in global configuration mode. To remove the configuration, use the **no** form of this command.

cs7 sms gsm-map *ssn* *ssn*

no cs7 sms gsm-map *ssn* *ssn*

Syntax Description

ssn	Specifies the subsystem number.
<i>ssn</i>	Subsystem number. Valid numbers range from 2 to 255.

Defaults

None.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The optional **cs7 sms gsm-map** command allows for the configuration of parameters that are specific to the GSM transport being used by the SMS subsystem.

Only one SMS transport (that is, GSM MAP or ANSI41 MAP) may be defined. The definition of the GSM transport *must* precede the definition for handling inbound GSM messages configured with the **cs7 sms route-table** command. Conversely, the GSM transport may not be removed until the handling of all GSM operations is removed from the CS7 SMS route table.

The **cs7 sms gsm-map** command enables cs7 sms gsm configuration mode.

Examples

The following example shows how to specify GSM transport for ssn 8:

```
cs7 sms gsm-map ssn 8
  invoke-times 30
  map-source-address digits 9991117771
  gprs-delivery prefer-Saxon
```

Related Commands

Command	Description
invoke-timer (cs7 sms gsm map transport)	Specifies a timer to supervise initiated dialogs.
map-source-addr (cs7 sms gsm map transport)	Specifies the local source address of the SMS application.

Command	Description
mnp (cs7 sms gsm map transport)	Allows the configuration of DSMR options specific to mobile number portability.
show cs7 sms gsm-map	Displays SMS GSM MAP transport information.
sm-sc-map-version (cs7 sms gsm map transport)	Specifies a locally supported MAP version.

Both Flexwan and SAMI processors distribute messages to a set of configured processors by WRR. of one for the offload CPU of two for the offload CPU, of one for the offload CPU,

cs7 sms ruleset

To configure an SMS ruleset, use the **cs7 sms ruleset** command in global configuration mode. To disable the ruleset, use the **no** form of this command.

cs7 sms ruleset *name* [**protocol** {**gsm-map** | **ansi41**}] [**event-trace**]

no cs7 sms ruleset *name*

Syntax Description

<i>name</i>	SMS ruleset name.
protocol	(Optional) Specifies an application layer protocol filter for this ruleset. The default behavior is that all operations may be specified within the ruleset.
gsm-map	(Optional) Uses GSM-MAP as the application layer protocol filter within this ruleset. Only gsm-map operations may be specified within the ruleset.
ansi41	(Optional) Uses ANSI-41 as the application layer protocol filter within this ruleset. Only ansi41 operations may be specified within the ruleset.
event-trace	Indicates that this ruleset is used for call tracing.

Defaults

For the **protocol** keyword, all operations may be specified within the ruleset.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The **cs7 sms ruleset** command enables cs7 sms set rule configuration mode, in which you can configure rules that customize the routing of SMS messages.

Examples

The following example shows how to specify a ruleset named SMS-RULES:

```
cs7 sms ruleset SMS-RULES
```

Related Commands

Command	Description
rule (cs7 sms set)	Specifies a rule for this ruleset.

cs7 snmp dest-max-r1-window

To specify the maximum number of rev1 destination state changes allowed per window, use the **cs7 snmp dest-max-r1-window** command in global configuration mode. To return to the default value, use the **no** form of this command.

cs7 snmp dest-max-r1-window *changes*

cs7 snmp dest-max-r1-window *changes*

Syntax Description	<i>changes</i>	Maximum number of destination state changes allowed per window. Valid range is 10 to 9000. The default is 60.

Defaults	60

Command Modes	Global configuration

Command History	Release	Modification
	12.4(15)SW7	This command was introduced.
	12.2(33)IRG	

Examples	The following example shows how to set the maximum number of rev1 destination state changes allowed per window to 500: cs7 snmp dest-max-r1-window 500

cs7 snmp dest-max-window

To specify the maximum number of destination state changes allowed per window, use the **cs7 snmp dest-max-window** command in global configuration mode. To return to the default value, use the **no** form of this command.

cs7 snmp dest-max-window *changes*

cs7 snmp dest-max-window *changes*

Syntax Description	changes	Maximum number of destination state changes allowed per window. Valid range is 10 to 9000. The default is 60.
Defaults	60	
Command Modes	Global configuration	
Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	
Examples	The following example shows how to set the maximum number of destination state changes allowed per window to 500:	
	cs7 snmp dest-max-window 500	

cs7 snmp mgmt-max-r1-window

To specify the maximum number of rev1 route management state changes allowed per window, use the **cs7 snmp mgmt-max-r1-window** command in global configuration mode. To return to the default value, use the **no** form of this command.

cs7 snmp mgmt-max-r1-window *changes*

no cs7 snmp mgmt-max-r1-window *changes*

Syntax Description	<i>changes</i>	Maximum number of route management state changes allowed per window. Valid range is 10 to 9000. The default is 60.

Defaults	60

Command Modes	Global configuration

Command History	Release	Modification
	12.4(15)SW7	This command was introduced.
	12.2(33)IRG	

Examples	The following example shows how to set the maximum number of rev1 route management state changes allowed per window to 500:

```
cs7 snmp mgmt-max-r1-window 500
```

cs7 snmp mgmt-max-window

To specify the maximum number of route management state changes allowed per window, use the **cs7 snmp mgmt-max-window** command in global configuration mode. To return to the default value, use the **no** form of this command.

cs7 snmp mgmt-max-window *changes*

no cs7 snmp mgmt-max-window *changes*

Syntax Description	<i>changes</i>	Maximum number of route management state changes allowed per window. Valid range is 10 to 9000. The default is 60.

Defaults	60

Command Modes	Global configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples	The following example shows how to set the maximum number of route management state changes allowed per window to 500:

```
cs7 snmp mgmt-max-window 500
```


cs7 sua

To specify the local port number for SUA and enter cs7 sua submode, use the **cs7 sua** command in global configuration mode. To delete the SUA configuration (if there are no SUA ASs or ASPs), use the **no** form of this command.

cs7 sua *port-number* [**offload**] [*line-card-slot-number*] [*bay-number*]

no cs7 sua *port-number* [**offload**] [*line-card-slot-number*] [*bay-number*]

Syntax Description

<i>port-number</i>	Indicates the local port number in the range 1024 to 65535. This port number may not be the same as the configured local port numbers for M2PA, M3UA, or SGMP. The SUA well-known port number is 14001.
offload	(Optional) Enables the ITP to perform SUA SCTP message processing on the line card. Offloading is restricted to the 7600 platform.
<i>line-card-slot-number</i>	(Optional) Line card slot number. Valid range is 0 to 16.

Defaults

None.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.
12.2(18)IXA 12.2(33)IRA	The offload keyword was added, enabling the xUA SCTP Offload feature.
12.2(33)IRA	Extended the range of the <i>bay-number</i> argument for use with SAMI processors.

Usage Guidelines

The range for *bay-number* (3 to 8) reflects the labeling of the SAMI card processors. It is consistent with other SAMI applications, as well as the faceplate numbering for the console connections.

SUA uses SCTP to communicate with application server processes (ASPs). The **offload** keyword enables the ITP to offload SUA SCTP message processing to the line card. If you are configuring SUA SCTP offload, the **local-ip** *ip-address* must be an IP address that was already configured on the line card to which you are offloading this SUA instance. When offload is enabled, only a single IP route is allowed for each destination.

If offloaded, a specific SUA instance can run on only one line card, but different offloaded SUA instances can run on the same line card or on different line cards. If you offload M3UA or SUA to a line card, that line card cannot also be used for M2PA offload.

Issuing the **cs7 sua** command enables cs7 sua submode.

The **cs7 sua** command cannot be specified with the **instance** keyword.

The SUA configuration must be removed before the variant or local point code can be removed.

Examples

The following example shows how to specify a local port number of 5000 for SUA:

```
cs7 sua 5000 offload 5 0
local-ip 10.10.10.4
```

The following example shows how to offload two different instances of SUA SCTP message processing to the line card in slot 5, bay 0 and another instance to the line card in slot 6, bay 0:

```
cs7 sua 6000 offload 5 0
local-ip 10.10.10.5
!
cs7 sua 6500 offload 5 0
local-ip 10.10.10.5
!
cs7 sua 7000 offload 6 0
local-ip 10.10.10.6
```

Related Commands

Command	Description
local-ip (CS7 SUA)	Configures up to four local IP addresses that will receive SUA packets.
show cs7 asp	Displays ASP information.
show cs7 sua	Displays SUA node information.

cs7 sua-allow-xudt-request

To allow the SUA ASP additional control in determining whether an SCCP UDT or XUDT message will be generated, use the **cs7 sua-allow-xudt-request** command in global configuration mode. To remove the configuration, use the **no** form of this command.

cs7 [*instance instance-number*] **sua-allow-xudt-request**

no cs7 [*instance instance-number*] **sua-allow-xudt-request**

Syntax Description

instance	(Optional) Specifies an instance.
<i>instance-number</i>	Instance number. An integer value in the range 0 to 7.

Defaults

If this command is *not* used, XUDT SCCP messages are generated only when segmentation of an SCCP message is performed by the ASP.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The **cs7 sua-allow-xudt-request** command allows the SUA ASP additional control in determining whether an SCCP UDT or XUDT message will be generated after receiving a CLDT message. When the command is specified, SUA requests the SCCP layer to generate an XUDT message if the ASP has provided either the IMPORTANCE or HOP_COUNTER parameter within the CLDT message.

Examples

The following example shows how to enable the SUA to request the SCCP layer to generate an XUDT message if the ASP has provided either the IMPORTANCE or HOP_COUNTER parameter within the CLDT message:

```
cs7 instance 2 sua-allow-xudt-request
```

cs7 summary-routing-exception

To turn off the use of summary/cluster routes (for the purpose of routing MSUs) for a configured full point code member, use the **cs7 summary-routing-exception** command in global configuration mode. To restore the default (allow the use of summary routes), use the **no** form of this command.

cs7 [*instance instance-number*] **summary-routing-exception**

no cs7 [*instance instance-number*] **summary-routing-exception**

Syntax Description

instance	(Optional) Turns off the use of summary/cluster routes on an instance.
<i>instance-number</i>	Instance number. An integer value in the range 0 to 7.

Defaults

The summary routing exception feature is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The **cs7 summary-routing-exception** command controls whether the summary route or the ANSI cluster route is used when the full point code route is not available. If the command is enabled, the summary route is *not* used. The ITP drops the MSU and sends a TFP.

This feature is useful for customers who want to split destinations between routes. For example, most destinations that are covered by a summary route will route on a certain group of linksets, but one or more of the destinations within that summary route will route on different linksets.

The feature only affects MSUs that are routed for a destination for which a set of full point code routes is configured.

Examples

The following example shows how to turn off the use of summary routes:

```
cs7 summary-routing-exception
```

Related Commands

Command	Description
cs7 mtp3 tuning rx-congestion-threshold	Enables multiple instances of a variant and network indicator combination.
update route (route-table)	Adds a summary route and updates the routing table.

cs7 tcap tid-timer

To set the minimum expiration time for TCAP transactions, use the **cs7 tcap tid-timer** command in global configuration mode. To reestablish the default timer value of 60 minutes, use the **no** form of this command.

cs7 tcap tid-timer *minutes*

no cs7 tcap tid-timer

Syntax Description	<i>minutes</i>	Time before TCAP may cancel a transaction. Valid range is 0 to 1440 minutes. The default is 60 minutes.

Defaults	60 minutes

Command Modes	Global configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples	The following example shows how to set the minimum expiration time for TCAP transactions to 120 minutes:

```
cs7 tcap tid-timer 120
```

Related Commands	Command	Description
	show cs7 tcap	Displays CS7 TCAP information.

cs7 tcap variant

To specify the variant for the TCAP layer, use the **cs7 tcap variant** command in global configuration mode. To remove the specification from the configuration, use the **no** form of this command.

cs7 tcap variant {ansi | itu}

no cs7 tcap variant {ansi | itu}

Syntax Description

ansi	TCAP layer uses the ANSI T1.114 variant. The ANSI T1.114 variant is required for proper ITP support of the ANSI-41 SMS Notification Proxy feature.
itu	TCAP layer uses the ITU/ETSI Q.77x variant. The ITU/ETSI Q.77x variant is required for proper ITP support of GSM MAP-based application features such as SIM Authentication, MMSC Gateway, GSM SMS MO Proxy, and DSMR.

Defaults

If the **cs7 tcap variant** command is not configured, ITU/ETSI is the default variant.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

Configuration changes made to the TCAP variant on a running system do not take effect until the ITP is reloaded with the saved configuration.

Examples

The following example shows how to enable the ANSI T1.114 variant:

```
cs7 tcap variant ansi
```

Related Commands

Command	Description
cs7 tcap tid-timer	Specifies the minimum expiration time for TCAP transactions.

cs7 tfc-pacing-ratio

To adjust the transfer control (TFC) pacing ratio to comply with the ANSI specification of one TFC for every dropped message signal unit (MSU), use the **cs7 tfc-pacing-ratio** command in global configuration mode. To reestablish the ITP default TFC pacing ratio (eight MSUs dropped for outbound link congestion for each TFC generated), use the **no** form of this command.

cs7 [*instance instance-number*] **tfc-pacing-ratio** *count*

no cs7 [*instance instance-number*] **tfc-pacing-ratio**

Syntax Description	instance	(Optional) Adjusts the transfer control (TFC) pacing ratio on an instance.
	<i>instance-number</i>	Instance number. An integer value in the range 0 to 7.
	<i>count</i>	Valid range is 1 to 16. The default is 8.

Defaults 8 MSUs

Command Modes Global configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines The **cs7 tfc-pacing-ratio** command controls the ratio of TFC MSUs sent in response to received MSUs being dropped due to outbound link congestion. The ANSI standard is a 1-to-1 ratio. To prevent congestion in the reverse direction, the ITP default configuration sets a ratio of 1 TFC for each 8 dropped MSUs.

Examples The following example shows how to send TFCs in a 1-to-1 ratio (TFC MSUs sent in response to MSUs dropped due to outbound congestion):

```
cs7 tfc-pacing-ratio 1
```

Related Commands	Command	Description
	cs7 mtp3 tuning rx-congestion-threshold	Enables multiple instances of a variant and network indicator combination.

cs7 uninhibit

To prevent the risk of losing connectivity by shutting down the last link in a linkset, use the **cs7 inhibit** user EXEC command with the linkset name and the link number. To reverse the inhibit, use the **cs7 uninhibit** command.

cs7 uninhibit *linkset link*

Syntax Description

<i>linkset</i>	Linkset name.
<i>link</i>	Link.

Defaults

None.

Command Modes

User EXEC

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The **cs7 inhibit** command prevents you from taking the last link in a linkset out of service. If you use the **shutdown** command to shut down the last link in a linkset, you could lose connectivity. The **cs7 inhibit** command first verifies whether a link is the last link in the linkset. The command allows you to either add linksets or reduce your bandwidth in the linksets by taking links out of service.

Examples

The following command shows how to uninhibit link 0 on the linkset named tony:

```
cs7 uninhibit tony 0
```

Related Commands

Command	Description
shutdown (cs7 link)	Disables a link or linkset.
cs7 ignore-sccp-pcconv	Inhibits a link.

cs7 upgrade analysis

To display the available links configured in each line card slot, a list of the destinations that might become inaccessible when the line card is upgraded, and a step-by-step description of the software upgrade process, use the **cs7 upgrade analysis** privileged EXEC command.

cs7 upgrade analysis

Syntax Description This command has no arguments or keywords.

Defaults None.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.

Examples The following example includes output from the **cs7 upgrade analysis** command:

```
ITP#cs7 upgrade analysis

          CS7 Version
          -----
          Major      Minor
Sup          1         1
Peer Sup     1         1
LC 1         1         1
LC 2         1         1

UPGRADE ANALYSIS FOR SLOT 1
-----

1. Linkset Name           : miramalo
   Available links (SLC)  : 0, 3

   Expected utilization of links on other slots (percent):
       Link      Rcvd      Sent
       1         7         7
   .

Step 4: Upgrade to new image on standby SUP
-----
Enter 'delete slavedisk0:old-image'
Enter 'copy disk0:new-image slavedisk0:new-image'
Enter 'hw-module module <standby sup> reset'
This will complete the upgrade process.
Verify that both SUPs are in SSO mode by entering
'show redundancy states'
```

Related Commands

Command	Description
cs7 upgrade module	Upgrades the software on the line card.

cs7 upgrade module

To upgrade the software on a line card, use the **cs7 upgrade module** privileged EXEC command.

cs7 upgrade module *slot bay*

Syntax Description	<i>slot</i>	Slot where the line card is installed.
	<i>bay</i>	Bay where the line card is installed.

Defaults	None.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples	The following example shows how to upgrade the software on the line card in slot 1, bay 0: <code>cs7 upgrade module 1 0</code>

Related Commands	Command	Description
	cs7 upgrade analysis	Displays a report indicating the probable impact of performing a software upgrade.

cs7 util-abate

To set the integer range utilization threshold, use the **cs7 util-abate** command in global configuration mode. To remove the configuration, use the **no** form of this command.

cs7 util-abate *percent*

no util-abate *percent*

Syntax Description	<i>percent</i>	Integer range utilization threshold as a percentage. The range is 0 to 40 percent. The default is 0.

Defaults	0 percent

Command Modes	Global configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	The abate delta reduces the number of cItpSpLinkRcvdUtilChange and cItpSpLinkSentUtilChange notifications generated when a link's utilization fluctuates around the specified threshold. The delta lowers the falling threshold so that a significant difference exists between the rising and falling thresholds. For example, if the threshold is set to 45 percent (using cs7 util-threshold 45) and the abate delta is set to 10 percent, then rising notifications are generated at 45 percent and falling notifications are generated at 35 percent.

This command is not instance related and cannot be specified with the **instance** keyword.

Examples	The following example shows how to set the utilization threshold to 30 percent: <pre>cs7 util-abate 30</pre>

Related Commands	Command	Description
	cs7 util-threshold	Specifies the global threshold for link utilization.
	plan-capacity-rcvd	Specifies link receive planning capacity.
	plan-capacity-send	Specifies link send planning capacity.
	threshold-rcvd	Specifies the receive threshold for a link.
	threshold-send	Specifies the send threshold for a link.

cs7 util-plan-capacity

To define a default for the **plan-capacity-rcvd** and **plan-capacity-send** configuration commands specified at the link level, use the **cs7 util-plan-capacity** command in global configuration mode. To remove the configuration, use the **no** form of this command.

cs7 util-plan-capacity *bps*

no cs7 util-plan-capacity *bps*

Syntax Description	<i>bps</i>	Default planned capacity in bps. The range is 56000 to 2147483647 bps.

Defaults	None.

Command Modes	Global configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	The configured default planned capacity is used as a default for an SCTP-based link. This value is used in place of the interface speed.
	This command is not instance related and cannot be specified with the instance keyword.

Examples	The following example shows how to set the default planned capacity to 100000 bps:
	<pre>cs7 util--plan capacity 100000</pre>

Related Commands	Command	Description
	cs7 util-abate	Specifies the integer range utilization threshold.
	cs7 util-threshold	Specifies the global threshold for link utilization.
	plan-capacity-rcvd	Specifies the link receive planning capacity.
	plan-capacity-send	Specifies the link send planning capacity.
	threshold-rcvd	Specifies the receive threshold for a link.
	threshold-send	Specifies the send threshold for a link.

cs7 util-sample-interval

To set the sample interval for link utilization, use the **cs7 util-sample-interval** command in global configuration mode. To remove the configuration, use the **no** form of this command.

cs7 util-sample-interval *seconds*

no cs7 util-sample-interval *seconds*

Syntax Description

<i>seconds</i>	Integer range utilization threshold. The range is 60 to 3600 seconds. The default is 300 seconds.

Defaults

300 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The **cs7 util-sample-interval** command specifies the duration of the sample interval. Shorter intervals allow network management systems to quickly see increases in traffic. However, shorter intervals might produce notifications that do not represent sustained link utilization problems. Longer intervals are less likely to produce false link utilization notifications, but require more time to detect link utilization problems.

This command is not instance related and cannot be specified with the **instance** keyword.

Examples

The following example shows how to set the sample interval for link utilization to 60 seconds:

```
cs7 util-sample-interval 60
```

Related Commands

Command	Description
cs7 util-abate	Specifies the integer range utilization threshold.
cs7 util-threshold	Specifies the global threshold for link utilization.
plan-capacity-rcvd	Specifies the link receive planning capacity.
plan-capacity-send	Specifies the link send planning capacity.
threshold-rcvd	Specifies the receive threshold for a link.
threshold-send	Specifies the send threshold for a link.

cs7 util-threshold

To set the global threshold for link utilization, use the **cs7 util-threshold** command in global configuration mode. To remove the configuration, use the **no** form of this command.

cs7 util-threshold *percent*

no cs7 util-threshold *percent*

Syntax Description	<i>percent</i>	Utilization threshold as a percentage. The range is 25 to 100 percent. The default is 40 percent.

Defaults	40 percent

Command Modes	Global configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	The cs7 util-threshold command specifies the rate at which a link is considered to be carrying traffic that exceeds the planned value. This value is specified as a percentage of the utilization. The cItpSpLinkRcvdUtilChange and cItpSpLinkSentUtilChange values are generated as a link's utilization rises and falls around the specified threshold.

The **cs7 util-threshold** command is global and applies to all SS7 links in this router. Thresholds on individual links can be specified using the **threshold-receive** and **threshold-send** cs7 link submodule commands.

This command is not instance related and cannot be specified with the **instance** keyword.

Examples	The following example shows how to set the threshold for link utilization to 100 percent:

```
cs7 util-threshold 100
```

Related Commands	Command	Description
	cs7 util-sample-interval	Specifies the sample interval for link utilization.

cs7 variant

To indicate which of the SS7 variations the ITP is running, use the **cs7 variant** command in global configuration mode. To remove the specification from the configuration, use the **no** form of this command.

cs7 [**instance** *instance-number*] **variant** {**ansi** | **china** | **itu** | **ttc**}

no cs7 [**instance** *instance-number*] **variant** {**ansi** | **china** | **itu** | **ttc**}

Syntax Description

instance	(Optional) Indicates which of the SS7 variations the ITP is running on an instance.
<i>instance-number</i>	Instance number. An integer value in the range 0 to 7.
ansi	American National Standards Institute (ANSI) SS7 protocol variant.
china	China SS7 protocol variant.
itu	International Telecommunications Union (ITU) SS7 protocol variant.
ttc	Japan Telecommunication Technology Committee (TTC) SS7 protocol variant, based on ITU.

Defaults

None.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

In the current release of Cisco ITP, the ANSI, CHINA, ITU, and TTC SS7 protocol variants are supported.

Cisco ITP supports the following Japan TTC standards added to the CCITT recommendations:

- Priority Indicator (PRI) field, used to transmit SUs with priority in the network.
- Generic transmission timing of SUs, including 4 new timers:
 - TA timer for sending SIE (default=20 ms)
 - TF timer for sending FISU (default=20 ms)
 - TO timer for sending SIO (default=20 ms)
 - TS timer for sending SIOS (default=20 ms)
- Outstanding number of MSUs transmittable without confirmation: MTP2/TTC uses the TTC default of 40.

- FIB and BIB comparison. If FIB or receive SU differs from BIB of last transmitted SU, the received SU is discarded.
- Negative Acknowledgement: Negative acknowledgement is transmitted by receiving a repeated MSU.
- Monitoring Timing: TTC defines SU error detection on Te timer. ITP implements the timer in the disabled state.

When you change a variant, you must remove all configurations that are specific to ITP. Remove the following ITP configuration statements in the following order:

- links
- linksets
- route table
- access list
- encapsulation on serial links (removes all MTP2 timers)
- AS route
- AS
- ASPs
- M3UA and SUA
- point code
- variant

Examples

The following example shows how to use the ANSI variant of SS7:

```
cs7 variant ansi
```

Related Commands

Command	Description
cs7 local-sccp-addr-ind	Customizes the setting of the national use field within SCCP management calling and called party addresses.
cs7 national-options	Configures the national options.
mtp2-timer ttc enable	Enables the use of the TTC TE timer.
mtp2-timer ttc te	Configures the TTC TE timer.
show cs7	Displays ITP configuration status.

cs7 xua-as-based-congestion

To enable AS Specific Congestion Level Operation, use the **cs7 xua-as-based-congestion** command in global configuration mode. To revert to the default AS PC congestion level operation, use the **no** form of this command.

cs7 xua-as-based-congestion

no cs7 xua-as-based-congestion

Syntax Description This command has no arguments or keywords.

Defaults None.

Command Modes Global configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines

In this mode, the priority of an incoming MSU is compared to the congestion level of the AS. If the priority of the MSU is lower than the AS congestion level, the MSU is dropped and counted. If TFC/SCON reporting is enabled, a TFC or SCON with the AS specific congestion level is sent to the originator of the MSU.

Because many ASes can share an AS PC, an especially busy AS can skew the congestion level for an AS PC, resulting in MSUs for ASes at lower congestion levels to be dropped. Operating in this mode can help reduce the potential of a very busy AS forcing MSU drops for other ASes that share the same PC.

In the default AS PC congestion level operation, the priority of an incoming MSU is compared to the congestion level of the AS PC for the AS. If the priority of the MSU is lower than the AS PC congestion level, the MSU is dropped and counted. If TFC/SCON reporting is enabled, a TFC or SCON with the AS PC congestion level is sent to the originator of the MSU.

Examples The following example shows how to base M3UA/SUA congestion on the AS congestion level:

```
cs7 xua-as-based-congestion
```

cs7 xua-daud-inactive

To allow ASP association establishment interworking, use the **cs7 xua-dad-inactive** command in global configuration mode. To remove the statement from the configuration, use the **no** form of this command.

cs7 xua-daud-inactive

no cs7 xua-daud-inactive

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Command Modes	Global configuration

Command History	Release	Modification
	12.2(18)IXH	This command was introduced.
	12.2(33)IRC	
	12.4(15)SW3	

Usage Guidelines	Third-party equipment may send DAUD messages to the Cisco ITP prior to the Cisco ITP sending ASPAC_ACK message. The Cisco ITP will return the error message:

Unexpected Message

Configuring the command **cs7 xua-daud-inactive** on the Cisco ITP will prevent the Cisco ITP from issuing this error message when receiving the DAUD message.

This command relates to the **RFC 3332 4.3.4.3**. section (**ASP Active Procedures**), which states:

The ASP SHOULD NOT send Data or SSNM messages for the related Routing Context(s) before receiving an ASP Active Ack message, or it will risk message loss.

Examples	The following example shows how to allow ASP association establishment interworking:

```
cs7 xua-daud-inactive
```

cs7 xua-err-diag-fmt

To modify the format of the diagnostic info parameter in outbound M3UA and SUA ERR messages, use the **cs7 xua-err-diag-fmt** command in global configuration mode. To remove the statement from the configuration, use the **no** form of this command.

cs7 xua-err-diag-fmt {msg-only | id-offset-msg}

no cs7 xua-err-diag-fmt {msg-only | id-offset-msg}

Syntax Description	id-offset-msg	Sets the diagnostic info parameter in outbound ERR messages to contain the received offending message preceded by the 4-byte err identifier and offset fields. This keyword is the default.
	msg-only	Sets the diagnostic info parameter in outbound ERR messages to contain only the received offending message (4-byte err identifier and offset fields are left out).

Defaults The **id-offset-msg** keyword

Command Modes Global configuration

Command History	Release	Modification
	12.2(18)IXG	This command was introduced.
	12.4(15)SW2	
	12.2(33)IRB	

Usage Guidelines Normally, the ITP inserts four bytes of additional information in front of returned error messages to help determine the cause of the error. Some implementations may try to examine this returned payload. These implementations require that the returned error contains only the original returned message. In that case, the four bytes of additional information inserted by the ITP may interfere with the examination of the payload. You can then use the **msg-only** keyword, which will eliminate the addition of the four bytes and allow a normal examination of the payload.

Examples The following example shows how to configure the **msg-only** keyword:

```
cs7 xua-err-diag-fmt msg-only
```

cs7 xua-errorHandling

To enable the XUA error handling feature, use the **cs7 xua-errorHandling** command in global configuration mode. To disable this feature, use the **no** form of this command.

cs7 xua-errorHandling

no cs7 xua-errorHandling

Syntax Description This command has no arguments or keywords.

Defaults By default this feature is not enabled.

Command Modes Global configuration

Command History	Release	Modification
	12.2(33)IRH 12.4(15)SW8	This command was introduced.

Usage Guidelines Enable the XUA error handling feature by using this command. To configure the counter, interval, and error codes, use the **counter** and **enable** commands in the **cs7 xua-errHandling** command submode.

Examples The following example shows how to enable XUA error handling:

```
ITP (config)# cs7 xua-errHandling

ITP(config-cs7-xua-errHandling)# ?
counter      Set the counter and interval
enable       Enable the Error types
no           Negate a command or set its defaults

ITP(config-cs7-xua-errHandling)# counter ?
<1-100>      set counter value, default is 5

ITP(config-cs7-xua-errHandling)# counter 20 interval ?
<5-600>      set interval value in seconds, default is 5 sec

ITP(config-cs7-xua-errHandling)# counter 20 interval 20

ITP(config-cs7-xua-errHandling)# enable ?
ALL          Enable all error codes, it is default action
XUA_ERR_INVALID_VERSION
XUA_ERR_UNSUPPORTED_MESSAGE_CLASS
XUA_ERR_UNSUPPORTED_MESSAGE_TYPE
XUA_ERR_UNSUPPORTED_TRAFFIC_MODE_TYPE
XUA_ERR_UNEXPECTED_MESSAGE
XUA_ERR_PROTOCOL_ERROR
XUA_ERR_INVALID_STREAM_IDENTIFIER
```

XUA_ERR_REFUSED_MANAGEMENT_BLOCKING
XUA_ERR_ASP_IDENTIFIER_REQUIRED
XUA_ERR_INVALID_ASP_IDENTIFIER
XUA_ERR_INVALID_PARAMETER_VALUE
XUA_ERR_PARAMETER_FIELD_ERROR
XUA_ERR_UNEXPECTED_PARAMETER
XUA_ERR_DESTINATION_STATUS_UNKNOWN
XUA_ERR_INVALID_NETWORK_APPEARANCE
XUA_ERR_MISSING_PARAMETER
XUA_ERR_INVALID_ROUTING_CONTEXT
XUA_ERR_NO_CONFIGURED_AS_FOR_ASP

cs7 xua-ssnm-filtering

To enable M3UA/SUA SSNM filtering, use the **cs7 xua-ssnm-filtering** command in global configuration mode. To remove the statement from the configuration, use the **no** form of this command.

cs7 xua-ssnm-filtering

no cs7 xua-ssnm-filtering

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Command Modes	Global configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples	The following example shows how to enable M3UA/SUA SSNM filtering: <pre>cs7 xua-ssnm-filtering</pre>

cs7 xua-tfc-allowed

To allow TFCs and SCONs to be sent when congestion is detected for MSUs, use the **cs7 xua-tfc-allowed** command in global configuration mode.

By default, the ITP has TFC and SCON reporting disabled. When congestion is detected for an incoming MSU, the MSU is dropped and counted, but a TFC or SCON is not sent.

To remove the statement from the configuration, use the **no** form of this command.

cs7 xua-tfc-allowed

no cs7 xua-tfc-allowed

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Command Modes	Global configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples	The following example shows how to allow TFCs and SCONs for M3UA/SUA congestion: <code>cs7 xua-tfc-allowed</code>

cumulative-sack (cs7 asp)

To configure the cumulative selective acknowledgment timeout value for the association, use the **cumulative-sack** command in cs7 asp configuration mode. To disable the configuration, use the **no** form of this command.

cumulative-sack *msec*

no cumulative-sack *msec*

Syntax Description	<i>msec</i>	Cumulative selective acknowledgment timeout value. Range is 50 to 500 milliseconds. The default is the value specified under the local port instance.

Defaults	The default acknowledgment timeout value is the value specified under the local port instance.

Command Modes	cs7 asp configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples	The following example shows how to set the cumulative selective acknowledgment timeout value to 300: <pre>cs7 asp ASP1 14001 15000 sua remote-ip 1.1.1.1 cumulative-sack 300</pre>

Related Commands	Command	Description
	cs7 asp	Specifies an application server process and enables cs7 asp submode.
	show cs7 asp detail	Displays detailed ASP information.

cumulative-sack (cs7 link)

To configure the cumulative selective acknowledgment timeout value for the link, use the **cumulative-sack** command in cs7 link configuration mode. To disable the configuration, use the **no** form of this command.

cumulative-sack *msec*

no cumulative-sack *msec*

Syntax Description

<i>msec</i>	Cumulative selective acknowledgment timeout value. Range is 50 to 500 milliseconds. The default is 200 milliseconds.

Defaults

200 milliseconds

Command Modes

cs7 link configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Examples

The following example shows how to set the cumulative selective acknowledgment timeout value to 300:

```
cs7 linkset michael 10.1.1
 link 0 sctp 172.18.44.147 7000 7000
  cumulative-sack 300
```

Related Commands

Command	Description
cs7 linkset	Specifies a linkset and enters cs7 linkset submode.
show cs7 m2pa	Displays ITP M2PA statistics.

cumulative-sack (cs7 m2pa profile)

To configure the cumulative selective acknowledgment timeout value for the link, use the **cumulative-sack** command in cs7 m2pa profile configuration mode. To disable the configuration, use the **no** form of this command.

cumulative-sack *msec*

no cumulative-sack *msec*

Syntax Description	<i>msec</i>	Cumulative selective acknowledgment timeout value. Range is 50 to 500 milliseconds. The default is 200 milliseconds.

Defaults	200 milliseconds

Command Modes	cs7 m2pa profile configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples The following example shows how to define a profile named m2parfc. The profile supports M2PA RFC, specifies the **cumulative-sack** command, and applies to all the links in the linkset named to_nyc.

```
cs7 profile m2parfc
 m2pa
  cumulative-sack 300
.
.
.
cs7 linkset to_nyc
 profile m2parfc
```

Related Commands	Command	Description
	m2pa	Specifies M2PA parameters in a CS7 profile.

cumulative-sack (cs7 m3ua)

To configure the cumulative selective acknowledgment timeout value used when a new SCTP association is started with the local port, use the **cumulative-sack** command in cs7 m3ua configuration mode. To disable the configuration, use the **no** form of this command.

cumulative-sack *msec*

no cumulative-sack *msec*

Syntax Description	<i>msec</i> Cumulative selective acknowledgment timeout value. Range is 50 to 500 milliseconds. The default is 200 milliseconds.	
Defaults	200 milliseconds	
Command Modes	cs7 m3ua configuration	
Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	
Examples	The following example shows how to set the cumulative selective acknowledgment timeout value to 300: cs7 m3ua 2905 local-IP 4.4.4.4 cumulative-sack 300	
Related Commands	Command	Description
	cs7 m3ua	Specifies the local port number for M3UA and enters cs7 m3ua submode.
	show cs7 m3ua	Displays M3UA information.

cumulative-sack (cs7 mated-sg)

To configure the cumulative selective acknowledgment timeout value for the association, use the **cumulative-sack** command in cs7 mated-sg configuration mode. To disable the configuration, use the **no** form of this command.

cumulative-sack *msec*

no cumulative-sack *msec*

Syntax Description	<i>msec</i>	Cumulative selective acknowledgment timeout value. Range is 50 to 500 milliseconds. The default is the value specified under the local SGMP port instance.

Defaults	The default selective acknowledgment timeout value is the value specified under the local SGMP port instance.

Command Modes	cs7 mated-sg configuration

Command History	Release	Modification
	12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.

Examples	The following example shows how to set the cumulative selective acknowledgment timeout value to 300: cs7 mated-sg mate2 5000 passive cumulative-sack 300

Related Commands	Command	Description
	cs7 mated-sg show cs7 mated-sg detail	Configures a connection to a mated SG. Displays detailed mated-SG information.

cumulative-sack (cs7 sgmp)

To configure the cumulative selective acknowledgment timeout value used when a new SCTP association is started with the local port, use the **cumulative-sack** command in **cs7 sgmp** configuration mode. To disable the configuration, use the **no** form of this command.

cumulative-sack *msec*

no cumulative-sack *msec*

Syntax Description	<i>msec</i>	Cumulative selective acknowledgment timeout value. Range is 50 to 500 milliseconds. The default is 200 milliseconds.

Defaults	200 milliseconds

Command Modes	cs7 sgmp configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples	The following example shows how to set the cumulative selective acknowledgment timeout value to 300:
	<pre>cs7 sgmp 5000 cumulative-sack 300</pre>

Related Commands	Command	Description
	cs7 sgmp	Specifies the local port number for SGMP and enters cs7 sgmp submode.
	show cs7 sgmp	Displays SGMP information.

cumulative-sack (cs7 sua)

To configure the cumulative selective acknowledgment timeout value used when a new SCTP association is started with the local port, use the **cumulative-sack** command in cs7 sua configuration mode. To disable the configuration, use the **no** form of this command.

cumulative-sack *msec*

no cumulative-sack *msec*

Syntax Description	<i>msec</i>	Cumulative selective acknowledgment timeout value. Range is 50 to 500 milliseconds. The default is 200 milliseconds.

Defaults	200 milliseconds

Command Modes	cs7 sua configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples	The following example shows how to set the cumulative selective acknowledgment timeout value to 300:
	cs7 sua 15000
	local-IP 4.4.4.4
	cumulative-sack 300

Related Commands	Command	Description
	cs7 sua	Specifies the local port number for SUA and enters cs7 sua submode.
	show cs7 sua	Displays SUA information.

cdcs

To add or remove a DCS endpoint to or from a DCS group, use the **cdcs** command in `cs7 dcs-group` configuration mode. To disable the configuration, use the **no** form of this command.

cdcs *name cost*

no dcs *name cost*

Syntax Description

cdcs	Endpoint that receives a proprietary probeless monitoring protocol (PMP).
<i>name</i>	Identifies the name of the DCS node that is added or removed from the DCS group. The name is specified as an alphanumeric string with a maximum of 12 characters.
<i>cost</i>	Defines which DCS node to use first if more than one DCS node is available in this DCS group. An integer with a value of 0 or 1.

Defaults

None.

Command Modes

`cs7 dcs-group` configuration

Command History

Release	Modification
12.4(15)SW3	This command was introduced.
12.2(33)IRC	

Usage Guidelines

The following rules and restrictions apply when configuring the **cdcs** command:

- You cannot delete a DCS group that is referenced by a linkset or AS.
- You cannot delete a DCS node that is referenced by a DCS group.
- You cannot add more than eight DCS nodes to a group.
- You cannot add a DCS node that is not configured to a DCS group.

Examples

The following example shows how to configure the DCS node with the name `cdcs4` and a cost of 0:

```
cs7 dcs-group dcs-group2
  dcs cdcs4 cost 0
```

Related Commands

Command	Description
<code>cs7 dcs-group</code>	Identifies a name to be associated with a DCS group.
<code>cs7 pmp</code>	Turns probeless monitoring on for all linksets and ASes.
<code>cs7 pmp hold-queue</code>	Sets the integer range of PMP hold queue thresholds.

Command	Description
show cs7 pmp	Displays errors and information about the PMP.
show cs7 dcs-group	Displays information about the DCS group.
show cs7 dcs	Displays information about the DCS node.

dcs-group

To associate a DCS group with a linkset or AS, use the **dcs-group** command in `cs7` linkset or `cs7` as configuration submode. To remove the DCS group, use the **no** form of this command.

dcs-group *dcs-group-name* { **in** | **out** | **all** }

no dcs-group { **in** | **out** | **all** }

Syntax Description

<i>dcs-group-name</i>	Identifies the name of the DCS group that is added or removed to or from the top mode of the linkset or AS. The name is specified as an alphanumeric string with a maximum of 12 characters.
in out all	Specifies the direction of the traffic that is copied to the specified group.

Defaults

None.

Command Modes

`cs7` linkset or `cs7` as configuration submode

Command History

Release	Modification
12.4(15)SW3	This command was introduced.
12.2(33)IRC	

Usage Guidelines

This command assigns existing DCS groups to monitor the inbound, outbound, or both-side traffic of a linkset or AS. The direction can be set to **all** only when no DCS group is yet assigned to the linkset or AS.

Examples

The following example shows how to use `cs7` linkset configuration mode to configure the DCS group named `group_pmp_01` with a direction of **all**:

```
cs7 instance 0 linkset to_balance_0 0.1.1
dcs-group group_pmp_01 all
cs7 instance 6 linkset to_halley_6 6.3.3
dcs-group group_pmp_02 in
dcs-group group_pmp_01 out
```

Related Commands

Command	Description
<code>cs7 dcs-group</code>	Identifies a name to be associated with a DCS group.
<code>cs7 pmp</code>	Turns probeless monitoring on for all linksets and ASes.
<code>cs7 pmp hold-queue</code>	Sets the integer range of PMP hold queue thresholds.
<code>cs 7 dcs</code>	Identifies a name to be associated with a DCS node.
<code>show cs7 pmp</code>	Displays errors and information about the PMP.

Command	Description
show cs7 dcs-group	Displays information about the DCS group.
show cs7 dcs	Displays information about the DCS node.

default

To create a default secondary trigger, use the **default** command in cs7 mlr trigger configuration mode within a primary address trigger. To disable the specific routing trigger, use the **no** form of this command.

```
default { block | continue | ruleset ruleset-name | result { pc pc [ssn ssn] | asname as-name | gt gta [gt-addr-type] | group group-name } }
```

```
no default { block | continue | ruleset ruleset-name | result { pc pc [ssn ssn] | asname as-name | gt gta [gt-addr-type] | group group-name } }
```

Syntax Description

block	Drops messages matching this trigger. The block keyword is ignored if combination triggers are defined within cs7 mlr trigger mode.
continue	Routes messages matching this trigger as received. This behavior is the same as if no primary trigger had been matched. The continue keyword is ignored if combination triggers are defined within cs7 mlr trigger mode.
ruleset	Specifies the MLR ruleset table that should be used if this trigger is matched, and not overruled by a secondary trigger ruleset.
<i>ruleset-name</i>	Name of an already defined CS7 MLR ruleset table. The name is specified as a character string with a maximum of 12 characters.
result	(Optional) Allows MLR users to route messages based on the trigger alone. If a trigger result is configured, the TCAP/MAP/SMS layers are not parsed. If a message matches a trigger with a result trigger action, then the message is redirected as indicated in the trigger result. Note: Result groups with dest-sme-binding mode are not valid trigger results.
pc	Routes based on point code.
<i>pc</i>	Point code.
ssn	(Optional) Routes based on PC and subsystem number.
<i>ssn</i>	Subsystem number.
asname	Routes based on AS name.
<i>as-name</i>	AS name.
gt	Routes based on global title.
<i>gta</i>	Global title address.
group	Routes based on result group.
<i>group-name</i>	Result group name.

Defaults

None.

Command Modes

cs7 mlr trigger configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

A combination trigger uses more than one network layer address for identifying a trigger match. One address is defined as the primary trigger and the other as the secondary trigger.

If you configure a secondary address in trigger submode, then *both* addresses must match for the packet to be routed using the specified ruleset.

With the definition of the secondary triggers configured as an *and* function with the primary trigger, a default secondary trigger handles packet routing on the primary trigger only when one or more other secondary triggers are defined.

The **default** command is used only if all other subtriggers are unmatched. If **default** is not specified, then packets not matching a combination trigger are routed according to standard SCCP or MTP3 procedures.

Examples

The following example shows how to define three secondary triggers based on the origin of the SMS message. All messages *not* originating from one of the secondary triggers are routed based on the default secondary trigger.

```
cs7 mlr table sms_table
trigger cdpa gt 9193334444 ruleset default_rules
cgpa gt 1111111 ruleset msc1_rules
cgpa gt 2222222 ruleset msc2_rules
cgpa gt 3333333 ruleset msc3_rules
!
default ruleset default_rules
```

Related Commands

Command	Description
cs7 mlr ruleset	Specifies sets of rules that will be used to process traffic matching triggers defined in a multilayer routing table.
show cs7 mlr table	Displays multilayer SMS routing information.
trigger cdpa (cs7 mlr table)	Specifies a routing trigger that is located in the SCCP called party address field of the incoming MSU.
trigger cgpa (cs7 mlr table)	Specifies a routing trigger that is located in the SCCP calling party address field of the incoming MSU.

default result

To specify the default screening result, use the **default result** command in gateway screening table configuration mode.

default result {**action** *action-set-name* | **table** *table-name*}

no default

Syntax Description

action	Screens by action set by default.
<i>action-set-name</i>	Action-set name. Valid names may not exceed 12 alphanumeric characters.
table	Screens by table by default.
<i>table-name</i>	Table name. Valid names may not exceed 12 alphanumeric characters.

Defaults

None.

Command Modes

Gateway screening table configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

Results defined as a screening step action can be either an action set or the next screening table name. The **default result** command is used in all screening tables, including gateway link set tables and AS tables.

Examples

The following example shows how to define the allowed DPC table and specify the default result as an action:

```
cs7 instance 6 gws table OPC6 type opc action allowed
default result action ALLOW
```

The following example shows how to define the allowed cgpa-pc-ssn table and specify the default result as a chained table:

```
cs7 instance 0 gws table PCSSN1 type cgpa-pc-ssn action allowed
default result table SEL1
```

Related Commands

Command	Description
show cs7 gws table	Displays GWS table information.

description (cs7 link)

To specify a description of the link, use the **description** command in cs7 link configuration mode. To remove the text string, use the **no** form of this command.

description *line*

no description *line*

Syntax Description	<i>line</i>	Text string description of the link. The string can be from 1 to 254 alphanumeric characters.

Defaults	None.

Command Modes	cs7 link configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples	The following example shows how to provide a description of link 0:

```
cs7 linkset to_doc
link 0
  description Link used to connect to point code 5.100.2
```

Related Commands	Command	Description
	cs7 linkset	Specifies a linkset and enters cs7 linkset submode.
	link (cs7 linkset)	Specifies a link and enters cs7 link submode.
	show cs7 linkset	Displays ITP linkset information.

description (cs7 linkset)

To specify a description of the linkset to be used by the administrator or the network management stations, use the **description** command in cs7 linkset configuration mode. To remove the text string, use the **no** form of this command.

description *line*

no description *line*

Syntax Description

<i>line</i>	Text string description of the linkset. The string can be from 1 to 254 alphanumeric characters.

Defaults

None.

Command Modes

cs7 linkset configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Examples

The following example shows how to provide a description for the linkset:

```
cs7 linkset to-Chicago-primary
description to-Chicago-primary
```

Related Commands

Command	Description
cs7 linkset	Specifies a linkset and enters cs7 linkset submode.
show cs7 linkset	Displays linkset information.

dest-port (cs7 mlr ruleset rule)

To specify a particular application port number value for a GSM MAP sms-mo or sms-mt operation, use the **dest-port** command in cs7 mlr ruleset rule configuration mode. To remove the statement, use the **no** form of this command.

dest-port *dest-port-number*

no dest-port *dest-port-number*

Syntax Description	<i>dest-port-number</i> Destination port number. Valid range is 0 to 65535.	
Defaults	None.	
Command Modes	cs7 mlr ruleset rule configuration	
Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	
Examples	The following example shows how to specify the address of the destination port number of 1234: cs7 mlr ruleset ruleset1 rule 10 gsm-map sms-mt dest-port 1234	
Related Commands	Command	Description
	rule (cs7 mlr ruleset)	Specifies the rules for a routing trigger within a multilayer ruleset table and enables cs7 mlr ruleset rule configuration mode.

dest-sme (cs7 mlr ruleset rule)

To specify the address of the destination short message entity (SME), use the **dest-sme** command in cs7 mlr ruleset rule configuration mode. To remove the specification, use the **no** form of this command.

dest-sme { * | *dest-addr* } [**exact**] [**min-digits** *min*] [**max-digits** *max*] [*dest-sme-addr-type*]

no dest-sme { * | *dest-addr* } [**exact**] [**min-digits** *min*] [**max-digits** *max*] [*dest-sme-addr-type*]

Syntax Description

*	Matches all address values.
<i>dest-addr</i>	When the rule operation is sms-mo, the <i>dest-addr</i> is an address string of 1 to 20 hexadecimal characters. When the rule operation is sri-sm, <i>dest-addr</i> is an address string of 1 to 16 hexadecimal characters. The string is not input in BCD-String format, but in normal form. The string always carries an implicit wildcard (*) at the end of the string, allowing only the prefix of a range of addresses to be specified.
<i>dest-sme-addr-type</i>	(Optional) Parameters that identify attributes of the SME address being used to match a rule. The address is composed of the following keywords: • [ton ton] The ton keyword specifies the type of number value associated with the SME address. The <i>ton</i> argument is an integer value in the range 0 to 7. • [np np] The np keyword specifies the numbering plan identification value associated with the SME address. The np keyword is not valid when defining the dest-sme in an smsNot operation. The <i>np</i> argument is an integer value in the range 0 to 15. • min Specifies that the address is a Mobile Identification Number (MIN). This keyword can be specified for the <i>sme-addr-type</i> of ANSI-41 operations. • imsi Specifies that the address is an International Mobile Subscriber Identification (IMSI) address. This keyword can be specified for the <i>sme-addr-type</i> of ANSI-41 operations.
exact	Indicates that the previously specified <i>dest-addr</i> should be matched only if the number of digits <i>and</i> the digit values match exactly as specified in <i>dest-addr</i> . If exact is not specified, then <i>dest-addr</i> carries an implicit wildcard (*) at the end of the string, allowing a match on the string as a prefix (range of addresses).
min-digits	(Optional) Specifies the minimum number of digits in the address string.
<i>min</i>	Minimum number of digits in the address string. The default is 1.
max-digits	(Optional) Specifies the maximum number of digits in the address string.
<i>max</i>	Maximum number of digits in the address string. The default is the length of the address string.

Defaults

See Syntax Description.

Command Modes cs7 mlr ruleset rule configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines **MLR/SMS rule-matching implementations before ITP release 12.2(25)SW3**
In ITP releases earlier than 12.2(25)SW3, MLR/SMS configuration allows matching of a rule parameter noa value with an incoming message as follows:

- If **noa 0** (noa unknown) is specified in a rule parameter, then MLR matches that rule to incoming messages containing the corresponding parameter, regardless of the corresponding parameter noa value.
- If an incoming message contains a parameter with noa unknown, then MLR matches that message to a rule for the corresponding parameter, regardless of the rule parameter noa specification.

MLR/SMS rule-matching implementations in ITP release 12.2(25)SW3

Starting with ITP release 12.2(25)SW3, MLR/SMS configuration allows matching of a rule parameter type of number/numbering plan (ton/np) value with an incoming message as follows:

- A new **ton** keyword replaces the **noa** keyword. The keywords **ton** and **np** are optional and mutually independent.
- If **ton/np** is specified on a rule parameter, then MLR matches that rule to only those incoming messages containing the exact ton/np value in the corresponding parameter.
- If **ton/np** is not specified on a rule parameter, then MLR matches that rule to incoming messages containing the corresponding parameter, regardless of the ton/np value received.

The **dest-sme** command allows you to specify the address of the destination SME within an SMS operation. This parameter is part of the rule used to match this route.

For the **sms-mo** operation, **dest-sme** identifies the SM-TP-DA field within the SMS user information field.

For the **sms-mt** operation, **dest-sme** identifies the IMSI contained in the SM-RP-DA field within the GSM MAP layer.

For the **sri-sm** operation, **dest-sme** identifies the destination MSISDN address within the GSM MAP layer.

[Table 20](#) shows the uses of the **dest-sme** command based on the rule operation.

Table 29 Dest-SME by Operation

	Length in hex	No <i>dest-sme-addr-type</i>	<i>dest-sme-addr-type</i> specified
sms-mo	1–20	Defaults to digit string matching only.	specific np/ton
sms-mt	1–20	Defaults to digit string matching only.	specific np/ton

Table 29 **Dest-SME by Operation**

	Length in hex	No <i>dest-sme-addr-type</i>	<i>dest-sme-addr-type</i> specified
sri-sm	1–16	Defaults to digit string matching only.	Specific np/ton
alertsc	1–16	Defaults to digit string matching only.	Specific np/ton
smdpp	1–20	Priority digit string matching based on the following order: SMS_OriginalDestinationAddress SMS_DestinationAddress MIN IMSI SCCP CdPA (RI=GT only)	min = MIN parameter only imsi = IMSI parameter only np/ton = Full address matching based on the parameter order: SMS_OriginalDestinationAddress SMS_DestinationAddress
smsReq	1–20	Priority digit string matching based on the following order: MobileDirectoryNumber MIN IMSI SCCP CdPA (RI=GT only)	min = MIN parameter only imsi = IMSI parameter only np/ton = MobileDirectoryNumber parameter only
smsNot	1–20	Priority digit string matching based on the following order: MobileDirectoryNumber MIN IMSI	min = MIN parameter only imsi = IMSI parameter only np/ton = MobileDirectoryNumber parameter only

Examples

The following example shows how to specify the address of the destination SME:

```
cs7 mlr ruleset ruleset1
rule 10 sms-mo
dest-sme 1234
```

Related Commands

Command	Description
match-unknown-ton-np (cs7 mlr ruleset rule)	Specifies that messages with unknown TON/NP will match the corresponding address parameters regardless of the rule's configured TON/NP.
rule (cs7 mlr ruleset)	Specifies the rules for a routing trigger within a multilayer ruleset table and enables cs7 mlr ruleset rule configuration mode.

dest-sme (cs7 sms set rule)

To specify a destination short message entity (SME), use the **dest-sme** command in cs7 sms set rule configuration mode. To remove the configuration, use the **no** form of this command.

dest-sme { * | *dest-address* } [**exact**] | [**min-digits** *min*] | [**max-digits** *max*] [*dest-sme-addr-type*]

no dest-sme { * | *dest-address* } [**exact**] | [**min-digits** *min*] | [**max-digits** *max*] [*dest-sme-addr-type*]

Syntax Description	
*	Matches all address values.
<i>dest-address</i>	Address of 1 to 20 hexadecimal digits.
<i>dest-sme-addr-type</i>	(Optional) Parameters that identify attributes of the SME address being used to match a rule. The address is composed of the following keywords: [ton <i>ton</i>] The ton keyword specifies type of number value associated with the SME address. The <i>ton</i> argument is an integer value in the range 0 to 7. [np <i>np</i>] The np keyword specifies the numbering plan identification value associated with the SME address. The np keyword is not valid when defining the dest-sme in an smsNot operation. The <i>np</i> argument is an integer value in the range 0 to 15.
exact	(Optional) Configured address must match dest-sme exactly.
min-digits	(Optional) Specifies the minimum number of digits in the address string.
<i>min</i>	Minimum number of digits in the address string. The default is 1.
max-digits	(Optional) Specifies the maximum number of digits in the address string.
<i>max</i>	Maximum number of digits in the address string. The default is the length of the address string.

Defaults See Syntax Description.

Command Modes cs7 sms set rule configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines **MLR/SMS rule-matching implementations before ITP release 12.2(25)SW3**
 In ITP releases earlier than 12.2(25)SW3, MLR/SMS configuration allows matching of a rule parameter noa value with an incoming message as follows:

- If **noa 0** (noa unknown) is specified in a rule parameter, then SMS matches that rule to incoming messages containing the corresponding parameter, regardless of the corresponding parameter noa value.
- If an incoming message contains a parameter with noa unknown, then SMS matches that message to a rule for the corresponding parameter, regardless of the rule parameter noa specification.

MLR/SMS rule-matching implementations in ITP release 12.2(25)SW3

Starting with ITP release 12.2(25)SW3, MLR/SMS configuration allows matching of a rule parameter type of number/numbering plan (ton/np) value with an incoming message as follows:

- A new **ton** keyword replaces the **noa** keyword. The keywords **ton** and **np** are optional and mutually independent.
- If **ton/np** is specified on a rule parameter, then SMS matches that rule to only those incoming messages containing the exact ton/np value in the corresponding parameter.
- If **ton/np** is not specified on a rule parameter, then SMS matches that rule to incoming messages containing the corresponding parameter, regardless of the ton/np value received.

Examples

The following example shows how to specify an SMS ruleset named SMS-RULES. The ruleset specifies a rule index of 20 and a destination SME matching all addresses.

```
cs7 sms ruleset SMS-RULES
rule 20 sms-mo
  dest-sme *
  result next-rule
```

Related Commands

Command	Description
cs7 sms ruleset	Specifies a ruleset.
dest-sme (cs7 mlr ruleset rule)	Specifies an application destination port number.
dest-sme-table (cs7 sms set rule)	Specifies an SMS table of destination SME addresses.
dest-smsc (cs7 sms set rule)	Specifies a destination SMSC.
match-unknown-ton-np (cs7 sms set rule)	Specifies that messages with unknown TON/NP will be a match to the corresponding address parameters regardless of the rule's configured TON/NP.
orig-imsi (cs7 sms set rule)	Specifies an origin IMSI.
orig-imsi-table (cs7 sms set rule)	Specifies an SMS table of origin IMSI addresses (address-table).
orig-sme (cs7 sms set rule)	Specifies an origin short message entity (SME).
orig-sme-table (cs7 sms set rule)	Specifies an SMS table of origin SME addresses (address-table).
pid (cs7 sms set rule)	Specifies a protocol identifier (TP-PID).
result (cs7 sms set rule)	Specifies a result.
ruleset (cs7 sms ansi41 smsnot)	Specifies a rule within a ruleset.

dest-sme-table (cs7 mlr ruleset rule)

To configure an MLR table of destination SME addresses, use the **dest-sme-table** command in cs7 mlr ruleset rule configuration mode. To remove the specification, use the **no** form of this command.

dest-sme-table *table-name* [*dest-sme-addr-type*]

no dest-sme-table

Syntax Description	
<i>table-name</i>	IMSI address table name. Valid range is up to 16 hexadecimal digits.
<i>dest-sme-addr-type</i>	(Optional) Parameters that identify attributes of the SME address being used to match a rule for the sms-mo and smpdd operation types. The address is composed of the following keywords: • [ton ton] The ton keyword specifies the type of number value associated with the SME address. The <i>ton</i> argument is an integer value in the range 0 to 7. • [np np] The np keyword specifies the numbering plan identification value associated with the SME address. The np keyword is not valid when defining the dest-sme in an smsNot operation. The <i>np</i> argument is an integer value in the range 0 to 15. • min Specifies that the address is a Mobile Identification Number (MIN). This keyword can be specified for the sme-addr-type of ANSI-41 operations. • imsi Specifies that the address is an International Mobile Subscriber Identification (IMSI) address. This keyword can be specified for the sme-addr-type of ANSI-41 operations.

Defaults None.

Command Modes cs7 mlr ruleset rule configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines **MLR/SMS rule-matching implementations before ITP release 12.2(25)SW3**

In ITP releases earlier than 12.2(25)SW3, MLR/SMS configuration allows matching of a rule parameter noa value with an incoming message as follows:

- If **noa 0** (noa unknown) is specified in a rule parameter, then MLR matches that rule to incoming messages containing the corresponding parameter, regardless of the corresponding parameter noa value.

- If an incoming message contains a parameter with noa unknown, then MLR matches that message to a rule for the corresponding parameter, regardless of the rule parameter noa specification.

MLR/SMS rule-matching implementations in ITP release 12.2(25)SW3

Starting with ITP release 12.2(25)SW3, MLR/SMS configuration allows matching of a rule parameter type of number/numbering plan (ton/np) value with an incoming message as follows:

- A new **ton** keyword replaces the **noa** keyword. The keywords **ton** and **np** are optional and mutually independent.
- If **ton/np** is specified on a rule parameter, then MLR matches that rule to only those incoming messages containing the exact ton/np value in the corresponding parameter.
- If **ton/np** is not specified on a rule parameter, then MLR matches that rule to incoming messages containing the corresponding parameter, regardless of the ton/np value received.

Examples

The following example shows how to specify an address of the destination SME:

```
cs7 mlr ruleset ruleset1
rule 10 sms-mt
dest-sme-table 2
```

Related Commands

Command	Description
match-unknown-ton-np (cs7 mlr ruleset rule)	Specifies that messages with unknown TON/NP will match the corresponding address parameters regardless of the rule's configured TON/NP.
rule (cs7 mlr ruleset)	Specifies the rules for a routing trigger within a multilayer ruleset table and enables cs7 mlr ruleset rule configuration mode.

dest-sme-table (cs7 sms set rule)

To specify an SMS table of destination SME addresses (address-table), use the **dest-sme-table** command in **cs7 sms set rule** configuration mode. To remove the configuration, use the **no** form of this command.

dest-sme-table *table-name* [*dest-sme-addr-type*]

no dest-sme-table

Syntax Description	<i>table-name</i>	Address table name.
	<i>dest-sme-addr-type</i>	(Optional) Parameters that identify attributes of the SME address being used to match a rule for the sms-mo and sri-sm operation types. The address is composed of the following keywords: • [ton ton] The ton keyword specifies type of number value associated with the SME address. The <i>ton</i> argument is an integer value in the range 0 to 7. • [np np] The np keyword specifies the numbering plan identification value associated with the SME address. The np keyword is not valid when defining the dest-sme in an smsNot operation. The <i>np</i> argument is an integer value in the range 0 to 15.

Defaults None.

Command Modes cs7 sms set rule configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines **MLR/SMS rule-matching implementations before ITP release 12.2(25)SW3**
 In ITP releases earlier than 12.2(25)SW3, MLR/SMS configuration allows matching of a rule parameter noa value with an incoming message as follows:

- If **noa 0** (noa unknown) is specified in a rule parameter, then SMS matches that rule to incoming messages containing the corresponding parameter, regardless of the corresponding parameter noa value.
- If an incoming message contains a parameter with noa unknown, then SMS matches that message to a rule for the corresponding parameter, regardless of the rule parameter noa specification.

MLR/SMS rule-matching implementations in ITP release 12.2(25)SW3

Starting with ITP release 12.2(25)SW3, MLR/SMS configuration allows matching of a rule parameter type of number/numbering plan (ton/np) value with an incoming message as follows:

- A new **ton** keyword replaces the **noa** keyword. The keywords **ton** and **np** are optional and mutually independent.
- If **ton/np** is specified on a rule parameter, then SMS matches that rule to only those incoming messages containing the exact ton/np value in the corresponding parameter.
- If **ton/np** is not specified on a rule parameter, then SMS matches that rule to incoming messages containing the corresponding parameter, regardless of the ton/np value received.

The **dest-sme-table**, **orig-imsi-table**, and **orig-sme-table** commands accept either an SMS address table name *or* an MLR address table name. This ability is primarily for customers who want the SMS-MO Proxy functionality. The address table names are unique between DSMR and MLR. You may enter an MLR address table name for an SMS rule parameter. However, MLR cannot reference SMS address tables.

If an incoming message matches an SMS rule that references an MLR address table, then any MLR address table result is mapped to an SMS result:

- BLOCK, PC, and PCSSN results map easily from MLR to SMS.
 - For result groups, the MLR result group name is mapped to an SMS result group name.
 - If the SMS result group is not configured, then the result specified on the rule is used.
- AS and CONTINUE results are not valid in SMS. For these cases, the result specified on the rule is used. If no result is specified, the result on the rule is used (same as MLR).

If multiple rule parameters are configured for a rule, then the rule result is used (rather than a result specified in the address table).

If the result type specified within the table is valid, it is used. Otherwise, the result in the rule is used.

For all tables, the **ton** and **np** must match before the table is accessed.

Examples

The following example shows how to specify an SMS ruleset named SMS-RULES. The ruleset specifies a rule index of 20 and an SMS table of destination SME addresses named SHORTLIST.

```
cs7 sms ruleset SMS-RULES
rule 20 sms-mo
  dest-sme-table SHORTLIST
  result block
```

Related Commands

Command	Description
cgpa (cs7 mlr trigger)	Tests the availability of CDR service queue as the input condition of the rule.
cs7 sms ruleset	Specifies a ruleset.
dest-sme (cs7 mlr ruleset rule)	Specifies an application destination port number.
dest-sme (cs7 sms set rule)	Specifies a destination short message entity (SME).
dest-smsc (cs7 sms set rule)	Specifies a destination SMSC.
match-unknown-ton-np (cs7 sms set rule)	Specifies that messages with unknown TON/NP will match the corresponding address parameters regardless of the rule's configured TON/NP.
orig-imsi (cs7 sms set rule)	Specifies an origin IMSI.

Command	Description
orig-imsi-table (cs7 sms set rule)	Specifies an SMS table of origin IMSI addresses (address-table).
orig-sme (cs7 sms set rule)	Specifies an origin SME.
orig-sme-table (cs7 sms set rule)	Specifies an SMS table of origin SME addresses (address-table).
pid (cs7 sms set rule)	Specifies a protocol identifier (TP-PID).
result (cs7 sms set rule)	Specifies a result.
ruleset (cs7 sms ansi41 smsnot)	Specifies a rule within a ruleset.

dest-smsc (cs7 mlr ruleset rule)

To specify the destination service center address, use the **dest-smsc** command in cs7 mlr ruleset rule configuration mode. To remove the specification, use the **no** form of this command.

dest-smsc { * | *address* } [**exact**] | [**min-digits** *min*] | [**max-digits** *max*] [*addr-type*]

no dest-smsc

Syntax Description	
*	Matches all addresses.
<i>address</i>	Address of 1 to 20 hexadecimal digits.
<i>addr-type</i>	(Optional) Parameters that identify attributes of the SMSC address being used to match a rule. The address is composed of the following keywords: • [ton <i>ton</i>] The ton keyword specifies the type of number value associated with the SMSC address. The <i>ton</i> argument is an integer value in the range 0 to 7. • [np <i>np</i>] The np keyword specifies the numbering plan identification value associated with the SMSC address. The <i>np</i> argument is an integer value in the range 0 to 15.
exact	(Optional) Configured address must match dest-smc exactly.
min-digits	(Optional) Specifies the minimum number of digits in the address string.
<i>min</i>	Minimum number of digits in the address string. The default is 1.
max-digits	(Optional) Specifies the maximum number of digits in the address string.
<i>max</i>	Maximum number of digits in the address string. The default is the length of the address string.

Defaults See Syntax Description.

Command Modes cs7 mlr ruleset rule configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines **MLR/SMS rule-matching implementations before ITP release 12.2(25)SW3**
In ITP releases earlier than 12.2(25)SW3, MLR/SMS configuration allows matching of a rule parameter noa value with an incoming message as follows:

- If **noa 0** (noa unknown) is specified in a rule parameter, then MLR matches that rule to incoming messages containing the corresponding parameter, regardless of the corresponding parameter noa value.
- If an incoming message contains a parameter with noa unknown, then MLR matches that message to a rule for the corresponding parameter, regardless of the rule parameter noa specification.

MLR/SMS rule-matching implementations in ITP release 12.2(25)SW3

Starting with ITP release 12.2(25)SW3, MLR/SMS configuration allows matching of a rule parameter type of number/numbering plan (ton/np) value with an incoming message as follows:

- A new **ton** keyword replaces the **noa** keyword. The keywords **ton** and **np** are optional and mutually independent.
- If **ton/np** is specified on a rule parameter, then MLR matches that rule to only those incoming messages containing the exact ton/np value in the corresponding parameter.
- If **ton/np** is not specified on a rule parameter, then MLR matches that rule to incoming messages containing the corresponding parameter, regardless of the ton/np value received.

If intermediate GTT is used toward the ITP SMS routers, then the CdPA routing trigger already contains the destination SMSC address and does not need to be specified on the rule.

Examples

The following example shows how to specify the destination service center address:

```
cs7 mlr ruleset ruleset1
rule 20 sms-mo
dest-smsc 1234
```

Related Commands

Command	Description
match-unknown-ton-np (cs7 mlr ruleset rule)	Specifies that messages with unknown TON/NP will match the corresponding address parameters regardless of the rule's configured TON/NP.
rule (cs7 mlr ruleset)	Specifies the rules for a routing trigger within a multilayer ruleset table and enables cs7 mlr ruleset rule configuration mode.

dest-smsc (cs7 sms set rule)

To specify a destination short message entity, use the **dest-sme** command in cs7 sms set rule configuration mode. To remove the configuration, use the **no** form of this command.

dest-smsc { * | *address* } [**exact**] | [**min-digits** *min*] | [**max-digits** *max*] [*addr-type*]

no dest-smsc

Syntax Description

*	Matches all addresses.
<i>address</i>	Address of 1 to 20 hexadecimal digits.
<i>addr-type</i>	(Optional) Parameters that identify attributes of the SMSC address being used to match a rule. The address is composed of the following keywords: [ton <i>ton</i>] The ton keyword specifies the type of number value associated with the SMSC address. The <i>ton</i> argument is an integer value in the range 0 to 7. [np <i>np</i>] The np keyword specifies the numbering plan identification value associated with the SMSC address. The <i>np</i> argument is an integer value in the range 0 to 15.
exact	(Optional) Configured address must match dest-sme exactly.
min-digits	(Optional) Specifies the minimum number of digits in the address string.
<i>min</i>	Minimum number of digits in the address string. The default is 1.
max-digits	(Optional) Specifies the maximum number of digits in the address string.
<i>max</i>	Maximum number of digits in the address string. The default is the length of the address string.

Defaults

See Syntax Description.

Command Modes

cs7 sms set rule configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

MLR/SMS rule-matching implementations before ITP release 12.2(25)SW3

In ITP releases earlier than 12.2(25)SW3, MLR/SMS configuration allows matching of a rule parameter noa value with an incoming message as follows:

- If **noa 0** (noa unknown) is specified in a rule parameter, then SMS matches that rule to incoming messages containing the corresponding parameter, regardless of the corresponding parameter noa value.
- If an incoming message contains a parameter with noa unknown, then SMS matches that message to a rule for the corresponding parameter, regardless of the rule parameter **noa** specification.

MLR/SMS rule-matching implementations in ITP release 12.2(25)SW3

Starting with ITP release 12.2(25)SW3, MLR/SMS configuration allows matching of a rule parameter type of number/numbering plan (ton/np) value with an incoming message as follows:

- A new **ton** keyword replaces the **noa** keyword. The keywords **ton** and **np** are optional and mutually independent.
- If **ton/np** is specified on a rule parameter, then SMS matches that rule to only those incoming messages containing the exact ton/np value in the corresponding parameter.
- If **ton/np** is not specified on a rule parameter, then SMS matches that rule to incoming messages containing the corresponding parameter, regardless of the ton/np value received.

Examples

The following example shows how to specify an SMS ruleset named SMS-RULES. The ruleset specifies a rule index of 20 and a destination SMSC matching all addresses.

```
cs7 sms ruleset SMS-RULES
rule 20 sms-mo
dest-smsc *
result block
```

Related Commands

Command	Description
cs7 sms ruleset	Specifies a ruleset.
dest-sme (cs7 mlr ruleset rule)	Specifies an application destination port number.
dest-sme (cs7 sms set rule)	Specifies a destination short message entity (SME).
dest-sme-table (cs7 sms set rule)	Specifies an SMS table of destination SME addresses.
match-unknown-ton-np (cs7 sms set rule)	Specifies that messages with unknown TON/NP will match the corresponding address parameters regardless of the rule's configured TON/NP.
orig-imsi (cs7 sms set rule)	Specifies an origin IMSI.
orig-imsi-table (cs7 sms set rule)	Specifies an SMS table of origin IMSI addresses (address-table).
orig-sme (cs7 sms set rule)	Specifies an origin SME.
orig-sme-table (cs7 sms set rule)	Specifies an SMS table of origin SME addresses (address-table).
pid (cs7 sms set rule)	Specifies a protocol identifier (TP-PID).
result (cs7 sms set rule)	Specifies a result.
ruleset (cs7 sms ansi41 smsnot)	Specifies a rule within a ruleset.

digits

To configure an MSC address in an SMS MSC table that indicates time zone information for an MSC relative to the ITP, use the **digits** command in `cs7 sms msc table` configuration mode. To remove the specification, use the **no** form of this command.

digits *address* **time-offset** { **add** | **subtract** } *time-difference*

no digits *address* **time-offset** { **add** | **subtract** } *time-difference*

Syntax Description

<i>address</i>	Full or partial prefix MSC E.164 address. All MSCs with E.164 addresses that include the coded prefix assume the traits configured for this MSC table entry.
time-offset	Specifies that the MSC is in a different time zone from the ITP.
add	Specifies that time is added to the ITP local time to match the MSC local time.
subtract	Specifies that time is subtracted from the ITP local time to match the MSC local time.
<i>time-difference</i>	Time offset to be applied to ITP local time to match MSC local time. Valid format is <i>hh:mm</i> where <i>hh</i> is the number of hours and <i>mm</i> is the number of minutes.

Defaults

If an MSC table is not configured, all messages to mobile destinations are delivered with delivery times indicating the local time of the ITP, regardless of the time zone of the message destination.

Command Modes

`cs7 sms msc table` configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The SMS MSC table stores information pertaining to MSCs with which the ITP communicates. The table stores information that indicates the time zone information for each MSC relative to the ITP.

If you configure an MSC table, short messages are delivered with delivery times indicated in the MSC's local time, which is typically also the local time of the receiver of the message.

If an MSC table is not configured, by default all messages to mobile destinations are delivered with delivery times indicating the local time of the ITP, regardless of whether the destination is in the same time zone as the ITP or not.

Examples

The following example shows how to specify SMS MSC addresses in an SMS MSC table:

```
cs7 sms msc-table
digits 19199332252 time-offset subtract 01:00
digits 1505 time-offset subtract 01:00
```

Related Commands

Command	Description
cs7 sms offload	Enables cs7 sms msc table configuration mode, in which you can configure an SMS MSC table.

display-name (cs7 link)

To define a text string to be included on traps related to the link, use the **display-name** command in cs7 link configuration mode. To remove the text string, use the **no** form of this command.

display-name *line*

no display-name *line*

Syntax Description

<i>line</i>	Text string description for the link. Length can be 30 characters.

Defaults

The default value of *line* is a formatted string containing the linkset name and the ITP point code.

Command Modes

cs7 link configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Examples

The following example shows how to configure the display name for the link:

```
cs7 linkset to_doc
link 0
display-name link0
```

Related Commands

Command	Description
cs7 linkset	Specifies a linkset and enters cs7 linkset submode.
link (cs7 linkset)	Specifies a link and enters cs7 link submode.
show cs7	Displays the ITP basic configuration, including the point code and capability point code.

display-name (cs7 linkset)

To define a text string to be included on traps related to the linkset, use the **display-name** command in cs7 linkset configuration mode. To remove the text string, use the **no** form of this command.

display-name *line*

no display-name *line*

Syntax Description

<i>line</i>	Text string description for the linkset. Length can be 30 characters.

Defaults

The default value of *line* is a formatted string containing the linkset name.

Command Modes

cs7 linkset configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Examples

The following example shows how to configure the display name for the linkset:

```
cs7 linkset to_doc
 display-name to_doc
```

Related Commands

Command	Description
cs7 linkset	Specifies a linkset and enters cs7 linkset submode.
show cs7	Displays the ITP basic configuration, including the point code and capability point code.

distribute-sccp-sequenced-negate

To negate the instance level setting of evenly distributing class1 SCCP non-segmented messages in an application group, use the **distribute-sccp-sequenced-negate** command in cs7 gtt application group submode. To return to the instance level setting, use the **no** form of this command.

distribute-sccp-sequenced-negate

no distribute-sccp-sequenced-negate

Defaults

None.

Command Modes

cs7 gtt application group submode

Command History

Release	Modification
12.4(15)SW5	This command was introduced.
12.2(33)IRE	

Usage Guidelines

The **distribute-sccp-sequenced-negate** command in application group submode can override the instance level setting of in-sequence or out-of-sequence delivery for that specific application group.

The following table explains the ITP behavior for the different configuration combinations:

Instance Level 0 Configuration	Application Group Alpha Configuration	
cs7 instance 0 distribute-sccp-sequenced	distribute-sccp-sequenced -negate	
not configured	not configured	Default in-sequence delivery for all the application groups in instance 0.
not configured	configured	In-sequence delivery for all the application groups in the instance 0 except out-of-sequence delivery for application group Alpha.
configured	not configured	Out-of-sequence delivery for all the application groups in instance 0.
configured	configured	Out-of-sequence delivery for all the application groups in the instance 0 except in-sequence delivery for application group Alpha.

Examples

The following example shows the **distribute-sccp-sequenced-negate** command in application group submode overriding the instance level **distribute-sccp-sequenced** command for application group alpha:

```
cs7 instance 0 distribute-sccp-sequenced
cs7 instance 0 gtt application-group alpha
multiplicity share
distribute-sccp-sequenced-negate
pc 1671 1 pcssn
pc 1672 1 pcssn
pc 1741 1 pcssn
pc 1740 1 pcssn
```

Related Commands

Command	Description
cs7 gtt application-group	Specifies a GTT application group.
cs7 gtt map	Configures a Global Title Mated Application (MAP) entry.
cs7 distribute-sccp-sequenced	Configures class 1 SCCP messages to use round-robin loadsharing.
pc (cs7 gtt application group)	Adds or changes a point code and optional subsystem number in the application group.
asname (cs7 gtt application group)	Assigns an M3UA or SUA AS directly to a global title
cs7 sccp-class1-wrr	Configures the WRR option for GTT application groups.

dpc

To configure a destination point code (DPC) entry in the PAM table, use the **dpc** command in CS7 PAM configuration submode. To remove the specification, use the **no** form of this command.

dpc *point-code*

no dpc *point-code*

Syntax Description

<i>point-code</i>	The signaling point code in the point code format.

Defaults

None.

Command Modes

CS7 PAM configuration submode

Command History

Release	Modification
12.4(15)SW5	This command was introduced.
12.2(33)IRE	

Usage Guidelines

None.

Examples

The following example shows the dpc signaling point code entry 2.3.4 in the point code format. It is configured for the PAM table named alpha:

```
cs7 instance 0 pam alpha
  cgpa gt prefix tt 0 pc 1.2.3 ssn 12
  cdpa gt prefix 15 123456789abcdef tt 250 gti 4 np 15 nai 127 pc 1.123.4 ssn 255
  opc 1.2.3
  dpc 2.3.4
  modify-failure resume
```

Related Commands

Command	Description
cs7 pam	Identifies a packet address modification (PAM) table and enters the CS7 PAM submode.
cgpa (cs7 pam)	Configures one cgpa entry in the PAM table.
cdpa (cs7 pam)	Configures one cdpa entry in the PAM table.
opc	Configures an OPC entry in the PAM table.
modify-failure (pam)	Specifies the desired action when the PAM table packet modification fails.

Command	Description
cs7 gws action-set	Defines gateway screening action sets that may include a PAM table.
gta asname	Creates or modifies a GTA entry that translates to an M3UA or SUA application server name. The GTA entry may include a PAM table.



ITP Command Set: E - R

This section documents new or modified commands. All other commands for this feature are documented in the Cisco IOS Command Reference publications.

- [egress-rate-lmt-timer \(config-gws-as\), page 760](#)
- [egress-rate-lmt-timer \(config-gws-ls\), page 761](#)
- [emdt, page 762](#)
- [enable-ussd ussd-tree-type \(cs7 mlr options\), page 764](#)
- [encapsulation hs-mtp2, page 766](#)
- [encapsulation mtp2, page 767](#)
- [exclude-concatSM-from-multiMsgDialogue, page 768](#)
- [execute-on all show cs7 offload instance, page 770](#)
- [false-congestion, page 774](#)
- [fast-cwnd-rate \(cs7 asp\), page 775](#)
- [fast-cwnd-rate \(cs7 link\), page 776](#)
- [fast-cwnd-rate \(cs7 m2pa profile\), page 777](#)
- [fast-cwnd-rate \(cs7 m3ua\), page 779](#)
- [fast-cwnd-rate \(cs7 mated-sg\), page 780](#)
- [fast-cwnd-rate \(cs7 \), page 781](#)
- [fast-cwnd-rate \(cs7 sua\), page 782](#)
- [gt \(cs7 mlr result\), page 783](#)
- [gta app-grp, page 785](#)
- [gta asname, page 787](#)
- [gta pcssn, page 789](#)
- [gta-prefix, page 791](#)
- [gta qos-class, page 793](#)
- [gta-start, page 795](#)
- [gtt-accounting \(as\), page 796](#)
- [gtt-accounting \(linkset\), page 797](#)
- [hold-transport \(cs7 link\), page 798](#)

- [hold-transport \(cs7 m2pa profile\)](#), page 799
- [hs-mtp2](#), page 800
- [hs-mtp2-timer \(cs7 link\)](#), page 801
- [hsl](#), page 803
- [idle-cwnd-rate \(cs7 asp\)](#), page 804
- [idle-cwnd-rate \(cs7 link\)](#), page 805
- [idle-cwnd-rate \(cs7 mated-sg\)](#), page 806
- [idle-cwnd-rate \(cs7 m2pa profile\)](#), page 807
- [idle-cwnd-rate \(cs7 m3ua\)](#), page 809
- [idle-cwnd-rate \(cs7 \)](#), page 810
- [idle-cwnd-rate \(cs7 sua\)](#), page 811
- [inbound \(config-gws-as\)](#), page 812
- [inbound \(config-gws-ls\)](#), page 814
- [init-cwnd-size \(cs7 asp\)](#), page 816
- [init-cwnd-size \(cs7 link\)](#), page 817
- [init-cwnd-size \(cs7 m2pa profile\)](#), page 818
- [init-cwnd-size \(cs7 m3ua\)](#), page 820
- [init-cwnd-size \(cs7 mated-sg\)](#), page 821
- [init-cwnd-size \(cs7 \)](#), page 822
- [init-cwnd-size \(cs7 sua\)](#), page 823
- [init-ip-dscp](#), page 824
- [init-ip-precedence](#), page 825
- [init-retransmit \(cs7 link\)](#), page 826
- [init-retransmit \(cs7 m2pa profile\)](#), page 827
- [init-retransmit \(cs7 m3ua\)](#), page 828
- [init-retransmit \(cs7 \)](#), page 829
- [init-retransmit \(cs7 sua\)](#), page 830
- [init-timeout \(cs7 link\)](#), page 831
- [init-timeout \(cs7 m2pa profile\)](#), page 832
- [init-timeout \(cs7 m3ua\)](#), page 833
- [init-timeout \(cs7 \)](#), page 834
- [init-timeout \(cs7 sua\)](#), page 835
- [insert-dpc-in-cdpa](#), page 836
- [ip-dscp \(cs7 m2pa profile\)](#), page 838
- [ip-precedence \(cs7 link\)](#), page 839
- [ip-precedence \(cs7 m2pa profile\)](#), page 840
- [isup-msg-type](#), page 841
- [keepalive \(cs7 asp\)](#), page 843

- [keepalive \(cs7 link\), page 844](#)
- [keepalive \(cs7 m2pa profile\), page 845](#)
- [keepalive \(cs7 m3ua\), page 846](#)
- [keepalive \(cs7 mated-sg\), page 847](#)
- [keepalive \(cs7\), page 848](#)
- [keepalive \(cs7 sua\), page 849](#)
- [large-msu-support \(cs7 link submode\), page 850](#)
- [large-msu-support \(cs7 m2pa profile\), page 851](#)
- [large-msu-support \(cs7 link submode\), page 850](#)
- [large-msu-support \(cs7 m2pa profile\), page 851](#)
- [linestate debounce, page 852](#)
- [link \(cs7 linkset\), page 853](#)
- [linkset \(cs7 billing account configuration submode\), page 856](#)
- [link-test, page 858](#)
- [link-timer, page 859](#)
- [load \(cs7 route table\), page 862](#)
- [local-ip \(cs7 dcs\), page 864](#)
- [local-ip \(cs7 m3ua\), page 866](#)
- [local-ip \(cs7 \), page 867](#)
- [local-ip \(cs7 sua\), page 868](#)
- [m2pa, page 869](#)
- [map-version, page 871](#)
- [match access-group, page 872](#)
- [match any \(cs7 asp\), page 873](#)
- [match any \(cs7 linkset\), page 874](#)
- [match si \(cs7 asp\), page 875](#)
- [match si \(cs7 linkset\), page 876](#)
- [match-unknown-ton-np \(cs7 mlr ruleset rule\), page 877](#)
- [max-inbound-streams \(cs7 m3ua\), page 883](#)
- [max-inbound-streams \(cs7 \), page 884](#)
- [max-inbound-streams \(cs7 sua\), page 885](#)
- [modify-failure \(pam\), page 887](#)
- [modify-profile \(cs7 mlr ruleset rule\), page 889](#)
- [mtp2, page 893](#)
- [mtp2-timer, page 894](#)
- [mtp2-timer ttc enable, page 896](#)
- [multiplicity, page 897](#)
- [nai, page 899](#)

- [network-appearance](#), page 900
- [new-name](#), page 901
- [next-table](#), page 902
- [np](#), page 904
- [opc](#), page 905
- [orig-imsi \(cs7 mlr ruleset rule\)](#), page 906
- [orig-imsi-table \(cs7 mlr ruleset rule\)](#), page 910
- [orig-sme \(cs7 mlr ruleset rule\)](#), page 914
- [orig-sme-table \(cs7 mlr ruleset rule\)](#), page 920
- [orig-smsc \(cs7 mlr ruleset rule\)](#), page 925
- [orig-smsc \(cs7 mlr modify-profile\)](#), page 927
- [outbound \(config-gws-as\)](#), page 929
- [outbound \(config-gws-ls\)](#), page 931
- [pam \(cs7 mlr ruleset rule\)](#), page 933
- [path-retransmit \(cs7 asp\)](#), page 935
- [path-retransmit \(cs7 link\)](#), page 936
- [path-retransmit \(cs7 m2pa profile\)](#), page 937
- [path-retransmit \(cs7 m3ua\)](#), page 938
- [path-retransmit \(cs7 mated-sg\)](#), page 939
- [path-retransmit \(cs7 \)](#), page 940
- [path-retransmit \(cs7 sua\)](#), page 941
- [pc \(cs7 gtt application group\)](#), page 942
- [pc \(cs7 mlr result\)](#), page 944
- [pc-range](#), page 946
- [pc-range ssn](#), page 947
- [peer-timer \(cs7 link\)](#), page 948
- [peer-timer \(cs7 m2pa profile\)](#), page 950
- [pid \(cs7 mlr ruleset rule\)](#), page 952
- [ping cs7](#), page 955
- [ping-interval](#), page 957
- [plan-capacity-rcvd](#), page 959
- [plan-capacity-send](#), page 961
- [pmp \(cs7 as\)](#), page 963
- [pmp \(cs7 linkset\)](#), page 965
- [point-code \(mtp3\)](#), page 967
- [point-code \(sccp\)](#), page 968
- [post-gtt-address-conversion](#), page 970
- [power enable unsequence](#), page 971

- [pre-gtt-address-conversion](#), page 972
- [preserve-opc \(cs7 mlr ruleset\)](#), page 973
- [preserve-opc \(cs7 mlr options\)](#), page 974
- [preventive-txp](#), page 975
- [qos-access-group](#), page 976
- [qos-class \(cs7 as\)](#), page 977
- [qos-class \(cs7 asp\)](#), page 978
- [qos-class \(cs7 gtt selector\)](#), page 979
- [qos-class \(cs7 link\)](#), page 980
- [qos-class \(cs7 mated-sg\)](#), page 981
- [qos-ip-dscp](#), page 982
- [qos-ip-precedence](#), page 983
- [rate-limit rate \(cs7 gws as rate-limit-timer\)](#), page 984
- [rate-limit rate \(gws as egress-rate-lmt-timer\)](#), page 987
- [rate-limit rate \(gws linkset egress-rate-lmt-timer\)](#), page 989
- [rate-limit rate \(gws linkset rate-limit-timer\)](#), page 991
- [rate-limit-timer \(cs7 gws as\)](#), page 994
- [rate-limit-timer \(cs7 gws linkset\)](#), page 996
- [receive-window \(cs7 local peer\)](#), page 998
- [receive-window \(cs7 m3ua\)](#), page 1000
- [receive-window \(cs7 \)](#), page 1001
- [receive-window \(cs7 sua\)](#), page 1002
- [recovery-timeout](#), page 1003
- [remote-ip \(cs7 asp\)](#), page 1004
- [remote-ip \(cs7 dcs\)](#), page 1005
- [remote-ip \(cs7 mated-sg\)](#), page 1007
- [remove route \(route table\)](#), page 1008
- [result \(cs7 mlr ruleset rule\)](#), page 1013
- [result \(cs7 sms set rule\)](#), page 1017
- [retransmit-cwnd-rate \(cs7 asp\)](#), page 1020
- [retransmit-cwnd-rate \(cs7 link\)](#), page 1022
- [retransmit-cwnd-rate \(cs7 m2pa profile\)](#), page 1024
- [retransmit-cwnd-rate \(cs7 m3ua\)](#), page 1026
- [retransmit-cwnd-rate \(cs7 mated-sg\)](#), page 1028
- [retransmit-cwnd-rate \(cs7 \)](#), page 1030
- [retransmit-cwnd-rate \(cs7 sua\)](#), page 1032
- [retransmit-timeout \(cs7 asp\)](#), page 1034
- [retransmit-timeout \(cs7 link\)](#), page 1036

- [retransmit-timeout \(cs7 m2pa profile\)](#), page 1038
- [retransmit-timeout \(cs7 m3ua\)](#), page 1040
- [retransmit-timeout \(cs7 mated-sg\)](#), page 1042
- [retransmit-timeout \(cs7 \)](#), page 1044
- [retransmit-timeout \(cs7 sua\)](#), page 1046
- [rotate-sls](#), page 1048
- [routing-key \(cs7 as\)](#), page 1050
- [rule \(cs7 mlr ruleset\)](#), page 1054

egress-rate-lmt-timer (config-gws-as)

To enable the rate limit feature on egress traffic of a given AS and set its associated timer, use the **egress-rate-lmt-timer** command in gws as configuration mode. To disable the rate limit feature on egress traffic of a given AS, use the **no** form of this command.

egress-rate-lmt-timer *timer*

no egress-rate-lmt-timer

Syntax Description	<i>timer</i>	Integer value, in seconds. The range is from 1 to 60.

Defaults	Disabled

Command Modes	gws as configuration (config-gws-as)

Command History	Release	Modification
	12.2(33)IRG	This command was introduced.
	12.4(15)SW7	

Usage Guidelines	The rate limit feature screens outgoing MSUs for the configured time period (<i>timer</i> value) and during this time period discards outbound MSUs that exceed the configured rate-limit rate value. To disable the rate limit feature on egress traffic of a given AS, remove the configuration. First, remove the rate-limit rate command in the egress-rate-lmt-timer configuration submode. Then, use the no form of the egress-rate-lmt-timer command.

Examples	The following example shows how to configure an outbound rate limit and its timer:

```
cs7 instance 0 gws as name as-1
  outbound result action-set as1
  egress-rate-lmt-timer 5
    rate-limit rate 2000 onset-threshold 80 abate-threshold 60
```

Related Commands	Command	Description
	show cs7 gws as	Displays ITP gateway screening information for the AS.

egress-rate-lmt-timer (config-gws-ls)

To enable the rate limit feature on egress traffic of a given linkset and set its associated timer, use the **egress-rate-lmt-timer** command in gws linkset configuration mode. To disable the rate limit feature on egress traffic of a given linkset, use the **no** form of this command.

egress-rate-lmt-timer *timer*

no egress-rate-lmt-timer

Syntax Description	<i>timer</i>	Integer value, in seconds. The range is from 1 to 60.

Defaults	Disabled

Command Modes	gws linkset configuration (config-gws-ls)

Command History	Release	Modification
	12.2(33)IRG	This command was introduced.
	12.4(15)SW7	

Usage Guidelines	The rate limit feature screens outgoing MSUs for the configured time period (<i>timer</i> value) and during this time period discards outbound MSUs that exceed the configured rate-limit rate value. To disable the rate limit feature on egress traffic of a given linkset, remove the configuration. First, remove the rate-limit rate command in the egress-rate-lmt-timer configuration submode. Then, use the no form of the egress-rate-lmt-timer command.

Examples	The following example shows how to configure an outbound rate-limit and its timer:

```
cs7 instance 0 gws linkset name ls-1
  outbound result action as1
  egress-rate-lmt-timer 5
  rate-limit rate 2000 onset-threshold 80 abate-threshold 60
```

Related Commands	Command	Description
	show cs7 gws linkset	Displays ITP gateway screening information for the linkset.

emdt

To specify the MSU data format encapsulation of the egress PMP packets, use the **emdt** **cs7 dcs** configuration submode command. To revert to the default encapsulation, use the **no** form of this command.

emdt [**emdt1** | **emdt2**]

no emdt

Syntax Description

emdt1	Encapsulated MSU Data Type 1. Takes advantage of an SNMP MIB to reduce the overhead of the MSU encapsulation header. This data type is the default.
emdt2	Encapsulated MSU Data Type 2. Includes all the context information with the MSU.

Defaults

The default data type is emdt1.

Command Modes

cs7 dcs configuration submode

Command History

Release	Modification
12.4(15)SW3	This command was introduced.
12.2(33)IRC	

Usage Guidelines

As with emdt1, emdt2 sends one or more MSUs together to the data collection server (DCS) node. The difference between emdt1 and emdt2 is that emdt2 includes all the context information together with the MSU. Including this information causes emdt2 to take up more encapsulation space than emdt1.

Examples

The following example shows how to configure emdt2 on the DCS node:

```
edmt emdt2
```

Related Commands

Command	Description
pmp (cs7 linkset)	Turns probeless monitoring on for a linkset.
pmp (cs7 as)	Turns probeless monitoring on for an AS.
cs7 dcs-group	Identifies a name to be associated with a DCS group.
cs7 pmp hold-queue	Sets the integer range of a PMP hold queue threshold.
cs7 dcs	Identifies a name to be associated with a DCS node.
show cs7 pmp	Displays errors and information about the PMP.

Command	Description
show cs7 dcs-group	Displays information about the DCS group.
show cs7 dcs	Displays information about the DCS node.

enable-ussd ussd-tree-type (cs7 mlr options)

To enable the USSD feature and set the USSD transaction timeout value, use the **enable-ussd ussd-tree-type** command in the cs7 mlr options submode. To disable the USSD feature, use the **no** form of this command.

enable-ussd ussd-tree-type *type* [**ussd-timer** *timer*]

no enable-ussd

Syntax Description	ussd-tree-type	Indicates the key used for USSD transaction tree.
	<i>type</i>	1. Based on tid
		2. Based on combination of opc and tid
	ussd-timer	Indicates the USSD transaction timeout value.
	<i>timer</i>	Integer value, in seconds. The range is from 1 to 180. The default is 120.

Defaults Disabled.

Command Modes cs7 mlr options submode

Command History	Release	Modification
	12.4(15)SW7	This command was introduced.
	12.2(33)IRG	

Usage Guidelines This command enables the USSD feature and establishes the USSD transaction timeout value to time out inactive USSD transactions.

A mobileUSSD MLR ruleset should be applied for both mobileInitiated USSD requests and their corresponding response messages. The purpose of applying a mobileUSSD rule on the response messages is to perform USSD processing on response messages. Only the request messages are routed based on the result of the mobileUSSD MLR rule. The response messages are not routed based on the result of the mobileUSSD MLR rule. The response messages are routed at SCCP/MTP3.

Examples The following example shows how to route mobile-initiated GSM-MAP messages containing USSD string *123*/# to DPC 1234:

```
cs7 ins 0 mlr options
  enable ussd-tree-type 2 ussd-timer 180
```

```
cs7 ins 0 mlr ruleset abc
  rule 1 gsm-map mobileUSSD
  ussd-string 123
  result pc 1234
```

```
cs7 instance 0 gws action-set ussd_action mlr ruleset abc
cs7 instance 0 gws linkset name from_msc
    inbound result action ussd_action
cs7 instance 0 gws linkset name from_ussd
    inbound result action ussd_action
```

The following example shows how to filter mobile-initiated GSM-MAP messages containing USSD string *123*/#:

```
cs7 ins 0 mlr options
    enable ussd-tree-type 2 ussd-timer 180

cs7 ins 0 mlr ruleset abc
    rule 1 gsm-map mobileUSSD
        ussd-string 123
        result block
```

Related Commands

Command	Description
cs7 mlr options	Specifies MLR global options.
show cs7 mlr options	Displays the MLR global options.

encapsulation hs-mtp2

To specify high-speed MTP2 encapsulation, use the **encapsulation hs-mtp2** command in interface configuration mode. To turn off high-speed MTP2 encapsulation for the interface and return to the default HDLC encapsulation, use the **no** form of this command.

encapsulation hs-mtp2

no encapsulation hs-mtp2

Syntax Description	This command has no arguments or keywords.

Defaults	The default encapsulation is HDLC.

Command Modes	Interface configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	After specifying the encapsulation, you can create a profile of high-speed MTP2 parameters and then apply the profile to all the links in a linkset. Or, you can specify high-speed MTP2 parameters for individual links.

Examples	The following example shows how to configure serial interface 4/1/0:0 to use high-speed MTP2 encapsulation:

```
interface serial4/1/0:0
no ip address
encapsulation hs-mtp2
```

Related Commands	Command	Description
	cs7 profile	Specifies a set of parameters that can be applied to links in a linkset.
	hs-mtp2-timer (cs7 link)	Specifies high-speed MTP2 timers for a link.

encapsulation mtp2

To specify MTP2 encapsulation, use the **encapsulation mtp2** command in interface configuration mode. To turn off MTP2 encapsulation for the interface and return to the default HDLC encapsulation, use the **no** form of this command.

encapsulation mtp2

no encapsulation mtp2

Syntax Description This command has no arguments or keywords.

Defaults The default encapsulation is HDLC.

Command Modes Interface configuration

Command History	Release	Modification
	12.2(18)IXA 12.4(11)SW 12.2(33)IRA 12.4(11)SW	This command was introduced.

Usage Guidelines The **encapsulation mtp2** command allows the interface to recognize SS7/MTP2 protocol packets and implements the MTP2 protocol on that interface. Traditional SS7 links use serial interfaces. You must configure ITP router interfaces to use MTP2 encapsulation.

Examples The following example shows how to configure serial interface 0 to use MTP2 encapsulation:

```
interface serial0/0
no ip address
encapsulation mtp2
```

Related Commands	Command	Description
	mtp2-timer	Tunes MTP2 encapsulation timers.

exclude-concatSM-from-multiMsgDialogue

To allow SMS-MO messages that are concatenated at the SMS layer to be routed directly with MLR, use the **exclude-concatSM-from-multiMsgDialogue** command in cs7 mlr options configuration mode. To remove the feature, use the **no** form of this command.

exclude-concatSM-from-multiMsgDialogue

no exclude-concatSM-from-multiMsgDialogue

Syntax Description This command has no keywords or arguments.

Defaults This command is disabled.

Command Modes cs7 mlr options configuration

Command History	Release	Modification
	12.2(18)IXG	This command was introduced.
	12.4(15)SW2	
	12.2(33)IRB	

Usage Guidelines You must meet at least one of the following conditions to use the **exclude-concatSM-from-multiMsgDialogue** command:

- The MSC ensures that generated concatenated SMs do not trigger TCAP/MAP segmentation.
- The MLR and SMS-MO Proxy rules for handling the last message in the SMS concatenation chain are identical, and configuration ensures that the same SMSC will receive all messages in the chain.
- The receiving SMSC complex does not require all messages in a concatenated message chain to be sent to the same SMSC.

Table 31 shows whether SMS layer segmented data sent within a TCAP begin message and with an invoke component will match the MLR rule.

Table 30 *Effect of exclude-concatSM-from-multiMsgDialogue on MLR Rule Matching*

	exclude-concatSM-from-multiMsgDialogue	no exclude-concatSM-from-multiMsgDialogue
rule 10 gsm-map sms-mo multi-message-dialogue result pc 7.7.2		Match rule
rule 10 gsm-map sms-mo orig-sme * result pc 7.7.1	Match rule	
rule 10 gsm-map sms-mo default allow-multi-message-dialogue result pc 7.7.1	Match rule	Match rule
rule 10 gsm-map sms-mo default result pc 7.7.1	Match rule	

As for the multi-message-dialogue (MMD), the following messages are not affected by this command and route using MO-Proxy.

- Segmented Begin without component
- Begin with MMS (more message to send)
- Segmented Continue without component
- Segmented Continue with component

Examples

The following example shows how to set up all incoming messages from a link (LINK0) to trigger the MLR_RULE. However, because **exclude-concatSM-from-multiMsgDialogue** has been configured, both concatenated messages and non-MMD messages will hit rule 30 and be routed to pc 7.7.1.

```
cs7 mlr options
exclude-concatSM-from-multiMsgDialogue
!
cs7 mlr ruleset MLR_RULE
rule 15 gsm-map sms-mo
multi-message-dialogue
result pc 7.7.2
rule 30 gsm-map sms-mo
orig-sme *
result pc 7.7.1
!
cs7 gws action-set ACTION1 mlr ruleset MLR_RULE
cs7 gws linkset name LINK0
inbound result action ACTION1
```

Related Commands

Commands	Description
cs7 mlr options	Specifies MLR global options.
preserve-opc (cs7 mlr ruleset)	Specifies an MLR ruleset and application layer protocol filter for the ruleset.

execute-on all show cs7 offload instance

To display the current status, counters, and events maintained by the cs7 offload feature, use the **execute-on all show cs7 offload instance** EXEC command.

execute-on {*flex-wan-number* | **all-flex**} **all show cs7 offload instance**

Syntax Description

<i>flex-wan-number</i>	Designates the output is from a specified FlexWan.
all-flex	Designates the output is from all FlexWans.
offload	The transfer of data operations.

Defaults

None.

Command Modes

EXEC

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

For the Cisco ITP Supervisor Module, the user enters the command **execute-on** {*flex-wan-number* | **all-flex**} **all show cs7 offload instance**. The similar **show cs7 offload instance** command is used for a Cisco ITP FlexWan.

Examples

The following output excerpt includes some of the most significant output fields for the **show cs7 offload instance** command. [Table 31](#) defines these output fields.

```
ITP# show cs7 offload instance

Instance 1
Point Code          235-33-0:1
SS7 Variant         ANSI

Dropped MSUs:
-----
bufferedPak_drops    0
bufferedPak_flushes  0
mgmt_pak_drops       0
tfc_attempt_drops    0
    tfc_attempt_count  0
loop_detected_drops  0
in_acl_drop          0
dcs7_route_pak_fail 125
no_route_link        124
out_acl_drop         0
alias_route_pak_fail 0
```



```

no_olink_err          0
invalid_pak_size_drops 0
circ rt detection drops 0
opc verification drops 0
no_rt_handle
current interval      0    total 6

```

Table 31 Significant Output Fields for the **show cs7 offload** command

Field	Description
bufferedPak_drops	Cisco ITP has capability to buffer packets at link level equal to bufferPak_threshold per instance. If the packets to be buffered exceed this threshold for an instance, ITP drops these packets and increase this counter.
bufferedPak_flushes	When the link or route is removed, then Cisco ITP flushes the packets if any are already buffered for that link/route. This counter is increased for every packet flushed.
tfc_attempt_drops	Increases to count number of times TFC was dropped.
tfc_attempt_count	Increases to count number of times TFC was send.
loop_detected_drops	Increases for packets drop due to loop detection by ITP.
in_acl_drop	Increases for the packet dropped due to inbound ACL/GWS.
dcs7_route_pak_fail	Increases when the routing of the packet is unsuccessful because no link is available in a linkset.
no_route_link	Increases when current route is not available due to the non-availabilty of the links in a linkset.
out_acl_drop	Increases for the outbound packet dropped due to ACL/GWS.
alias_route_pak_fail	Increases when the routing to the alias pc failed.
no_olink_err	Increases when the outgoing link is not
invalid_pak_size_drops	Increases when the sizeof mtp3 packet received at ITP is invalid.
circ rt detection drops	Increases when MSUs dropped due to CRD
mgmt_pak_drops	Increases when MGMT paks drop
opc verification drops	Increase for packet drop due to opc verification failed when CRD is enabled.
no_rt_handle/Count/total	Increases when there is no route info for the destination.

The following output is from the **execute-on {flex-wan-number | all-flex} all show cs7 offload instance** command.

```

ITP_251#execute-on 3 all show cs7 offload instance
----- slot:3 cpu:0 command:show cs7 offload instance -----

Global configuration:
=====
dcs7_tfc_exceeding_max_rate(LC pacing): 0

Origination table is disabled

Instance specific configuration:
=====

```

■ execute-on all show cs7 offload instance

```

Instance 0
Point Code          3.1.1:0
SS7 Variant         ITU
Network Indicator   national
Secondary PCs       3.2.2
Capability PCs
C-link linkset      (none)
C-link linkset secondary (none)
Total Linksets      7
Available Linksets  2
Total Links         7
Available Links     0
Ok to activate links T
natopt_tfr          F
natopt_multcon      F
sccp_unsequenced    T
sccp_sequenced      T
natopt_rct          F
natopt_cls_ls       T
use_summary_routing T
mgmt_sls_value       0
itu_sls_shift_opc_dpc F   opc shift = 0   dpc shift = 0
itu_sls_shift        0
Circular rt detection F
sccp_class1_loadshare F
sccp_class1_wrr      F
mgmt_sls_type        Round Robin
remote_cong_msgs     T
punt                 F
mlr_enabled          F
gws_enabled          F
Large MSU Support    F
bufferedPak_count    0
bufferedPak_count_peak 0
bufferedPak_threshold 20000

```

Dropped MSUs:

```

-----
bufferedPak_drops      0
bufferedPak_flushes   0
mgmt_pak_drops         0
tfc_attempt_drops     0
    tfc_attempt_count  0
loop_detected_drops    0
in_acl_drop            0
dcs7_route_pak_fail    0
no_route_link          0
out_acl_drop           0
alias_route_pak_fail   0
no_olink_err           0
invalid_pak_size_drops 0
circ rt detection drops 0
opc verification drops 0
no_rt_handle
current interval      0   total 0

```

Informational Counts:

```

-----
alias_instance_punt    0
olink_punt             0
invalid_pak_size (bytes) 0
dcs7_send_vip_pak_fails 0

```


false-congestion

To configure the false congestion detection level for a linkset, use the **false-congestion** command in **cs7** linkset configuration mode. To remove the setting, use the **no** form of this command.

false-congestion *level*

no false-congestion *level*

Syntax Description	<i>level</i> Level at which false congestion is detected. Valid values are 1, 2, or 3.	
Defaults	None.	
Command Modes	cs7 linkset configuration	
Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	
Examples	The following example shows how to set false congestion level 2 for the linkset named to_doc: cs7 linkset to_doc false-congestion 2	
Related Commands	Command	Description
	cs7 linkset	Specifies a linkset and enters cs7 linkset submode.
	show cs7	Displays the ITP basic configuration, including the point code and capability point code.

fast-cwnd-rate (cs7 asp)

To configure the rate at which the SCTP congestion window size is reduced due to a fast retransmission, use the **fast-cwnd-rate** command in cs7 asp configuration mode. To disable the configuration, use the **no** form of this command.

fast-cwnd-rate *percent*

no fast-cwnd-rate *percent*

Syntax Description	<i>percent</i>	Rate at which the size of the SCTP congestion window is decreased due to a fast retransmission. Range is 0 to 100 percent. The default is 50 percent.

Defaults	The default rate is 50 percent.

Command Modes	cs7 asp configuration

Command History	Release	Modification
	12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.

Usage Guidelines	The fast-cwnd-rate command allows the administrator to configure a rate at which the SCTP congestion window is decreased due to a fast retransmission on the SCTP association.



Caution

The behavior of the SCTP congestion control algorithms is not compliant with RFC 2960 or RFC 4960 when this command is changed to values other than the default. This command should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples	The following example shows how to set the fast congestion window rate to 60 percent:

```
cs7 asp ASP1 2905 2905 m3ua
remote-ip 1.1.1
fast-cwnd-rate 60
```

Related Commands	Command	Description
	retransmit-cwnd-rate (cs7 asp)	Configures the rate at which the SCTP congestion window size is reduced due to retransmission timer expirations.

fast-cwnd-rate (cs7 link)

To configure the rate at which the SCTP congestion window size is reduced due to a fast retransmission, use the **fast-cwnd-rate** command in cs7 link configuration mode. To disable the configuration, use the **no** form of this command.

fast-cwnd-rate *percent*

no fast-cwnd-rate *percent*

Syntax Description	<i>percent</i>	Rate at which the size of the SCTP congestion window is decreased due to a fast retransmission. Range is 0 to 100 percent. The default is 50 percent.

Defaults	The default rate is 50 percent.

Command Modes	cs7 link configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	The fast-cwnd-rate command allows the administrator to configure a rate at which the SCTP congestion window is decreased due to a fast retransmission on the SCTP association.



Caution

The behavior of the SCTP congestion control algorithms is not compliant with RFC 2960 or RFC 4960 when this command is changed to values other than the default. This command should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples	The following example shows how to set the fast congestion window rate to 60 percent:

```
cs7 linkset michael 10.1.1
 link 0 sctp 172.18.44.147 7000 7000

 fast-cwnd-rate 60
```

Related Commands	Command	Description
	retransmit-cwnd-rate (cs7 link)	Rate at which the size of the SCTP congestion window is decreased due to a fast retransmission. Range is 0 to 100 percent. The default is 50 percent.

fast-cwnd-rate (cs7 m2pa profile)

To configure the rate at which the SCTP congestion window size is reduced due to a fast retransmission, use the **fast-cwnd-rate** command in cs7 m2pa profile configuration mode. To disable the configuration, use the **no** form of this command.

fast-cwnd-rate *percent*

no fast-cwnd-rate *percent*

Syntax Description	<i>percent</i>	Rate at which the size of the SCTP congestion window is decreased due to a fast retransmission. Range is 0 to 100 percent. The default is 50 percent.

Defaults	The default rate is 50 percent.

Command Modes	cs7 m2pa profile configuration

Command History	Release	Modification
	12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.

Usage Guidelines	The fast-cwnd-rate command allows the administrator to configure a rate at which the SCTP congestion window is decreased due to a fast retransmission on the SCTP association.



Caution

The behavior of the SCTP congestion control algorithms is not compliant with RFC 2960 or RFC 4960 when this command is changed to values other than the default. This command should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples	The following example shows how to define a profile named m2parfc. The profile supports M2PA RFC, specifies the fast-cwnd command, and applies to all the links in the linkset named to_nyc.

```
cs7 profile m2parfc
  m2pa
    fast-cwnd-rate 60
.
.
.
cs7 linkset to_nyc
  profile m2parfc
```

 fast-cwnd-rate (cs7 m2pa profile)**Related Commands**

Command	Description
m2pa	Specifies M2PA parameters in a CS7 profile.

fast-cwnd-rate (cs7 m3ua)

To configure the rate at which the SCTP congestion window size is reduced due to a fast retransmission, use the **fast-cwnd-rate** command in cs7 m3ua configuration mode. To disable the configuration, use the **no** form of this command.

fast-cwnd-rate *percent*

no fast-cwnd-rate *percent*

Syntax Description	<i>percent</i>	Rate at which the size of the SCTP congestion window is decreased due to a fast retransmission. Range is 0 to 100 percent. The default is 50 percent.

Defaults	The default rate is 50 percent.

Command Modes	cs7 m3ua configuration

Command History	Release	Modification
	12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.

Usage Guidelines	The fast-cwnd-rate command allows the administrator to configure a rate at which the SCTP congestion window is decreased due to a fast retransmission on the SCTP association.



Caution

The behavior of the SCTP congestion control algorithms is not compliant with RFC 2960 or RFC 4960 when this command is changed to values other than the default. This command should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples	The following example shows how to set the fast congestion window rate to 60 percent:

```
cs7 m3ua 2905 offload 2 0
 local-ip 4.4.4.4
 fast-cwnd-rate 60
```

Related Commands	Command	Description
	retransmit-cwnd-rate (cs7 m3ua)	Rate at which the size of the SCTP congestion window is decreased due to a fast retransmission. Range is 0 to 100 percent. The default is 50 percent.

fast-cwnd-rate (cs7 mated-sg)

To configure the rate at which the SCTP congestion window size is reduced due to a fast retransmission, use the **fast-cwnd-rate** command in cs7 mated-sg configuration mode. To disable the configuration, use the **no** form of this command.

fast-cwnd-rate *percent*

no fast-cwnd-rate *percent*

Syntax Description

<i>percent</i>	Rate at which the size of the SCTP congestion window is decreased due to a fast retransmission. Range is 0 to 100 percent. The default is 50 percent.

Defaults

The default rate is 50 percent.

Command Modes

cs7 mated-sg configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The **fast-cwnd-rate** command allows the administrator to configure a rate at which the SCTP congestion window is decreased due to a fast retransmission on the SCTP association.



Caution

The behavior of the SCTP congestion control algorithms is not compliant with RFC 2960 or RFC 4960 when this command is changed to values other than the default. This command should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples

The following example shows how to set the fast congestion window rate to 60 percent:

```
cs7 mated-sg BLUE 5000
remote-ip 5.5.5.5
fast-cwnd-rate 60
```

Related Commands

Command	Description
retransmit-cwnd-rate (cs7 mated-sg)	Rate at which the size of the SCTP congestion window is decreased due to a fast retransmission. Range is 0 to 100 percent. The default is 50 percent.

fast-cwnd-rate (cs7)

To configure the rate at which the SCTP congestion window size is reduced due to a fast retransmission, use the **fast-cwnd-rate** command in `cs7` configuration mode. To disable the configuration, use the **no** form of this command.

fast-cwnd-rate *percent*

no fast-cwnd-rate *percent*

Syntax Description	<i>percent</i>	Rate at which the size of the SCTP congestion window is decreased due to a fast retransmission. Range is 0 to 100 percent. The default is 50 percent.

Defaults	The default rate is 50 percent.

Command Modes	<code>cs7</code> configuration

Command History	Release	Modification
	12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.

Usage Guidelines	The fast-cwnd-rate command allows the administrator to configure a rate at which the SCTP congestion window is decreased due to a fast retransmission on the SCTP association.



Caution

The behavior of the SCTP congestion control algorithms is not compliant with RFC 2960 or RFC 4960 when this command is changed to values other than the default. This command should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples	The following example shows how to set the fast congestion window rate to 60 percent:

```
cs7 5000
 local-ip 4.4.4.4
 fast-cwnd-rate 60
```

Related Commands	Command	Description
	retransmit-cwnd-rate (cs7)	Rate at which the size of the SCTP congestion window is decreased due to a fast retransmission. Range is 0 to 100 percent. The default is 50 percent.

fast-cwnd-rate (cs7 sua)

To configure the rate at which the SCTP congestion window size is reduced due to a fast retransmission, use the **fast-cwnd-rate** command in cs7 sua configuration mode. To disable the configuration, use the **no** form of this command.

fast-cwnd-rate *percent*

no fast-cwnd-rate *percent*

Syntax Description	<i>percent</i>	Rate at which the size of the SCTP congestion window is decreased due to a fast retransmission. Range is 0 to 100 percent. The default is 50 percent.

Defaults	The default rate is 50 percent.

Command Modes	cs7 sua configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	The fast-cwnd-rate command allows the administrator to configure a rate at which the SCTP congestion window is decreased due to a fast retransmission on the SCTP association.



Caution

The behavior of the SCTP congestion control algorithms is not compliant with RFC 2960 or RFC 4960 when this command is changed to values other than the default. This command should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples	The following example shows how to set the fast congestion window rate to 60 percent:

```
cs7 sua 15000 offload 2 0
local-ip 4.4.4.4
fast-cwnd-rate 60
```

Related Commands	Command	Description
	retransmit-cwnd-rate (cs7 sua)	Rate at which the size of the SCTP congestion window is decreased due to a fast retransmission. Range is 0 to 100 percent. The default is 50 percent.

gt (cs7 mlr result)

To specify an outbound global title destination from within a result group, use the **gt** command in cs7 mlr result configuration mode. To delete the specification, use the **no** form of this command.

gt *addr-string* [**tt** *tt* [**gti** *gti*] [**np** *np* **nai** *nai*]] [**order** *order*] [**weight** *weight*]

no **gt** *addr-string* [**tt** *tt* [**gti** *gti*] [**np** *np* **nai** *nai*]] [**order** *order*] [**weight** *weight*]

Syntax	Description
<i>addr-string</i>	An address string of 1 to 15 hexadecimal characters. The string is not input in BCD format, but in normal form.
tt	(Optional) Identifies a translation type specified within the address.
<i>tt</i>	Integer in the range 0 to 255.
gti	(Optional) Identifies the global title indicator for the specified address. This value is specified only when the variant is ITU or China.
<i>gti</i>	Integer value of 2 or 4.
np	(Optional) Identifies the numbering plan of the specified address. Configured only when the <i>gti</i> value is 4.
<i>np</i>	Integer in the range 0 to 15.
nai	(Optional) Identifies the nature of the specified address. Configured only when the <i>gti</i> value is 4.
<i>nai</i>	Integer in the range 0 to 127.
order	Specifies the order in which the results are stored in the result group. Required for (and present only in the CLI for) results in dest-sme-binding mode. Results in a wrp result group are not able to configure an order parameter.
<i>order</i>	Integer in the range 1 to 1000.
weight	(Optional) Specifies the load-balancing weight.
<i>weight</i>	For dest-sme-binding mode, an integer value in the range 1 to 2147483647. The weight value should reflect the relative capacity of the result (SMSC). This value is used by the dynamic B-address routing algorithm to select a deterministic result (SMSC) based on the message B-address. If not configured, the default <i>weight</i> value is 1. For wrp mode, an integer value in the range 0 to 10. A value of 10 indicates the resource should be selected 10 times more than a resource assigned a weight of 1. A weight of 0 indicates that the resource should be used only when all nonzero-weighted resources are unavailable. If multiple zero-weighted resources exist, then messages are equally distributed between them if all nonzero-weighted resources fail. If not specified, a default weight of 1 is used.

Defaults

The default weight value is 1.

Command Modes

cs7 mlr result configuration

■ **gt (cs7 mlr result)****Command History**

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The **gt** result is always considered to be available and uncongested. The network global title translation function then assumes all further load-balancing, congestion, and distribution decisions for the message. This behavior is true for both wr mode and dest-sme-binding mode.

Examples

The following example shows how to configure an SMS result group named POSTPAY with several optional parameters specified:

```
cs7 mlr result POSTPAY
gt 11111111 tt 0 gti 4 np 1 nai 4 weight 1
```

Related Commands

Command	Description
cs7 mlr result-group	Configures an SMS result group.

gta app-grp

To create or modify a GTA entry that translates a GTA to a GTT application group, use the **gta app-grp** command in **cs7 gtt selector** configuration mode. To delete a GTA entry, use the **no** form of this command.

```
gta { gta | default } app-grp app-grp [pam pam-name]
```

```
no gta { gta | default }
```

Syntax Description

<i>gta</i>	Global Title Address. Valid values are hexadecimal numbers in the range of 1 to 15 characters.
default	Specifies the default translation to use if no specific GTAs match.
app-grp	Result type specifying that GTA translates to a GTT application group.
<i>app-grp</i>	Name of application group.
pam	This keyword indicates a PAM table is part of the GTA entry.
<i>pam-name</i>	Name used to specify the particular PAM table.

Defaults

None.

Command Modes

cs7 gtt selector configuration

Command History

Release	Modification
12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.
12.4(15)SW5 12.2(33)IRE	The ability to include the PAM table was introduced.

Usage Guidelines

If load sharing is required for the intermediate GTT, then the result of the GTT must use a GTT application group.

Examples

The following example shows how to translate gta 919363 to the application group named group1:

```
cs7 gtt selector selector1 tt 250 gti 2
  gta 919363 app-grp group1
```

Related Commands

Command	Description
cs7 gtt concern-pclist	Configures a GTT concerned point code list.
cs7 gtt selector	Specifies a GTT selector.

Command	Description
gta asname	Creates or modifies a GTA entry that translates to an M3UA or SUA application server name.
gta pcssn	Creates or modifies a GTA entry that translates a GTA to a point code and optional subsystem number.
show cs7 gtt gta	Displays CS7 GTT GTA entries.
show cs7 gtt map	Displays CS7 GTT MAP entries.

gta asname

To create or modify a GTA entry that translates to an M3UA or SUA application server name, use the **gta asname** command in cs7 gtt selector configuration mode. To delete a GTA entry, use the **no** form of this command.

```
gta {gta | default} asname as-name {gt | pcssn} [ntt ntt | ssn ssn | sccp-allow-pak-conv number |
pam pam-name]

no gta {gta | default}
```

Syntax Description	
<i>gta</i>	Global Title Address. Valid values are hexadecimal numbers in the range of 1 to 15 characters.
default	Specifies the default translation to use if no specific GTAs match.
asname	Result type specifying that GTA translates to an M3UA or SUA application server name.
<i>as-name</i>	Name of the M3UA or SUA application server.
gt	Sets the routing indicator (RI) to Route on Global Title.
pcssn	Sets the RI to Route on Point Code and Subsystem Number.
ntt	Specifies a new translation type.
<i>ntt</i>	New translation type, in the range 0 to 255.
ssn	Specifies a subsystem number.
<i>ssn</i>	Subsystem number, in the range 2 to 255.
sccp-allow-pak-conv	Enables conversion of SCCP packet between XUDT/XUDTS and UDT/UDTS.
<i>number</i>	1 specifies XUDT/XUDTS to UDT/UDTS conversion 2 specifies UDT/UDTS to XUDT/XUDTS conversion 3 specifies NO CONVERSION
pam	This keyword indicates a PAM table is part of the GTA entry.
<i>pam-name</i>	Name used to specify the particular PAM table.

Defaults None.

Command Modes cs7 gtt selector configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Release	Modification
12.4(15)SW5 12.2(33)IRE	The ability to include the PAM table was introduced.
12.4(15)SW9 12.2(33)IRI	The sccp-allow-pak-conv keyword was added.

Usage Guidelines

The **gta asname** command allows you to assign a global title translation to an M3UA or SUA AS, instead of to a point code and SSN. By specifying the AS name, backup systems solely reside underneath the AS specified with the **cs7 as** command.

Examples

The following example shows how to configure a GTA entry that translates to an SUA AS named GREENASP3:

```
cs7 as GREENASP3 sua
  routing-key 3 gtt
  asp ASP3
.
.
.
cs7 gtt selector E164SEL 14
  gta 1123456789001 asname GREENASP3 pcssn
```

The following example shows how to configure separate GTA asname entries that refer respectively to PAM tables named pam2 and pam3:

```
cs7 instance 1 gtt selector test1 tt 0 gti 2
  gta 123 pcssn 1.2.3 gt pam pam1
  gta 124 asname as1 gt pam pam2
  gta default asname as2 gt pam pam3
```

Related Commands

Command	Description
cs7 as	Specifies an application server and enables cs7 as submode.
cs7 gtt selector	Specifies a GTT selector.
cs7 m3ua	Specifies the local port number for M3UA and enters cs7 m3ua submode.
cs7 sua	Specifies the local port number for SUA and enters cs7 sua submode.
show cs7 gtt gta	Displays CS7 GTT GTA entries.
cs7 pam	Identifies a packet address modification (PAM) table and enters the CS7 PAM submode.
cgpa (cs7 pam)	Configures one cgpa entry in the PAM table.
cdpa (cs7 pam)	Configures one cdpa entry in the PAM table.
opc	Configures an opc entry in the PAM table.
dpc	Configures a dpc entry in the PAM table.
gta pcssn	Creates or modifies a GTA entry that translates a GTA to a point code and optional subsystem number.
modify-failure (pam)	Specifies the desired action when the PAM table packet modification fails.
cs7 gws action-set	Defines gateway screening action sets that may include a PAM table.

gta pcssn

To create or modify a GTA entry that translates a GTA to a point code and optional subsystem number, use the **gta pcssn** command in cs7 gtt selector configuration mode. To delete a GTA entry, use the **no** form of this command.

```
gta {gta | default} pcssn pc {gt | pcssn} [ntt ntt | ssn ssn | sccp-allow-pak-conv number | pam
pam-name]

no gta {gta | default}
```

Syntax Description		
<i>gta</i>		Global Title Address. Valid values are hexadecimal numbers in the range of 1 to 15 characters.
default		Specifies the default translation to use if no specific GTAs match.
pcssn		Result type specifying that GTA translates to a point code and optional subsystem number.
<i>pc</i>		Point code, in the form zone.region.sp.
gt		Sets the routing indicator (RI) to Route on Global Title
pcssn		Sets the RI to Route on Point Code and Subsystem Number.
ntt		Specifies a new translation type.
<i>ntt</i>		New translation type, in the range 0 to 255.
ssn		Specifies a subsystem number.
<i>ssn</i>		Subsystem number, in the range 2 to 255.
sccp-allow-pak-conv		Enables conversion of SCCP packet between XUDT/XUDTS and UDT/UDTS.
<i>number</i>		1 specifies XUDT/XUDTS to UDT/UDTS conversion 2 specifies UDT/UDTS to XUDT/XUDTS conversion 3 specifies NO CONVERSION
pam		This keyword indicates a PAM table is part of the GTA entry.
<i>pam-name</i>		Name used to specify the particular PAM table.

Defaults None.

Command Modes cs7 gtt selector configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Release	Modification
12.4(15)SW5 12.2(33)IRE	The ability to include the PAM table was introduced.
12.4(15)SW9 12.2(33)IRI	The sccp-allow-pak-conv keyword was added.

Usage Guidelines

You must configure at least one subsystem for the point code. Otherwise, the command fails.

Examples

The following example shows how to add GTA entry 1111 translating to point code 1.2.3 and set the routing indicator to route on the global title:

```
gta 1111 pcssn 1.2.3 gt
```

The following example shows how to modify GTA entry 1111 translating to point code 1.2.3 and set the routing indicator to route on the point code and subsystem number:

```
gta 1111 pcssn 1.2.3 pcssn
```

The following example shows how to delete GTA entry 1111:

```
no gta 1111
```

The following example shows how to configure a GTA pcssn entry that refers to a PAM table named pam2:

```
cs7 instance 1 gtt selector test1 tt 0 gti 2
gta 123 pcssn 1.2.3 gt pam pam1
gta 124 asname as1 gt pam pam2
gta default asname as2 gt pam pam3
```

Related Commands

Command	Description
cs7 gtt concern-pelist	Configures a GTT concerned point code list.
cs7 gtt selector	Specifies a GTT selector.
gta asname	Creates or modifies a GTA entry that translates to an M3UA or SUA application server name.
show cs7 gtt gta	Displays CS7 GTT GTA entries.
show cs7 gtt map	Displays CS7 GTT MAP entries.

gta-prefix

To specify a partial or a prefix match of the global title address, use the **gta-prefix** command in gws table configuration mode. To remove the specification, use the **no** form of this command.

```
gta-prefix { gta-pref [exact] | * } [min-digits min-digits] [max-digits max-digits] result { action
action-set | table table-name }
```

```
no gta-prefix { gta-pref | * }
```

Syntax Description

<i>gta-pref</i>	Partial or prefix digits of the global title addresses.
exact	Screens for the exact match.
*	Wildcard. (See the Usage Guidelines section.)
min-digits	Screens against the minimum number of digits of the global title address.
<i>min-digits</i>	Minimum number of digits.
max-digits	Screens against the maximum number of digits of the global title address.
<i>max-digits</i>	Maximum number of digits.
result	Specifies the next step.
action	Specifies that the next step is an action set.
<i>action-set</i>	Action set name. Valid names may not exceed 12 alphanumeric characters.
table	Specifies that the next step is a table.
<i>table-name</i>	Name of the next step table.

Command Default

None.

Command Modes

gws table configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The **gta-prefix** command is valid in the following table types: cgpa-gta-prefix, cdpa-gta-prefix.

The GTA prefix table is typically the next step for CgPA PC-SSN or CdPA PC-SSN screening, pre-GTT and post-GTT respectively. The table is used for partial or prefix matching of the global title address. If **min-digits** and **max-digits** are specified, every screening is verified against the minimum and maximum number of digits in the GTA. If the optional keyword **exact** is specified, the GTA is checked for the exact match. When a wildcard (*) is specified along with **min-digits** and/or **max-digits**, the GTA is checked for the minimum and/or maximum number of digits in the GTA.

Examples

In the following example, the second line screens for the partial prefix 455 and specifies the next step as the action set ALLOW. The third line screens for the partial prefix 556677 and specifies the next step as the action set BLOCK.

```
cs7 instance 2 gws table PGTA222 type cgpa-gta-prefix action allowed
gta-prefix 455 result action ALLOW
gta-prefix 556677 max-digits 10 result action BLOCK
```

Related Commands

Command	Description
cs7 gws table	Configures a gateway screening table.

gta qos-class

To set the QoS class for a global title address, use the **gta qos-class** command in cs7 gtt selector configuration mode. To remove the configuration, use the **no** form of this command.

```
gta { gta | default } qos-class qos-class { app-grp app-grp | asname as-name | pcssn pc [{ gt | pcssn }  
{ ntt ntt } | { ssn ssn } ] }
```

```
no gta { gta | default } qos-class
```

Syntax Description

<i>gta</i>	Global Title Address. Valid values are hexadecimal numbers in the range of 1 to 15 characters.
default	Specifies the default translation to use if no specific GTAs match.
<i>qos-class</i>	QoS class. Valid range is 0 to 7.
app-grp	GTA translated to a GTT application group.
<i>app-grp</i>	Name of the application group.
asname	Result type specifying that GTA translates to an M3UA or SUA application server name.
<i>as-name</i>	Name of the M3UA or SUA application server.
pcssn	GTA translated to a point code and optional subsystem number.
<i>pc</i>	Point code in the form zone.region.sp.
gt	Sets the routing indicator to “route on global title.”
ntt	Specifies a new translation type.
<i>ntt</i>	New translation type. Valid range is 0 to 255.
pcssn	Sets the routing indicator to “route on point code and subsystem number.”
ssn	Specifies a subsystem number.
<i>ssn</i>	Subsystem number. Valid range is 2 to 255.

Defaults

None.

Command Modes

cs7 gtt selector configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

If the QoS class entered for a GTA is not defined, SCCP packets for the GTA are routed over the default class peer link members.

Examples

The following example shows how to configure a QoS class 3 for the GTA 1324:

```
cs7 gtt selector c7gsp tt 3 gti 2
gta 1324 qos-class 3 pcssn 2.2.2 gt ssn 2
```

Related Commands

Command	Description
cs7 qos class	Defines a QoS class.
show cs7 qos	Displays QoS class information.

gta-start

To specify a GTA range, use the **gta-start** command in gws digit-screening table configuration mode. To remove the specification, use the **no** form of this command.

gta-start *start-gta* [**gta-end** *end-gta*] **result** {**action** *action-set* | **table** *table-name*}

no gta-start *start-gta* [**gta-end** *end-gta*]

Syntax Description		
<i>start-gta</i>		Starting GTA, in the range of 1 to 15 hexadecimal digits.
gta-end		Specifies an ending GTA.
<i>end-gta</i>		Ending GTA, in the range of 1 to 15 hexadecimal digits.
result		Specifies the next step.
action		Specifies that the next step is an action set.
<i>action-set</i>		Action set name. Valid names may not exceed 12 alphanumeric characters.
table		Specifies that the next step is a table.
<i>table-name</i>		Name of the next step table.

Defaults None.

Command Modes gws digit-screening table configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines The **gta-start** command is valid in the following table types: cdpa-gta-range, cgpa-gta-range.

Examples The following example shows how to specify a set of GTA ranges and the next step for each range:

```
cs7 instance 0 gws table GTA1 type cgpa-gta-range action allowed
gta-start 4500 gta-end 5000 result action ALLOW
gta-start 34555 result action action ALLOW
gta-start 3922000 gta-end 3924000 result action ALLOW
```

Related Commands	Command	Description
	cs7 gws table	Configures a gateway screening table.

gtt-accounting (as)

To enable GTT accounting for an xUA AS, use the **gtt-accounting** *cs7* as submode command.

To disable accounting for an xUA AS, use the **no** form of this command.

gtt-accounting

no gtt-accounting

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled.

Command Modes

cs7 as submode

Related Commands

Usage Guidelines

GTT accounting is performed after a successful GTT packet is received from the AS.

For an M3UA AS, GTT accounting is performed on a payload data message. For an SUA AS, GTT accounting is performed on a CLDT message where the routing indicator is GT.

Examples

The following example shows how to enable GTT accounting:

```
gtt-accounting
```

Related Commands

Command	Description
cs7 as	Defines an application server (AS).

gtt-accounting (linkset)

To enable GTT accounting on a linkset, use the **gtt-accounting** command in cs7 linkset configuration mode. To disable GTT accounting on a linkset, use the **no** form of this command.

gtt-accounting

no gtt-accounting

Syntax Description This command has no arguments or keywords.

Defaults This command is disabled.

Command Modes cs7 linkset configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples The following example shows how to enable GTT accounting on the linkset named to_doc:

```
cs7 linkset to_doc
gtt-accounting
```

Related Commands	Command	Description
	cs7 linkset	Specifies a linkset and enters cs7 linkset submode.
	show cs7 accounting	Displays ITP accounting details.

hold-transport (cs7 link)

To specify that the SCTP association will stay up when the link is shut down, use the **hold-transport** command in cs7 link configuration mode. To specify to take down the association when the link is shut down, use the **no** form of this command.

hold-transport

no hold-transport

Syntax Description

This command has no arguments or keywords.

Defaults

The default is to leave the link up.

Command Modes

cs7 link configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Examples

The following example shows how to specify, for link 0 in the linkset named to_nyc, that the SCTP association will stay up when the link is shut down:

```
cs7 linkset to_nyc 10.1.1
link 0 sctp 172.18.44.147 7000 7000
hold-transport
```

Related Commands

Command	Description
link (cs7 linkset)	Configures a link.

hold-transport (cs7 m2pa profile)

To specify in a CS7 M2PA profile that the SCTP association will stay up when the link is shut down, use the **hold-transport** command in cs7 m2pa profile configuration mode. To specify in the profile to take down the association when the link is shut down, use the **no** form of this command.

hold-transport

no hold-transport

Syntax Description	This command has no arguments or keywords.

Defaults	The default is to leave the link up.

Command Modes	cs7 m2pa profile configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples	The following example shows how to define a profile named m2parfc. The profile supports M2PA RFC, specifies the hold-transport command, and applies to all the links in the linkset named to_nyc.

```
cs7 profile m2parfc
 m2pa
  hold-transport
.
.
.
cs7 linkset to_nyc
 profile m2parfc
```

Related Commands	Command	Description
	m2pa	Specifies M2PA parameters in a CS7 profile.

hs-mtp2

To configure CS7 link profile parameters for high-speed MTP2, use the **hs-mtp2** cs7 profile submode command. To disable the settings, use the **no** form of this command.

hs-mtp2

no hs-mtp2

Syntax Description This command has no arguments or keywords.

Defaults This command is disabled.

Command Modes cs7 profile submode

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples The following example shows how to define a profile named TIMERS. The profile supports high-speed MTP2, configures the t1 and t2 settings, and applies to all the links in the linkset named ITP_A.

```
cs7 profile TIMERS
  hs-mtp2
    timer t1 100
    timer t2 10
  .
  .
  .
cs7 linkset ITP_A
  profile TIMERS
```

Related Commands	Command	Description
	cs7 profile	Defines a profile that you can apply to all the links in a linkset.
	timer (cs7 hs-mtp2 profile)	Specifies timers for high-speed MTP2 links.
	tx-queue-depth (cs7 hs-mtp2 profile)	Specifies the number of packets that can be queued for transmission.
	variant jt1	Configures a CS7 link profile variant.

hs-mtp2-timer (cs7 link)

To configure high-speed MTP2 encapsulation timers on a link, use the **hs-mtp2-timer** command in cs7 link configuration mode. To reset the timers, use the **no** form of this command.

hs-mtp2-timer {**t1** msec | **t2** msec | **t3** msec | **t4e** msec | **t4n** msec | **t5** msec | **t6** msec | **t7** msec | **t8** msec}

no hs-mtp2-timer {**t1** msec | **t2** msec | **t3** msec | **t4e** msec | **t4n** msec | **t5** msec | **t6** msec | **t7** msec | **t8** msec}

Syntax Description	
t1	Alignment ready timer. ANSI range: 165 to 200 seconds. Default 170 seconds. ITU range 25 to 350 seconds. Default 300 seconds.
t2	Not aligned timer. ANSI range 5 to 14 seconds. Default 11.5 seconds. ITU range 5 to 150 seconds. Default 5 seconds.
t3	Aligned timer. ANSI range 5 to 14 seconds. Default 11.5 seconds. ITU range 1 to 2 seconds. Default 1.5 seconds.
t4e	Emergency proving period timer. ANSI range: 4.5 to 5.5 seconds. Default 5 seconds. ITU range: 400 to 600 milliseconds. Default 500 milliseconds.
t4n	Normal proving period timer. ANSI range: 27 to 33 seconds. Default 30 seconds. ITU range: 3 to 70 seconds. Default 30 seconds.
t5	Sending SIB timer. ANSI range: 80 to 120 milliseconds. Default 100 milliseconds. ITU range: 80 to 120 milliseconds. Default 100 milliseconds.
t6	Remote congestion timer. ANSI range: 1 to 6 seconds. Default 1 second. ITU range 3 to 6 seconds. Default 3 seconds.
t7	Excessive delay of acknowledgment timer. ANSI range: 500 to 2000 milliseconds. Default 1000 milliseconds. ITU range: 500 to 2000 milliseconds. Default is 1000 milliseconds.
t8	Interval timer for errored interval monitor. ANSI range: 80 to 120 milliseconds. Default 100 milliseconds. ITU range: 80 to 120 milliseconds. Default 100 milliseconds.

Defaults

T1: ANSI = 170 seconds; ITU = 300 seconds

T2: ANSI = 11.5 seconds; ITU = 5 seconds

T3: ANSI = 11.5 seconds; ITU = 1.5 seconds

T4E: ANSI = 5 seconds; ITU = 500 milliseconds

T4N: ANSI = 30 seconds; ITU = 30 seconds

T5: ANSI = 100 milliseconds; ITU = 100 milliseconds

T6: ANSI = 1 second; ITU = 3 seconds

T7: ANSI = 1000 milliseconds; ITU = 1000 seconds

T8: ANSI = 100 milliseconds; ITU = 100 milliseconds

Command Modes

cs7 link configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

High-speed MTP2 parameters can also be specified in cs7 profile configuration mode.

Examples

The following example shows how to specify timers for link 0 of linkset TO_NYC:

```
cs7 linkset TO_NYC 3.3.3
 link 0 Serial4/1/0:0
   hs-mtp2-timer t1 100
   hs-mtp2-timer t2 10
```

Related Commands.

Command	Description
cs7 profile	Defines a profile of MTP2 parameters that you can apply to all the links in a linkset.
tx-queue-depth (cs7 link)	Configures the high-speed MTP2 transmit queue depth.

hsl

To configure CS7 link profile parameters for HSL (high-speed linking), use the **hsl** command in cs7 profile configuration mode. To disable the settings, use the **no** form of this command.

hsl

no hsl

Syntax Description	This command has no arguments or keywords.

Defaults	This command is disabled.

Command Modes	cs7 profile configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples	The following example shows how to define a profile named SAAL. The profile supports HSL, specifies the packet bundling interval and SSCF NNI timers, and applies to all the links in the linkset named to_nyc.

```
cs7 profile SAAL
  hsl
    bundling 10
    sscf-nni t1 10
    sscf-nni t2 150
    sscf-nni t3 100
.
.
cs7 linkset to_nyc
  profile SAAL
```

Related Commands	Command	Description
	cs7 profile	Defines a profile that you can apply to all the links in a linkset.
	variant jtl	Specifies which of the SS7 variations the CS7 profile is running.

idle-cwnd-rate (cs7 asp)

To configure the rate at which the SCTP congestion window size is reduced due to idle time, use the **idle-cwnd-rate** command in **cs7 asp** configuration mode. To disable the configuration, use the **no** form of this command.

idle-cwnd-rate *percent*

no idle-cwnd-rate *percent*

Syntax Description

<i>percent</i>	Rate at which the size of the SCTP congestion window is decreased due to an idle association. Range is 0 to 100 percent. The default is 50 percent.

Defaults

The default rate is 50 percent.

Command Modes

cs7 asp configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The **idle-cwnd-rate** command allows the administrator to configure a rate at which the SCTP congestion window is decreased due to the SCTP association being idle. The SCTP congestion window does not decrease below the initial congestion window size, regardless of the rate and the length of idle time.



Caution

The behavior of the SCTP congestion control algorithms is not compliant with RFC 2960 or RFC 4960 when this command is changed to values other than the default. This command should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples

The following example shows how to set the idle congestion window rate to 60 percent:

```
cs7 asp ASP1 2905 2905 m3ua
  remote-ip 1.1.1
  idle-cwnd-rate 60
```

Related Commands

Command	Description
init-cwnd-size (cs7 asp)	Configures the SCTP initial congestion window size.

idle-cwnd-rate (cs7 link)

To configure the rate at which the SCTP congestion window size is reduced due to idle time, use the **idle-cwnd-rate** command in cs7 link configuration mode. To disable the configuration, use the **no** form of this command.

idle-cwnd-rate *percent*

no idle-cwnd-rate *percent*

Syntax Description

<i>percent</i>	Rate at which the size of the SCTP congestion window is decreased due to an idle association. Range is 0 to 100 percent. The default is 50 percent.

Defaults

The default rate is 50 percent.

Command Modes

cs7 link configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The **idle-cwnd-rate** command allows the administrator to configure a rate at which the SCTP congestion window is decreased due to the SCTP association being idle. The SCTP congestion window does not decrease below the initial congestion window size, regardless of the rate and the length of idle time.



Caution

The behavior of the SCTP congestion control algorithms is not compliant with RFC 2960 or RFC 4960 when this command is changed to values other than the default. This command should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples

The following example shows how to set the idle congestion window rate to 60 percent:

```
cs7 linkset michael 10.1.1
 link 0 sctp 172.18.44.147 7000 7000

 idle-cwnd-rate 60
```

Related Commands

Command	Description
init-cwnd-size (cs7 link)	Configures the SCTP initial congestion window size.

idle-cwnd-rate (cs7 mated-sg)

To configure the rate at which the SCTP congestion window size is reduced due to idle time, use the **idle-cwnd-rate** command in cs7 mated-sg configuration mode. To disable the configuration, use the **no** form of this command.

idle-cwnd-rate *percent*

no idle-cwnd-rate *percent*

Syntax Description

<i>percent</i>	Rate at which the size of the SCTP congestion window is decreased due to an idle association. Range is 0 to 100 percent. The default is 50 percent.

Defaults

The default rate is 50 percent.

Command Modes

cs7 mated-sg configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The **idle-cwnd-rate** command allows the administrator to configure a rate at which the SCTP congestion window is decreased due to the SCTP association being idle. The SCTP congestion window does not decrease below the initial congestion window size, regardless of the rate and the length of idle time.



Caution

The behavior of the SCTP congestion control algorithms is not compliant with RFC 2960 or RFC 4960 when this command is changed to values other than the default. This command should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples

The following example shows how to set the idle congestion window rate to 60 percent:

```
cs7 mated-sg BLUE 5000
remote-ip 5.5.5.5
idle-cwnd-rate 60
```

Related Commands

Command	Description
init-cwnd-size (cs7 mated-sg)	Configures the SCTP initial congestion window size.

idle-cwnd-rate (cs7 m2pa profile)

To configure the rate at which the SCTP congestion window size is reduced due to idle time, use the **idle-cwnd-rate** command in cs7 m2pa profile configuration mode. To disable the configuration, use the **no** form of this command.

idle-cwnd-rate *percent*

no idle-cwnd-rate *percent*

Syntax Description

percent Rate at which the size of the SCTP congestion window is decreased due to an idle association. Range is 0 to 100 percent. The default is 50 percent.

Defaults

The default rate is 50 percent.

Command Modes

cs7 m2pa profile configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The **idle-cwnd-rate** command allows the administrator to configure a rate at which the SCTP congestion window is decreased due to the SCTP association being idle. The SCTP congestion window does not decrease below the initial congestion window size, regardless of the rate and the length of idle time.



Caution

The behavior of the SCTP congestion control algorithms is not compliant with RFC 2960 or RFC 4960 when this command is changed to values other than the default. This command should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples

The following example shows how to define a profile named m2parfc. The profile supports M2PA RFC, specifies the **idle-cwnd-rate** command, and applies to all the links in the linkset named to_nyc.

```
cs7 profile m2parfc
  m2pa
    idle-cwnd-rate 60
  .
  .
  .
cs7 linkset to_nyc
  profile m2parfc
```

 idle-cwnd-rate (cs7 m2pa profile)**Related Commands**

Command	Description
m2pa	Specifies M2PA parameters in a CS7 profile.

idle-cwnd-rate (cs7 m3ua)

To configure the rate at which the SCTP congestion window size is reduced due to idle time, use the **idle-cwnd-rate** command in cs7 m3ua configuration mode. To disable the configuration, use the **no** form of this command.

idle-cwnd-rate *percent*

no idle-cwnd-rate *percent*

Syntax Description

<i>percent</i>	Rate at which the size of the SCTP congestion window is decreased due to an idle association. Range is 0 to 100 percent. The default is 50 percent.

Defaults

The default rate is 50 percent.

Command Modes

cs7 m3ua configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The **idle-cwnd-rate** command allows the administrator to configure a rate of the offload CPU that is used in the weighted round robin distribution mechanism at which the SCTP congestion window is decreased due to the SCTP association being idle. The SCTP congestion window does not decrease below the initial congestion window size, regardless of the rate and the length of idle time.



Caution

The behavior of the SCTP congestion control algorithms is not compliant with RFC 2960 or RFC 4960 when this command is changed to values other than the default. This command should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples

The following example shows how to set the idle congestion window rate to 60 percent:

```
cs7 m3ua 2905
 local-ip 4.4.4.4
 idle-cwnd-rate 60
```

Related Commands

Command	Description
init-cwnd-size (cs7 m3ua)	Configures the SCTP initial congestion window size.

idle-cwnd-rate (cs7)

To configure the rate at which the SCTP congestion window size is reduced due to idle time, use the **idle-cwnd-rate** command in **cs7** configuration mode. To disable the configuration, use the **no** form of this command.

idle-cwnd-rate *percent*

no idle-cwnd-rate *percent*

Syntax Description

<i>percent</i>	Rate at which the size of the SCTP congestion window is decreased due to an idle association. Range is 0 to 100 percent. The default is 50 percent.

Defaults

The default rate is 50 percent.

Command Modes

cs7 configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The **idle-cwnd-rate** command allows the administrator to configure a rate at which the SCTP congestion window is decreased due to the SCTP association being idle. The SCTP congestion window does not decrease below the initial congestion window size, regardless of the rate and the length of idle time.



Caution

The behavior of the SCTP congestion control algorithms is not compliant with RFC 2960 or RFC 4960 when this command is changed to values other than the default. This command should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples

The following example shows how to set the idle congestion window rate to 60 percent:

```
cs7 5000
 local-ip 4.4.4.4
 idle-cwnd-rate 60
```

Related Commands

Command	Description
init-cwnd-size (cs7)	Configures the SCTP initial congestion window size.

idle-cwnd-rate (cs7 sua)

To configure the rate at which the SCTP congestion window size is reduced due to idle time, use the **idle-cwnd-rate** command in cs7 sua configuration mode. To disable the configuration, use the **no** form of this command.

idle-cwnd-rate *percent*

no idle-cwnd-rate *percent*

Syntax Description	<i>percent</i>	Rate at which the size of the SCTP congestion window is decreased due to an idle association. Range is 0 to 100 percent. The default is 50 percent.

Defaults	The default rate is 50 percent.

Command Modes	cs7 sua configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	The idle-cwnd-rate command allows the administrator to configure a rate at which the SCTP congestion window is decreased due to the SCTP association being idle. The SCTP congestion window does not decrease below the initial congestion window size, regardless of the rate and the length of idle time.



Caution

The behavior of the SCTP congestion control algorithms is not compliant with RFC 2960 or RFC 4960 when this command is changed to values other than the default. This command should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples	The following example shows how to set the idle congestion window rate to 60 percent:

```
cs7 sua 15000 offload 2 0
local-ip 4.4.4.4
idle-cwnd-rate 60
```

Related Commands	Command	Description
	init-cwnd-size (cs7 sua)	Configures the SCTP initial congestion window size.

inbound (config-gws-as)

To configure screening of inbound messages, use the **inbound** command in gws as configuration mode. To remove the configuration, use the **no** form of this command.

inbound [**logging type** { **allow** | **block** | **rate-limit** | **both** } { **silent** | **file** [**verbose**] | **console** [**verbose**] | **file** [**verbose**] **console** [**verbose**]}] **result** { **action** *action-set-name* | **table** *table-name* }

no inbound

Syntax Description

logging	(Optional) Enables logging.
type	Specifies the logging type.
allow	Messages allowed for further processing.
block	Messages blocked.
both	Allowed and blocked messages.
rate-limit	Logs the number of MSUs discarded due to a configured rate limit.
silent	Messages are screened without logging.
file	Log is copied to a file.
verbose	(Optional) The packet (up to 40 bytes) is printed to the file and/or displayed on the console.
console	Log is displayed on the console.
result	Specifies the next step.
action	Specifies that the next step is an action set.
<i>action-set-name</i>	Action set name. Valid names may not exceed 12 alphanumeric characters.
table	Specifies that the next step is a table.
<i>table-name</i>	Name of the next step table.

Defaults

The default screening is silent.

Command Modes

gws as configuration

Command History

Release	Modification
12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.
12.4(15)SW6 12.2(33)IRF	The rate-limit keyword was added.

Examples

The following example shows how to configure inbound and outbound default screening for all ASes:

```
cs7 instance 0 gws as default
```

```
inbound logging type block file console verbose result table SIO0
outbound result action BLOCK
```

Related Commands

Command	Description
show cs7 gws as	Displays ITP gateway screening information for the AS.

inbound (config-gws-ls)

To configure screening of inbound messages, use the **inbound** command in gws linkset configuration mode. To remove the configuration, use the **no** form of this command.

inbound [**logging type** { **allow** | **block** | **rate-limit** | **both** } { **silent** | **file** [**verbose**] | **console** [**verbose**] | **file** [**verbose**] **console** [**verbose**]}] **result** { **action** *action-set-name* | **table** *table-name* }

no inbound

Syntax Description

logging	(Optional) Enables logging.
type	Specifies the logging type.
allow	Messages allowed for further processing.
block	Messages blocked.
rate-limit	Logs the number of MSUs discarded due to a configured rate limit.
both	Allowed and blocked messages.
silent	Messages are screened without logging.
file	Log is copied to a file.
verbose	(Optional) The packet (up to 40 bytes) is printed to the file and/or displayed on the console.
console	Log is displayed on the console.
result	Specifies the next step.
action	Specifies that the next step is an action set.
<i>action-set-name</i>	Action set name. Valid names may not exceed 12 alphanumeric characters.
table	Specifies that the next step is a table.
<i>table-name</i>	Name of the next step table.

Defaults

The default screening is silent.

Command Modes

gws linkset configuration

Command History

Release	Modification
12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.
12.4(15)SW6 12.2(33)IRF	The rate-limit keyword was added.

Examples

The following example shows how to configure inbound and outbound screening for all linksets:

```
cs7 instance 0 gws linkset name to_morehead1
```

```
inbound result table OPCTTC1
outbound result action ALLOW
```

Related Commands

Command	Description
show cs7 gws linkset	Displays ITP gateway screening information for the linkset.

init-cwnd-size (cs7 asp)

To configure the SCTP initial congestion window size, use the **init-cwnd-size** command in cs7 asp configuration mode. To disable the configuration, use the **no** form of this command.

init-cwnd-size *window-size*

no init-cwnd-size *window-size*

Syntax Description

<i>window-size</i>	Size in bytes of the SCTP initial congestion window size. Range is 3000 to 20971520 bytes. The default is two times the smallest MTU of the SCTP interfaces (in bytes).

Defaults

The default window size is two times the smallest MTU of the SCTP interfaces (in bytes).

Command Modes

cs7 asp configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The **init-cwnd-size** command allows the administrator to configure an initial congestion window size for an SCTP association.

If this command is provisioned, the window size specified must match the receive window size of the remote end of the SCTP association. If the initial window size does not match the receive window size, congestion control behavior will be unpredictable.



Caution

The behavior of the SCTP congestion control algorithms is not compliant with RFC 2960 or RFC 4960 when this command is changed to values other than the default. This command should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples

The following example shows how to set the initial congestion window size to 5000 bytes:

```
cs7 asp ASP1 2905 2905 m3ua
  remote-ip 1.1.1
  init-cwnd-size 5000
```

Related Commands

Command	Description
receive-window (cs7 local peer)	Configures the local receive window size.

init-cwnd-size (cs7 link)

To configure the SCTP initial congestion window size, use the **init-cwnd-size** command in cs7 link configuration mode. To disable the configuration, use the **no** form of this command.

init-cwnd-size *window-size*

no init-cwnd-size *window-size*

Syntax Description

<i>window-size</i>	Size in bytes of the SCTP initial congestion window size. Range is 3000 to 20971520 bytes. The default is two times the smallest MTU of the SCTP interfaces (in bytes).

Defaults

The default window size is two times the smallest MTU of the SCTP interfaces (in bytes).

Command Modes

cs7 link configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The **init-cwnd-size** command allows the administrator to configure an initial congestion window size for an SCTP association.



Caution

The behavior of the SCTP congestion control algorithms is not compliant with RFC 2960 or RFC 4960 when this command is changed to values other than the default. This command should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples

The following example shows how to set the initial congestion window size to 5000 bytes:

```
cs7 linkset michael 10.1.1
 link 0 sctp 172.18.44.147 7000 7000
  init-cwnd-size 5000
```

Related Commands

Command	Description
receive-window (cs7 local peer)	Configures the local receive window size.

init-cwnd-size (cs7 m2pa profile)

To configure the SCTP initial congestion window size, use the **init-cwnd-size** command in cs7 m2pa profile configuration mode. To disable the configuration, use the **no** form of this command.

init-cwnd-size *window-size*

no init-cwnd-size *window-size*

Syntax Description

<i>window-size</i>	Size in bytes of the SCTP initial congestion window size. Range is 3000 to 20971520 bytes. The default is two times the smallest MTU of the SCTP interfaces (in bytes).

Defaults

The default window size is two times the smallest MTU of the SCTP interfaces (in bytes).

Command Modes

cs7 m2pa profile configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The **init-cwnd-size** command allows the administrator to configure an initial congestion window size for an SCTP association.



Caution

The behavior of the SCTP congestion control algorithms is not compliant with RFC 2960 or RFC 4960 when this command is changed to values other than the default. This command should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples

The following example shows how to define a profile named m2parfc. The profile supports M2PA RFC, specifies the **init-cwnd-size** command, and applies to all the links in the linkset named to_nyc.

```
cs7 profile m2parfc
 m2pa
  init-cwnd-size 5000
.
.
.
cs7 linkset to_nyc
 profile m2parfc
```

Related Commands

Command	Description
m2pa	Specifies M2PA parameters in a CS7 profile.

init-cwnd-size (cs7 m3ua)

To configure the SCTP initial congestion window size, use the **init-cwnd-size** command in cs7 m3ua configuration mode. To disable the configuration, use the **no** form of this command.

init-cwnd-size *window-size*

no init-cwnd-size *window-size*

Syntax Description

<i>window-size</i>	Size in bytes of the SCTP initial congestion window size. Range is 3000 to 20971520 bytes. The default is two times the smallest MTU of the SCTP interfaces (in bytes).

Defaults

The default window size is two times the smallest MTU of the SCTP interfaces (in bytes).

Command Modes

cs7 m3ua configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The **init-cwnd-size** command allows the administrator to configure an initial congestion window size for an SCTP association.



Caution

The behavior of the SCTP congestion control algorithms is not compliant with RFC 2960 or RFC 4960 when this command is changed to values other than the default. This command should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples

The following example shows how to set the initial congestion window size to 5000 bytes:

```
cs7 m3ua 2905 offload 2 0
 local-ip 4.4.4.4
  init-cwnd-size 5000
```

Related Commands

Command	Description
receive-window (cs7 m3ua)	Configures the local receive window size.

init-cwnd-size (cs7 mated-sg)

To configure the Sctp initial congestion window size, use the **init-cwnd-size** command in cs7 mated-sg configuration mode. To disable the configuration, use the **no** form of this command.

init-cwnd-size *window-size*

no init-cwnd-size *window-size*

Syntax Description

<i>window-size</i>	Size in bytes of the Sctp initial congestion window size. Range is 3000 to 20971520 bytes. The default is two times the smallest MTU of the Sctp interfaces (in bytes).

Defaults

The default window size is two times the smallest MTU of the Sctp interfaces (in bytes).

Command Modes

cs7 mated-sg configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The **init-cwnd-size** command allows the administrator to configure an initial congestion window size for an Sctp association.



Caution

The behavior of the Sctp congestion control algorithms is not compliant with RFC 2960 or RFC 4960 when this command is changed to values other than the default. This command should not be changed without a thorough understanding of Sctp congestion control algorithms.

Examples

The following example shows how to set the initial congestion window size to 5000 bytes:

```
cs7 mated-sg BLUE 5000
remote-ip 5.5.5.5
init-cwnd-size 5000
```

Related Commands

Command	Description
receive-window (cs7 local peer)	Configures the local receive window size.

init-cwnd-size (cs7)

To configure the SCTP initial congestion window size, use the **init-cwnd-size** command in cs7 configuration mode. To disable the configuration, use the **no** form of this command.

init-cwnd-size *window-size*

no init-cwnd-size *window-size*

Syntax Description

<i>window-size</i>	Size in bytes of the SCTP initial congestion window size. Range is 3000 to 20971520 bytes. The default is two times the smallest MTU of the SCTP interfaces (in bytes).

Defaults

The default window size is two times the smallest MTU of the SCTP interfaces (in bytes).

Command Modes

cs7 configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The **init-cwnd-size** command allows the administrator to configure an initial congestion window size for an SCTP association.



Caution

The behavior of the SCTP congestion control algorithms is not compliant with RFC 2960 or RFC 4960 when this command is changed to values other than the default. This command should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples

The following example shows how to set the initial congestion window size to 5000 bytes:

```
cs7 5000
 local-ip 4.4.4.4
 init-cwnd-size 5000
```

Related Commands

Command	Description
receive-window (cs7)	Configures the local receive window size.

init-cwnd-size (cs7 sua)

To configure the Sctp initial congestion window size, use the **init-cwnd-size** command in cs7 sua configuration mode. To disable the configuration, use the **no** form of this command.

init-cwnd-size *window-size*

no init-cwnd-size *window-size*

Syntax Description

<i>window-size</i>	Size in bytes of the Sctp initial congestion window size. Range is 3000 to 20971520 bytes. The default is two times the smallest MTU of the Sctp interfaces (in bytes).

Defaults

The default window size is two times the smallest MTU of the Sctp interfaces (in bytes).

Command Modes

cs7 sua configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The **init-cwnd-size** command allows the administrator to configure an initial congestion window size for an Sctp association.



Caution

The behavior of the Sctp congestion control algorithms is not compliant with RFC 2960 or RFC 4960 when this command is changed to values other than the default. This command should not be changed without a thorough understanding of Sctp congestion control algorithms.

Examples

The following example shows how to set the initial congestion window size to 5000 bytes:

```
cs7 sua 15000
 local-ip 4.4.4.4
  init-cwnd-size 5000
```

Related Commands

Command	Description
receive-window (cs7 sua)	Configures the local receive window size.

init-ip-dscp

To set the differentiated services code point (DSCP) bits in the IP header ToS byte for the peer link initialization packets, use the **init-ip-dscp** command in cs7 local-peer configuration mode. To set the DSCP setting to the default of zero, use the **no** form of this command.

init-ip-dscp *dscp*

no init-ip-dscp

Syntax Description	<i>dscp</i> IP DSCP setting, in decimal notation. Valid range is 0 to 63, or you can use one of the following keywords: ef, af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1, cs2, cs3, cs4, cs5, or cs7.	
Defaults	The IP ToS default is 0.	
Command Modes	cs7 local-peer configuration	
Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	
Examples	The following example shows how to set the IP type of service to DSCP 56 for the peer link initialization packets: cs7 local-peer 4096 init-ip-dscp 56	
Related Commands	Command	Description
	cs7 local-peer	Specifies the local peer.
	init-ip-precedence	Specifies the IP precedence bits in the IP header type of service (ToS) byte for the peer link initialization packets.

init-ip-precedence

To set the IP precedence bits in the IP header type of service (ToS) byte for the peer link initialization packets, use the **init-ip-precedence** command in cs7 local-peer configuration mode. To disable the configuration, use the **no** form of this command.

init-ip-precedence *ip-tos*

no init-ip-precedence *ip-tos*

Syntax Description

keyword

ip-tos IP precedence setting, in decimal notation. Range is 0 to 7. The default is 0.

Defaults

The IP ToS default is 0.

Command Modes

cs7 local-peer configuration

Command History

Release

Modification

12.2(18)IXA

This command was introduced.

12.4(11)SW

12.2(33)IRA

Examples

The following example shows how to set the IP type of service to 5 for peer link initialization packets:

```
cs7 local-peer 4096
  init-ip-precedence 5
```

Related Commands

Command

Description

[cs7 local-peer](#)

Specifies the local peer.

[init-ip-dscp](#)

Specifies the differentiated services code point (DSCP) bits in the IP header ToS byte for the peer link initialization packets

init-retransmit (cs7 link)

To configure the number of retransmissions for peer initialization messages, use the **init-retransmit** command in cs7 link configuration mode. To disable the configuration, use the **no** form of this command.

init-retransmit *max-retries*

no init-retransmit *max-retries*

Syntax Description	<i>max-retries</i> Maximum number of initialization packet retries. The range is 2 to 20. The default is 8 retries.	
Defaults	8 retries	
Command Modes	cs7 link configuration	
Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	
Examples	The following example shows how to set the number of retransmissions for peer initialization messages to 10: cs7 linkset michael 10.1.1 link 0 sctp 172.18.44.147 7000 7000 init-retransmit 10	
Related Commands	Command	Description
	cs7 linkset	Specifies a linkset and enters cs7 linkset submode.
	link (cs7 linkset)	Specifies a link and enters cs7 link submode.
	show cs7 m2pa	Displays M2PA statistics.

init-retransmit (cs7 m2pa profile)

To configure the number of retransmissions for peer initialization messages, use the **init-retransmit** command in cs7 m2pa profile configuration mode. To disable the configuration, use the **no** form of this command.

init-retransmit *max-retries*

no init-retransmit *max-retries*

Syntax Description	<i>max-retries</i>	Maximum number of initialization packet retries. The range is 2 to 20. The default is 8 retries.

Defaults	8 retries

Command Modes	cs7 m2pa profile configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples The following example shows how to define a profile named m2parfc. The profile supports M2PA RFC, specifies the **init-retransmit** command, and applies to all the links in the linkset named to_nyc.

```
cs7 profile m2parfc
  m2pa
    init-retransmit 10
  .
  .
  .
cs7 linkset to_nyc
  profile m2parfc
```

Related Commands	Command	Description
	m2pa	Specifies M2PA parameters in a CS7 profile.

init-retransmit (cs7 m3ua)

To configure the number of retransmissions for peer initialization packets for this local port, use the **init-retransmit** command in cs7 m3ua configuration mode. To disable the configuration, use the **no** form of this command.

init-retransmit *max-retries*

no init-retransmit *max-retries*

Syntax Description	<i>max-retries</i> Maximum number of initialization packet retries. The range is 2 to 20. The default is 8 retries.							
Defaults	8 retries							
Command Modes	cs7 m3ua configuration							
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>12.2(18)IXA</td><td rowspan="3">This command was introduced.</td></tr><tr><td>12.4(11)SW</td></tr><tr><td>12.2(33)IRA</td></tr></table>		Release	Modification	12.2(18)IXA	This command was introduced.	12.4(11)SW	12.2(33)IRA
Release	Modification							
12.2(18)IXA	This command was introduced.							
12.4(11)SW								
12.2(33)IRA								
Examples	The following example shows how to set the number of retransmissions for peer initialization messages to 10: <pre>cs7 m3ua 2905 local-ip 4.4.4.4 init-retransmit 10</pre>							
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>cs7 m3ua</td><td>Specifies the local port number for M3UA and enters cs7 m3ua submode.</td></tr><tr><td>show cs7 m3ua</td><td>Displays M3UA statistics.</td></tr></table>		Command	Description	cs7 m3ua	Specifies the local port number for M3UA and enters cs7 m3ua submode.	show cs7 m3ua	Displays M3UA statistics.
Command	Description							
cs7 m3ua	Specifies the local port number for M3UA and enters cs7 m3ua submode.							
show cs7 m3ua	Displays M3UA statistics.							

init-retransmit (cs7)

To configure the number of retransmissions for peer initialization packets for this local port, use the **init-retransmit** command in **cs7** configuration mode. To disable the configuration, use the **no** form of this command.

init-retransmit *max-retries*

no init-retransmit *max-retries*

Syntax Description	<i>max-retries</i> Maximum number of initialization packet retries. The range is 2 to 20. The default is 8 retries.	
Defaults	8 retries	
Command Modes	cs7 configuration	
Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	
Examples	The following example shows how to set the number of retransmissions for peer initialization messages to 10: cs7 5000 init-retransmit 10	
Related Commands	Command	Description
	cs7 sgmp	Specifies the local port number for and enters cs7 submode.
	show cs7	Displays statistics.

init-retransmit (cs7 sua)

To configure the number of retransmissions for peer initialization packets for this local port, use the **init-retransmit** *cs7 sua* submode command. To disable the configuration, use the **no** form of this command.

init-retransmit *max-retries*

no init-retransmit *max-retries*

Syntax Description	<i>max-retries</i> Maximum number of initialization packet retries. The range is 2 to 20. The default is 8 retries.	
Defaults	8 retries	
Command Modes	cs7 sua submode	
Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	
Examples	The following example shows how to set the number of retransmissions for peer initialization messages to 10: cs7 sua 15000 local-ip 4.4.4.4 init-retransmit 10	
Related Commands	Command	Description
	cs7 sua	Specifies the local port number for SUA and enters cs7 sua submode.
	show cs7 sua	Displays SUA statistics.

init-timeout (cs7 link)

To configure the timeout value for retransmission of association setup messages, use the **init-timeout** cs7 link submode command. To disable the configuration, use the **no** form of this command.

init-timeout *msec*

no init-timeout *msec*

Syntax Description	<i>msec</i>	Timeout value in milliseconds. Range is 1000 to 60000 milliseconds. The default is 1000 milliseconds.

Defaults	1000 milliseconds

Command Modes	cs7 link submode

Command History	Release	Modification
	12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.

Examples The following example shows how to set the timeout value for retransmission of association setup messages to 2000 milliseconds:

```
cs7 linkset michael 10.1.1
link 0 sctp 172.18.44.147 7000 7000
init-timeout 2000
```

Related Commands	Command	Description
	cs7 linkset	Specifies a linkset and enters cs7 linkset submode.
	link (cs7 linkset)	Specifies a link and enters cs7 link submode.
	show cs7 m2pa	Displays M2PA statistics.

init-timeout (cs7 m2pa profile)

To configure the timeout value for retransmission of association setup messages, use the **init-timeout** cs7 m2pa profile submode command. To disable the configuration, use the **no** form of this command.

init-timeout *msec*

no init-timeout *msec*

Syntax Description	<i>msec</i> Timeout value in milliseconds. Range is 1000 to 60000 milliseconds. The default is 1000 milliseconds.	
Defaults	1000 milliseconds	
Command Modes	cs7 m2pa profile submode	
Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	
Examples	The following example shows how to define a profile named m2parfc. The profile supports M2PA RFC, specifies the init-timeout command, and applies to all the links in the linkset named to_nyc. <pre>cs7 profile m2parfc m2pa init-timeout 2000 . . . cs7 linkset to_nyc profile m2parfc</pre>	
Related Commands	Command	Description
	m2pa	Specifies M2PA parameters in a cs7 profile.

init-timeout (cs7 m3ua)

To configure the maximum interval for the init packet retransmission timeout value, use the **init-timeout** cs7 m3ua submode command. To disable the configuration, use the **no** form of this command.

init-timeout *msec*

no init-timeout *msec*

Syntax Description	<i>msec</i> Timeout value in milliseconds. Range is 1000 to 60000 milliseconds. The default is 1000 milliseconds.	
Defaults	1000 milliseconds	
Command Modes	cs7 m3ua submode	
Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	
Examples	The following example shows how to set the timeout value for retransmission of association setup messages to 2000 milliseconds: cs7 m3ua 2905 local-ip 4.4.4.4 init-timeout 2000	
Related Commands	Command	Description
	cs7 m3ua	Specifies the local port number for M3UA and enters m3ua submode.
	show cs7 m3ua	Displays M2PA statistics.

init-timeout (cs7)

To configure the maximum interval for the init packet retransmission timeout value, use the **init-timeout** *cs7* submode command. To disable the configuration, use the **no** form of this command.

init-timeout *msec*

no init-timeout *msec*

Syntax Description	<i>msec</i>	Timeout value in milliseconds. Range is 1000 to 60000 milliseconds. The default is 1000 milliseconds.

Defaults	1000 milliseconds

Command Modes	<i>cs7</i> submode

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples The following example shows how to set the timeout value for retransmission of association setup messages to 2000 milliseconds:

```
cs7 5000
  init-timeout 2000
```

Related Commands	Command	Description
	cs7 sgmp	Specifies the local port number for and enters <i>cs7</i> submode.
	show cs7 sgmp	Displays statistics.

init-timeout (cs7 sua)

To configure the maximum interval for the init packet retransmission timeout value, use the **init-timeout** cs7 sua submode command. To disable the configuration, use the **no** form of this command.

init-timeout *msec*

no init-timeout *msec*

Syntax Description	<i>msec</i>	Timeout value in milliseconds. Range is 1000 to 60000 milliseconds. The default is 1000 milliseconds.

Defaults	1000 milliseconds

Command Modes	cs7 sua submode

Command History	Release	Modification
	12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.

Examples The following example shows how to set the timeout value for retransmission of association setup messages to 2000 milliseconds:

```
cs7 sua 15000
local-ip 4.4.4.4
init-timeout 2000
```

Related Commands	Command	Description
	cs7 sua	Specifies the local port number for SUA and enters cs7 sua submode.
	show cs7 sua	Displays SUA statistics.

insert-dpc-in-cdpa

To enable a global multilayer routing (MLR) option to insert a destination point code (dpc) into the called party (cdpa) point code (pc) for packets that are routed with MLR, use the **insert-dpc-in-cdpa** command in cs7 options configuration mode. To remove the specification, use the **no** form of this command.

insert-dpc-in-cdpa

no insert-dpc-in-cdpa

Syntax Description This command has no arguments or keywords.

Defaults None.

Command Modes cs7 options configuration

Command History	Release	Modification
	12.2(18)IXB	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines The **insert-dpc-in-cdpa** command is a cdpa modification enhancement. When this option is configured and a packet is routed with MLR, the MTP dpc is inserted into the cdPa pc if the cdPa pc is null. This MLR option is configured globally per instance, so that it can be applied to all MLR-routed results, including trigger results, rule results, and address-table results. The cdpa pc is updated for MLR results of pc, point code and subsystem number (pcssn), global title (gt), and asname. This option does not apply to the MLR results **block** or **continue**.

MLR can modify the cdPa pc and the calling party (cgpa) pc of an MSU. MLR verifies that the modified MSU fits in 273 bytes. A “Failed to insert data into MSU” statistic is displayed in the MLR global statistics if the MSU is not modified. In the failed cases, the packet is still routed with MLR but without the updated Signaling Connection Control party (SCCP) addresses.

Preserving the original dpc in the cdpa is not possible with an MLR GT result. The SCCP always overwrites the cdpa pc with the new GT translated dpc.

Examples The following example shows how to enable global options and specifies that, when a packet is routed with MLR, the MTP dpc is inserted into the cdpa pc if the cdpa is null:

```
cs7 instance 0 mlr options
  insert-dpc-in-cdpa
```

Related Commands

Command	Description
cs7 mlr options	Specifies global MLR options.

ip-dscp (cs7 m2pa profile)

To set the differentiated services code point (DSCP) bits in the IP header ToS byte, use the **ip-dscp** cs7 m2pa profile submode command. To set the DSCP setting to the default of zero, use the **no** form of this command.

ip-dscp *ip-tos*

no ip-dscp

Syntax Description	<i>ip-tos</i>	IP DSCP setting, in decimal notation. Range is 5000 to 63. The default is 0.

Defaults	The IP ToS default is 0.

Command Modes	cs7 m2pa profile submode

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	The IP DSCP configured on the peer link overrides any IP ToS setting assigned to the peer link using a QoS class.

Examples	The following example shows how to define a profile named m2parfc. The profile supports M2PA RFC, specifies the ip-dscp command, and applies to all the links in the linkset named to_nyc.

```
cs7 profile m2parfc
  m2pa
    ip-dscp 56
  .
  .
  .
cs7 linkset to_nyc
  profile m2parfc
```

Related Commands	Command	Description
	m2pa	Specifies M2PA parameters in a CS7 profile.

ip-precedence (cs7 link)

To set the IP precedence bits in the IP header type of service (ToS) byte, use the **ip-precedence** cs7 link submode command. To disable the configuration, use the **no** form of this command.

ip-precedence *ip-tos*

no ip-precedence *ip-tos*

Syntax Description	<i>ip-tos</i>	IP precedence setting, in decimal notation. Range is 0 to 7. The default is zero.

Defaults	The IP precedence default is 0.

Command Modes	cs7 link submode

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	The IP precedence configured on the peer link overrides any ToS setting assigned to the peer link using a QoS class.

Examples	The following example shows how to set the IP type of service to 5:

```
cs7 linkset michael 10.1.1
link 0 sctp 172.18.44.147 7000 7000
ip-prec 5
```

Related Commands	Command	Description
	cs7 linkset	Specifies a linkset.
	ip-dscp (cs7 m2pa profile)	Specifies a differentiated services code point.
	link (cs7 linkset)	Configures a link.

ip-precedence (cs7 m2pa profile)

To set the IP precedence bits in the IP header type of service (ToS) byte, use the **ip-precedence** cs7 m2pa profile submode command. To disable the configuration, use the **no** form of this command.

ip-precedence *ip-tos*

no ip-precedence *ip-tos*

Syntax Description	<i>ip-tos</i>	IP precedence setting, in decimal notation. Range is 0 to 7. The default is 0.

Defaults	The IP precedence default is 0.

Command Modes	cs7 m2pa profile submode

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	The IP precedence configured on the peer link overrides any ToS setting assigned to the peer link using a QoS class.

Examples	The following example shows how to define a profile named m2parfc. The profile supports M2PA RFC, specifies the ip-precedence command, and applies to all the links in the linkset named to_nyc.

```
cs7 profile m2parfc
  m2pa
    ip-prec 5
  .
  .
  .
cs7 linkset to_nyc
  profile m2parfc
```

Related Commands	Command	Description
	m2pa	Specifies M2PA parameters in a CS7 profile.

isup-msg-type

To specify an ISUP message type, use the **isup-msg-type** command in cs7 gws isup message table configuration mode. To remove the specification, use the **no** form of this command.

isup-msg-type *isup-msg-type* **result** {**action** *action-set-name* | **table** *table-name*}

no isup-msg-type *isup-msg-type*

Syntax Description

<i>isup-msg-type</i>	ISUP message types are listed in Table 28 in the Usage Guidelines.
result	Specifies the next step.
action	Action set name.
<i>action-set</i>	Name of the action set in the next step. Valid names may not exceed 12 alphanumeric characters.
table	Specifies that the next step is a table.
<i>table-name</i>	Name of the table in the next step.

Defaults

None.

Command Modes

cs7 gws isup message table configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

[Table 32](#) lists the ISUP message types.

Table 32 *ISUP Message Types*

ACM	ANM	APM (ITU only)	BLA
BLO	CCR	CFN	CGB
CGBA	CGU	CGUA	CRG
CON	COT	CPG	CQM
CQR	CVR (ANSI only)	CVT (ANSI only)	EXM (ANSI only)
FAC	FAA (ITU only)	FRJ (ITU only)	FAR (ITU only)
FOT	IDR (ITU only)	IRS (ITU only)	INF
INR	GRA	GRS	IAM
LPA	LOP (ITU only)	NRM (ITU only)	OLM (ITU only)
PAM	PRI (ITU only)	REL	RES

Table 32 *ISUP Message Types (continued)*

RLC	RSC	SUS	SGM (ITU only)
SAM (ITU only)	SDN (ITU only)	UBA	UBL
UCIC	UPA (ITU only)	UPT (ITU only)	USR

Examples

The following example shows how to specify three ISUP message types and the next step for each type:

```
cs7 instance 0 gws table ISUP0 type isup-msg-type action allow
default result action ALLOW
isup-msg-type SAM result action ALLOW
isup-msg-type ANM result action ALLOW
isup-msg-type REL result action ALLOW
```

Related Commands

Command	Description
cs7 gws table	Configures a gateway screening table.

keepalive (cs7 asp)

To specify if a keepalive timer is supported, and to specify the keepalive interval for the association, use the **keepalive** cs7 asp submode command. To disable the keepalive, use the **no** form of this command.

keepalive *msec*

no keepalive *msec*

Syntax Description

<i>msec</i>	Keepalive interval, in milliseconds. The range is 300 to 30000 milliseconds. The default is the value specified under the local instance.

Defaults

Keepalive is enabled.

The keepalive interval defaults to the value specified under the local instance.

Command Modes

cs7 asp submode

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Examples

The following example shows how to set the keepalive value to 1000 milliseconds:

```
cs7 asp ASP1 2904 2905 m3ua
  remote-ip 1.1.1.1
  keepalive 1000
```

Related Commands

Command	Description
cs7 asp	Specifies an application server process (ASP) and enables cs7 asp submode.
show cs7 asp	Displays ASP statistics.

keepalive (cs7 link)

To enable a peer link keepalive interval, use the **keepalive** cs7 link submode command. To disable the keepalive interval, use the **no** form of this command.

keepalive *msec*

no keepalive *msec*

Syntax Description	<i>msec</i>	Keepalive interval, in milliseconds. The range is 300 to 30000 milliseconds. The default interval is 30000 milliseconds.

Defaults	Keepalive is enabled. The default keepalive interval is 30000 milliseconds.

Command Modes	cs7 link submode

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples	The following example shows how to set the keepalive value to 1000 milliseconds:

```
cs7 linkset michael 10.1.1
 link 0 sctp 172.18.44.147 7000 7000
  keepalive 1000
```

Related Commands	Command	Description
	cs7 linkset	Specifies a linkset and enters cs7 linkset submode.
	link (cs7 linkset)	Specifies a link and enters cs7 link submode.
	show cs7 m2pa	Displays M2PA statistics.

keepalive (cs7 m2pa profile)

To enable a peer link keepalive interval, use the **keepalive** cs7 m2pa profile configuration command. To disable the keepalive interval, use the **no** form of this command.

keepalive *msec*

no keepalive *msec*

Syntax Description	<i>msec</i>	Keepalive interval, in milliseconds. The range is 300 to 30000 milliseconds. The default interval is 30000 milliseconds.

Defaults	Keepalive is enabled. The default keepalive interval is 30000 milliseconds.

Command Modes	cs7 m2pa profile configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples	The following example shows how to define a profile named m2parfc. The profile supports M2PA RFC, specifies the keepalive command, and applies to all the links in the linkset named to_nyc.

```
cs7 profile m2parfc
  m2pa
    keepalive 1000
.
.
.
cs7 linkset to_nyc
  profile m2parfc
```

Related Commands	Command	Description
	m2pa	Specifies M2PA parameters in a CS7 profile.

keepalive (cs7 m3ua)

To specify a keepalive interval to be used when a new SCTP association is started with the local port, use the **keepalive** cs7 m3ua submode command. To disable the keepalive interval, use the **no** form of this command.

keepalive *msec*

no keepalive *msec*

Syntax Description

<i>msec</i>	Keepalive interval, in milliseconds. The range is 300 to 30000 milliseconds. The default interval is 30000 milliseconds.

Defaults

Keepalive is enabled.

The default keepalive interval is 30000 milliseconds.

Command Modes

cs7 m3ua submode

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Examples

The following example shows how to set the keepalive value to 1000 milliseconds:

```
cs7 m3ua 2905
 local-ip 4.4.4.4
 keepalive 1000
```

Related Commands

Command	Description
cs7 m3ua	Specifies the local port number for M3UA and enters cs7 m3ua submode.
show cs7 m3ua	Displays M3UA statistics.

keepalive (cs7 mated-sg)

To enable a keepalive interval for the association, use the **keepalive** cs7 mated-sg submode command. To disable the keepalive interval, use the **no** form of this command.

keepalive *msec*

no keepalive *msec*

Syntax Description	<i>msec</i>	Keepalive interval, in milliseconds. The range is 300 to 30000 milliseconds. The default interval is 30000 milliseconds.

Defaults	Keepalive is enabled. The keepalive interval defaults to the value specified under the local port instance.

Command Modes	cs7 mated-sg submode

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples	The following example shows how to set the keepalive value to 1000 milliseconds: <pre>cs7 mated-sg BLUE 2905 remote-ip 5.5.5.5 keepalive 1000</pre>

Related Commands	Command	Description
	cs7 mated-sg	Configures a connection to a mated SG and enters cs7 mated-sg submode.
	show cs7 mated-sg	Displays mated-SG statistics.

keepalive (cs7)

To specify a keepalive interval to be used when a new SCTP association is started with the local port, use the **keepalive** *cs7* submode command. To disable the keepalive interval, use the **no** form of this command.

keepalive *msec*

no keepalive *msec*

Syntax Description

<i>msec</i>	Keepalive interval, in milliseconds. The range is 300 to 30000 milliseconds. The default interval is 30000 milliseconds.

Defaults

Keepalive is enabled.

The default keepalive interval is 30000 milliseconds.

Command Modes

cs7 submode

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Examples

The following example shows how to set the keepalive value to 1000 milliseconds:

```
cs7 5000
 local-ip 4.4.4.4
 keepalive 1000
```

Related Commands

Command	Description
cs7 sgmp	Specifies the local port number for and enters <i>cs7</i> submode.
show cs7 sgmp	Displays statistics.

keepalive (cs7 sua)

To specify a keepalive interval to be used when a new SCTP association is started with the local port, use the **keepalive** cs7 sua submode command. To disable the keepalive interval, use the **no** form of this command.

keepalive *msec*

no keepalive *msec*

Syntax Description	<i>msec</i>	Keepalive interval, in milliseconds. The range is 300 to 30000 milliseconds. The default interval is 30000 milliseconds.

Defaults	Keepalive is enabled. The default keepalive interval is 30000 milliseconds.

Command Modes	cs7 sua submode

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples	The following example shows how to set the keepalive value to 1000 milliseconds: <pre>cs7 sua 15000 local-ip 4.4.4.4 keepalive 1000</pre>

Related Commands	Command	Description
	cs7 sua	Specifies the local port number for SUA and enters cs7 sua submode.
	show cs7 sua	Displays SUA statistics.

large-msu-support (cs7 link submode)

To configure large MSU support for an M2PA link, use the **large-msu-support** cs7 link submode command. To disable the support, use the **no** form of this command.

large-msu-support

no large-msu-support

Syntax Description This command has no arguments or keywords.

Defaults M2PA restricts the size of the outgoing packet to 273 bytes.

Command Modes cs7 link submode

Command History	Release	Modification
	12.2(18)IXH	This command was introduced.
	12.4(15)SW3	
	12.2(33)IRC	

Usage Guidelines This command allows an M2PA link to carry MSU sizes of up to 4096 bytes instead of the default maximum of 273 bytes. SCTP segmentation and reassembly is used for MSUs that are larger than 1500 bytes and carried by the M2PA link, because M2PA runs over IP networks with a maximum MSU size of 1500 bytes.

Examples The following example shows how to configure large MSU support on a M2PA link:

```
cs7 instance 0 linkset alaska 1-4-4
link 0
large-msu-support
```

Related Commands	Command	Description
	show cs7 m2pa peer	Displays ITP M2PA statistics.

large-msu-support (cs7 m2pa profile)

To configure large MSU support for all M2PA links in a linkset, use the **large-msu-support** command in cs7 m2pa profile configuration mode. To disable the support, use the **no** form of this command.

large-msu-support

no large-msu-support

Syntax Description

This command has no arguments or keywords.

Defaults

M2PA restricts the size of the outgoing packet to 273 bytes.

Command Modes

cs7 m2pa profile configuration

Command History

Release	Modification
12.2(18)IXH	This command was introduced.
12.4(15)SW3	
12.2(33)IRC	

Usage Guidelines

This command allows an M2PA link to carry MSU sizes of up to 4096 bytes instead of the default maximum of 273 bytes. SCTP segmentation and reassembly is used for MSUs that are larger than 1500 bytes and carried by the M2PA links, because M2PA runs over IP networks with a maximum MSU size of 1500 bytes.

Examples

The following example shows how to configure large MSU support in an M2PA profile:

```
cs7 instance 0 linkset alaska0 1-4-4
profile alpha
m2pa
    large-msu-support
```

Related Commands

Command	Description
m2pa	Specifies M2PA parameters in a CS7 profile.
show cs7 m2pa peer	Displays ITP M2PA statistics.

linestate debounce

To suppress rapid linestate transitions that may occur due to brief interruption of the framing on an E1 line, use the **linestate debounce** command in controller configuration mode. To disable linestate debounce, use the **no** form of this command.

linestate debounce

no linestate debounce

Syntax Description This command has no arguments or keywords.

Defaults None.

Command Modes Controller configuration

Command History	Release	Modification
	12.2(18)IXB	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines Enabling linestate debounce changes the behavior for an individual E1 line such that a Loss of Frame (LOF) condition must persist or subside for approximately 100 milliseconds before the ITP software is notified of the linestate change.

Examples The following example shows how to enable linestate bounce:

```
controller e1 4/0/0
  linestate bounce
```

Related Commands	Command	Description
	controller	Specifies a controller.

link (cs7 linkset)

To configure an SS7 link, use the **link** command in cs7 linkset submode command. To remove a link from a linkset, use the **no** form of this command. A link must be shut down before it can be removed from a linkset.

Serial or T1/E1 TDM SS7 link

link *slc* [*name*] **serial** *interface-number*[:*timeslot*]

no link *slc* [*name*] **serial** *slot*[/*bay*] [:*timeslot*]

M2PA SS7 over IP link

link *slc* [*name*] **sctp** *remote-ip-addr* [*remote-ip-addr* ...] *remote-port-num* *local-port-num* [**passive** | **draft2**]

no link *slc* [*name*] **sctp** *remote-ip-addr* [*remote-ip-addr* ...] *remote-port-num* *local-port-num* [**passive** | **draft2**]

ATM HSL SS7 link

link *slc* [*name*] **atm** *interface-number* [.*subinterface number*]

Syntax Description

atm	ATM interface.
<i>slc</i>	Signal Link Code. Valid range is 0 to 15. The <i>slc</i> value uniquely identifies this link within the linkset. The <i>slc</i> value must match the value configured on the partner node for this link.
<i>name</i>	Name of the group peer on which the link physically resides. The <i>name</i> parameter is valid (and required) only if the ITP Group feature has been configured.
serial	Serial interface.
<i>interface-number</i>	Interface identifier using slot, bay, and port notation, as required for the chassis in use (for example, 3/0, 1/1/0).
sctp	Stream Control Transmission Protocol.
<i>remote-ip-addr</i>	Remote IP address that is one of the four IP addresses configured as local IP addresses on the remote peer. At least one, and up to four, remote IP addresses can be specified.
<i>remote-port-num</i>	Remote port number (the local port number configured on the remote ITP).
<i>local-port-num</i>	Local port number.
passive	Indicates that the remote ITP must establish the peer connection.
draft2	Specifies a peer link that permanently uses the M2PA draft2 protocol.
link	CS7 link definition.
<i>subinterface number</i>	(Optional) Specifies a subinterface number. A period (.) must be used to separate the interface number from the subinterface number (for example, 2/0.1).
: <i>timeslot</i>	Channel group number.

Defaults

The 12.2(25)SW3 software assumes that the protocol of choice is the M2PA RFC version. However, if an endpoint using the pre-RFC M2PA protocol (draft2) communicates with the ITP, then the 12.2(25)SW3 software switches to the M2PA draft2 protocol.

Command Modes

cs7 linkset submode

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The SLC must be the same at both ends of the signaling link to align.

When you issue the **link** command you enter cs7 linkset submode. In cs7 linkset submode, you have access to commands that allow you to further configure links.

When a link is removed from configuration using the **no** form of the command, the issuing user experiences a delayed response of a few seconds. The delay ensures that all previous shutdown-related activity has completed for the link.

Release 12.2(25)SW3 M2PA Version Migration Strategy

In Release 12.2(25)SW3, ITP supports both the current version of M2PA (draft2) and the RFC version. The migration strategy for upgrading from an earlier release to Release 12.2(25)SW3 is as follows:

The ITP detects and uses the protocol that is being used by the peer endpoint. If an endpoint using the M2PA draft2 protocol communicates with the ITP, then the 12.2(25)SW3 software switches to the M2PA draft2 protocol. If an endpoint using the M2PA RFC protocol communicates with the ITP, then the 12.2(25)SW3 software uses the M2PA RFC protocol. This strategy provides the flexibility to upgrade some ITPs in your network to 12.2(25)SW3 and not upgrade other ITPs. M2PA links will work without any configuration changes.

You also have the option to define a link to be a permanent M2PA draft2 link by specifying the draft2 keyword in the link statement. A link configured as such would always expect the remote endpoint to use the M2PA draft2 protocol. If the endpoint does not communicate using M2PA draft2 protocol then the M2PA link will not come up.

Examples

The following example shows how to configure links 0 and 1 to a legacy SS7 device. The names smith and jones are the group peers on which each link resides (indicating that the ITP Group feature has been enabled).

```
cs7 linkset black 5.100.1
 link 0 smith serial1/0/0:0
 link 1 jones serial2/0/0:0
```

The following example shows how to assign link 0 to the ITP linkset named white and how to assign the SCTP peers (remote instance at IP address 172.18.44.147 port 7000 and local instance at port 7000). The link is defined as a permanent M2PA draft2 link.

```
cs7 linkset white 10.1.1
 link 0 sctp 172.18.44.147 7000 7000 draft2
```

The following example shows how to assign link 0 to the ITP linkset named white and assign the SCTP peers (remote instance at IP address 172.18.44.147 port 7000 and local instance at port 7000). In Release 12.2(25)SW3, the ITP assumes that the protocol of choice is the M2PA RFC version.

```
cs7 linkset white 10.1.1
link 0 sctp 172.18.44.147 7000 7000
```

Related Commands

Command	Description
cs7 linkset	Specifies a linkset.
encapsulation mtp2	Specifies MTP2 encapsulation.

linkset (cs7 billing account configuration submode)

To configure a criteria entry of a billing account, use the **linkset** command in the cs7 billing account configuration submode. To remove the criteria, use the **no** form of this command.

```
linkset linkset_name {inbound | outbound} [ type {mtp3 | sccp | sms_sccp} ] {opc-table | dpc-table} pctbl_name
```

```
no linkset linkset_name {inbound | outbound} [ type {mtp3 | sccp | sms_sccp} ] {opc-table | dpc-table} pctbl_name
```

Syntax Description

<i>linkset_name</i>	Name of the criteria entry.
inbound	Messages on inbound interfaces are used for accounting criteria.
outbound	Messages on outbound interfaces are used for accounting criteria.
mtp3	Protocol type for accounting criteria.
sccp	Protocol type for accounting criteria.
sms_sccp	Protocol type for accounting criteria.
opc-table	Point-code specified for the pc-table. Ingress point code (OPC).
dpc-table	Point-code specified for the pc-table. Egress point code (DPC).
<i>pctbl_name</i>	Name of the pc table associated with this entry.

Defaults

None.

Command Modes

cs7 billing account configuration submode

Command History

Release	Modification
12.4(15)SW4 12.2(33)IRD	This command was introduced.
12.4(15)SW6 12.2(33)IRF	The keyword sms_sccp was introduced.

Usage Guidelines

This command specifies an entry of accounting criteria in a billing account.

If you are configuring the cs7 billing account for the SMS protocol, the criteria can only be defined on the inbound interface.

For SMS account IDs, no counters are incremented at the MTP3 or SCCP level. The defined parameters operate at the MAP/IS41 layer to isolate SMS messages for this particular account and increment the relevant counters.

Examples

The following example shows entering the cs7 billing account configuration submode to configure a criteria entry of a billing account with a linkset named **Linkset_01**, an inbound traffic direction, an mtp3 protocol type, an OPC, and a pc table name of PCTBL_01 :

```
cs7 instance 0 billing account BILL_ACCNT
  linkset LINKSET_01 inbound type mtp3 opc-table PCTBL_01
```

The following example shows entering the cs7 billing account configuration submode to configure a criteria entry of a billing account with a linkset named **hsl_tg13_FW1**, an inbound traffic direction, an sms protocol type, an OPC, and a pc table name of PCTBL_01 :

```
cs7 instance 0 billing account BILL_ACCNT-AT-1
  linkset hsl_tg13_FW1 inbound type sms_sccp opc-table PCTBL_01
```

Related Commands

Command	Description
cs7 billing pc-table	Configures a pc-table for the billing account.
cs7 billing options	Configures options for billing.
cs7 billing account	Configures a billing account.
cs7 billing load	Specifies the billing configuration file to load.

link-test

Link testing is performed by sending an SLTM message and verifying the acknowledgement (SLTA) from the adjacent node. Link testing is performed on serial and peer links. To enable link testing, use the **link-test** cs7 link submode command. To disable link testing, use the **no** form of this command.

link-test

no link-test

Syntax Description

This command has no arguments or keywords.

Defaults

This command is enabled by default and tests the links every 30 seconds.

A link test is run automatically when the link first comes into service.

Command Modes

cs7 link submode

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

By default, a link test is run when the link first comes into service, and periodically while the link is in service. If the link test fails, the link is taken out of service.

The slt-t2 timer determines the interval for sending signaling link test messages.

The slt-t1 timer determines the interval to wait for the signaling link test acknowledgement.

If an SLTA is not received in the specified interval, a second SLTM is sent. If an SLTA is not received for the second SLTM, then the link restoration and activation procedure is initiated.

The **no link-test** command disables the link test. The **link-test** command reenables link testing.

Examples

The following example shows how to disable link testing:

```
cs7 linkset michael 10.1.1
link 0 sctp 172.18.44.147 7000 7000
no link-test
```

Related Commands

Command	Description
cs7 mtp3 timer	Configures MTP3 timers.
link (cs7 linkset)	Specifies a link.

link-timer

To configure the ITP MTP3 management timers that control the link, use the **link-timer** cs7 link submode command. To reset a timer to its default value, use the **no** form of this command.

```
link-timer {retry msec | slt-t1 msec | slt-t2 msec | t01 msec | t02 msec | t03 msec | t04 msec | t05 msec | t12 msec | t13 msec | t14 msec | t17 msec | t19 msec | t20 msec | t21 msec | t22 msec | t23 msec | t24 msec | t25 msec | t32 msec}
```

```
no link-timer {retry | slt-t1 | slt-t2 | t01 | t02 | t03 | t04 | t05 | t12 | t13 | t14 | t17 | t19 | t20 | t21 | t22 | t23 | t24 | t32}
```



Note

Ranges are defined by ANSI or ITU.

Syntax Description

retry msec	(ANSI, ITU) Link activation retry timer. (ANSI, ITU) Range of msec is 60000 to 90000 milliseconds. (ANSI, ITU) Default is 60000 milliseconds.
slt-t1 msec	(ANSI, ITU) Link test acknowledgment timer. (ANSI, ITU) Range of msec is 4000 to 12000 milliseconds. (ANSI, ITU) Default is 8000 milliseconds.
slt-t2 msec	(ANSI, ITU) Interval timer for sending test messages. (ANSI, ITU) Range of msec is 30000 to 90000 milliseconds. (ANSI, ITU) Default is 60000 milliseconds.
t01 msec	(ANSI, ITU) Delay to avoid message missequencing. (ANSI, ITU) Range of msec is 500 to 1200 milliseconds. (ANSI, ITU) Default is 800 milliseconds.
t02 msec	(ANSI, ITU) Wait for changeover acknowledgment. (ANSI, ITU) Range of msec is 700 to 2000 milliseconds. (ANSI, ITU) Default is 1400 milliseconds.
t03 msec	(ANSI, ITU) Delay to avoid missequencing in changeback. (ANSI, ITU) Range of msec is 500 to 1200 milliseconds. (ANSI, ITU) Default is 800 milliseconds.
t04 msec	(ANSI, ITU) Wait for changeback acknowledgment (first attempt). (ANSI, ITU) Range of msec is 500 to 1200 milliseconds. (ANSI, ITU) Default is 800 milliseconds.
t05 msec	(ANSI, ITU) Wait for changeback acknowledgment (second attempt). (ANSI, ITU) Range of msec is 500 to 1200 milliseconds. (ANSI, ITU) Default is 800 milliseconds.
t12 msec	(ANSI, ITU) Wait for uninhibited acknowledgment. (ANSI, ITU) Range of msec is 800 to 1500 milliseconds. (ANSI, ITU) Default is 1150 milliseconds.
t13 msec	(ANSI, ITU) Wait for force uninhibited. (ANSI, ITU) Range of msec is 800 to 1500 milliseconds. (ANSI, ITU) Default is 1150 milliseconds.
t14 msec	(ANSI, ITU) Wait for inhibition acknowledgment. (ANSI, ITU) Range of msec is 2000 to 3000 milliseconds. (ANSI, ITU) Default is 2500 milliseconds.

t17 msec	(ANSI, ITU) Delay to avoid oscillation of alignment failure and link restart. (ANSI, ITU) Range of <i>msec</i> is 800 to 1500 milliseconds. (ANSI, ITU) Default is 1150 milliseconds.
t19 msec	(ANSI) Failed link craft referral timer. (ANSI) Range of <i>msec</i> is 480000 to 600000 milliseconds. (ANSI) Default is 540000.
t20 msec	(ANSI) Waiting to repeat local inhibit test. (ANSI) Range of <i>msec</i> is 90000 to 120000 milliseconds. (ANSI) Default is 105000 milliseconds.
t21 msec	(ANSI) Waiting to repeat remote inhibit test. (ANSI) Range of <i>msec</i> is 90000 to 120000 milliseconds. (ANSI) Default is 105000 milliseconds.
t22 msec	(ITU) Local inhibit test timer. (ITU) Range of <i>msec</i> is 180000 to 360000 milliseconds. (ITU) Default is 300000 milliseconds.
t23 msec	(ITU) Remote inhibit test timer. (ITU) Range of <i>msec</i> is 180000 to 360000 milliseconds. (ITU) Default is 300000 milliseconds.
t24 msec	(ITU) Stabilizing timer after removal of local processor outage, used in LPO latching to RPO. (ITU) Range of <i>msec</i> is 400 to 600 milliseconds. (ITU) Default is 500 milliseconds.
t25 msec	(ANSI) Timer at SP adjacent to restarting SP, waiting for traffic restart allowed message. (ANSI) Range of <i>msec</i> is 30000 to 35000 milliseconds. (ANSI) Default is 30000 milliseconds.
t32 msec	(ANSI) Link oscillation timer - Procedure A. Range of <i>msec</i> is 60000 to 120000 milliseconds. Default is 60000 milliseconds.

Defaults

See the defaults listed in Syntax Description.

Command Modes

cs7 link submode

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

MTP3 timers can be defined at three levels: global, linkset, and link.

All global, linkset, and link specific timers can be defined at the global level. These values serve as defaults and are propagated down to the lower levels.

All linkset and link specific timers can be defined at the linkset level. These values serve as defaults for the linkset and all links defined within that linkset. Any values defined here override any global values.

All timers defined at the link level apply to the link and override any values for that timer defined at either the linkset or global level.

Examples

The following example shows how to set the ITP MTP3 T1 timer to 1000 milliseconds for link 0 of linkset1:

```
cs7 linkset linkset1
  link 0
    link-timer t01 1000
```

Related Commands

Command	Description
cs7 linkset	Specifies a linkset and enters cs7 linkset submode.
link (cs7 linkset)	Specifies a link and enters cs7 link submode.
cs7 mtp3 timer	Configures all global, linkset, and link specific timers.
show cs7 linkset	Used with the timer keyword, displays all timers for a linkset and indicates at which level the timers were defined. Displays all the link timers for the linkset.
show cs7 mtp3 timers	Displays all global timers, and all linkset and link timers that have been defined at the global level.
timer (cs7 linkset)	Configures timers for a linkset (and, optionally, timers for links on the linkset).

load (cs7 route table)

Route table contents can be loaded from a URL that locates a binary version of the route table. To load route table contents, use the **load** command in cs7 route table configuration mode. To remove the **load** command from the configuration, use the **no** form of this command.

load { **flash** | **ftp** | **rcp** | **tftp** } *url*

no load { **flash** | **ftp** | **rcp** | **tftp** } *url*

Syntax Description	{ flash ftp rcp tftp }	Device where the route table is stored.
	<i>url</i>	Path and filename of the route table contents.

Defaults None.

Command Modes cs7 route table configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines

The **load** command enters the (new) routing table immediately. When reloading the router, the **load** command is executed before any update route.

Removing the **load** command from the configuration does not empty the routing table, but no table is loaded when the next router reload occurs.

Use this command to load an MTP3 route table upon ITP startup. At startup the ITP loads the route table specified by *url* from a local flash file system or from a remote file system using TFTP/FTP/RCP. After the route table is loaded, all **update route** or **remove route** commands are applied to the previously loaded route table.

If you use the **load** command while the ITP is operational the current (actual/active) route table is replaced with the one specified by *url* and the configured update/remove route commands are reapplied.

Examples The following example shows how to load a file named route.txt from a TFTP server:

```
load tftp://64.102.16.25/route.txt
```

Related Commands	Command	Description
	cs7 route-table	Specifies the ITP route table
	cs7 save route-table	Saves an active route table into a file.

Command	Description
show cs7 route	Displays the ITP routing table.
update route (route-table)	Updates a route.

local-ip (cs7 dcs)

To configure a local IP address for an instance used to send PMP to DCS nodes, use the **local-ip** cs7 dcs configuration submode command. To remove the configuration, use the **no** form of this command.

local-ip *addr port*

no local-ip *addr port*

Syntax Description

<i>addr</i>	An IPv4 address in the form xxx.xxx.xxx.xxx. It is the source IP address for PMP data packets.
<i>port</i>	Source IP address port with an integer range of 1024 to 49151.

Defaults

None.

Command Modes

cs7 dcs configuration submode

Command History

Release	Modification
12.4(15)SW3	This command was introduced.
12.2(33)IRC	

Usage Guidelines

You must shut down the DCS node before deleting a local IP address on that node. You can only modify the local IP address when the DCS node is not part of any DCS group.

Examples

The following example shows how to configure a local IP address with 209.165.201.30 as the address and 3033 as the port on the CS7 DCS node named dcs1:

```
cs7 dcs dcs1
  remote-ip 209.165.201.31 209.165.201.28 33500
  local-ip 209.165.201.30 33500
  ping-interval 5
  timeout-count 3
  udp-checksum
```

Related Commands

Command	Description
cdcs	Adds or removes a DCS endpoint to or from a DCS group.
cookie-life (cs7 local peer)	Identifies a name to be associated with a DCS node.
cs7 dcs-group	Identifies a name to be associated with a DCS group.
cs7 pmp	Turns probeless monitoring on for all linksets and ASes.

local-ip (cs7 local peer)

To configure a local IP address for an instance, use the **local-ip** cs7 local peer submode command. To remove the configuration, use the **no** form of this command.

local-ip *addr*

no local-ip *addr*

Syntax Description	<i>addr</i> IP address.	
Defaults	None.	
Command Modes	cs7 local peer submode	
Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	
Usage Guidelines	You must configure one (and may configure up to four) local IP addresses for each local peer. Cisco ITP uses one of the four local IP addresses for a primary local endpoint instance and uses the other three IP addresses as backups.	
Examples	The following example shows how to assign IP address 172.18.44.254 to the local peer at port 7000: <pre>cs7 local-peer 7000 local-ip 172.18.44.254</pre>	
Related Commands	Command	Description
	cs7 local-peer	Specifies the local peer and enters cs7 local peer submode.

local-ip (cs7 m3ua)

To configure a local IP address for an instance, use the **local-ip** cs7 m3ua submode command. To remove the configuration, use the **no** form of this command.

local-ip *addr*

no local-ip *addr*

Syntax Description	<i>addr</i>	IP address.

Defaults	None.

Command Modes	cs7 m3ua submode

Command History	Release	Modification
	12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.

Usage Guidelines	You must configure one (and may configure up to four) local IP addresses that will receive packets for the configured local port. You can configure multiple IP addresses for SCTP multihoming by specifying additional local-ip commands. The local port will receive packets only from an IP address that was configured.

The local IP address associated with an instance can be added only on the first visit to the instance submode, or when the instance submode is shut down. The local IP address associated with an instance can be removed only when the instance is shut down.

Examples	The following example shows how to assign IP address 4.4.4.4 to the local peer at port 2905:

```
cs7 m3ua 2905
 local-ip 4.4.4.4
```

Related Commands	Command	Description
	cs7 m3ua	Specifies the local port number for M3UA and enters m3ua submode.

local-ip (cs7)

To configure a local IP address for an instance, use the **local-ip** cs7 submode command. To remove the configuration, use the **no** form of this command.

local-ip *addr*

no local-ip *addr*

Syntax Description	<i>addr</i>	IP address.

Defaults	None.

Command Modes	cs7 submode

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	You must configure one (and may configure up to four) local IP addresses that will receive packets for the configured local port. You can configure multiple IP addresses for SCTP multihoming by specifying additional local-ip commands. The local port will receive packets only from an IP address that was configured.

The local IP address associated with an instance can be added only on the first visit to the instance submode, or when the instance submode is shut down. The local IP address associated with an instance can be removed only when the instance is shut down.

Examples	The following example shows how to assign IP address 4.4.4.4 to the local peer at port 5000:

```
cs7 5000
 local-ip 4.4.4.4
```

Related Commands	Command	Description
	cs7 sgmp	Specifies the local peer.

local-ip (cs7 sua)

To configure a local IP address for an instance, use the **local-ip** cs7 sua submode command. To remove the configuration, use the **no** form of this command.

local-ip *addr*

no local-ip *addr*

Syntax Description	<i>addr</i>	Local IP address.

Defaults	None.

Command Modes	cs7 sua submode

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	You must configure one (and may configure up to four) local IP addresses that will receive packets for the configured local port. You can configure multiple IP addresses for SCTP multihoming by specifying additional local-ip commands. The local port will receive packets only from an IP address that was configured.

The local IP address associated with an instance can be added only on the first visit to the instance submode, or when the instance submode is shut down. The local IP address associated with an instance can be removed only when the instance is shut down.

Examples	The following example shows how to assign IP address 4.4.4.4 to the local peer at port 15000: <pre>cs7 sua 15000 local-ip 4.4.4.4</pre>

Related Commands	Command	Description
	cs7 sua	Specifies the local port number for SUA and enters cs7 sua submode.

m2pa

To specify M2PA parameters in a CS7 profile, use the **m2pa** command in cs7 profile configuration mode. To remove the specification, use the **no** form of this command.

m2pa

no m2pa

Syntax Description This command has no arguments or keywords.

Defaults None.

Command Modes cs7 profile configuration

Command History	Release	Modification
	12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.

Examples The following example shows how to define a profile named m2parfc. The profile supports M2PA RFC, specifies the **hold-transport** command, and applies to all the links in the linkset named to_nyc.

```
cs7 profile m2parfc
  m2pa
    hold-transport
  .
  .
  .
cs7 linkset to_nyc
  profile m2parfc
```

Related Commands	Command	Description
	assoc-retransmit	Configures association retransmissions.
	bundling (cs7 link)	Enables and configures message bundling.
	cumulative-sack	Configures cumulative selective ack timeout.
	fast-cwnd-rate	Specifies the rate at which the SCTP congestion window size decreases due to a fast retransmission.
	hold-transport (cs7 m2pa profile)	Specifies that the SCTP association will stay up when the link is shut down.
	idle-cwnd-rate	Specifies the rate at which the SCTP congestion window size decreases due to idle destination.
	init-cwnd-size	Specifies the initial SCTP congestion window size.

Command	Description
init-retransmit	Specifies the number of retransmissions for peer initialization packets.
init-timeout	Specifies the maximum interval for the init packet retransmission timeout value.
ip-dscp	Specifies the differentiated services code point bits in the IP header ToS byte.
ip-precedence	Configures IP precedence.
keepalive	Enables peer link keepalives.
path-retransmit	Configures path retransmissions on the remote-peer address.
peer-timer	Specifies the CS7 peer link timer.
qos-class	Configures the QoS class.
retransmit-cwnd-rate	Configures the rate at which the SCTP congestion window size is reduced due to retransmission timer expiration.
retransmit-timeout	Specifies the minimum retransmission timeout value for the association.
tx-queue-depth (cs7 link)	Configures the MTP2 transmit queue depth.

map-version

To filter specific versions of a gsm-map message, use the **map-version** command in cs7 mlr ruleset rule configuration mode. To remove the configuration, use the **no** form of this command.

map-version *version-number*

no map-version

Syntax Description

<i>version-number</i>	Specifies the specific MAP version used to filter the gsm-map messages. Valid range is 1 to 3.

Defaults

Matches all map-versions.

Command Modes

cs7 mlr ruleset rule configuration

Command History

Release	Modification
12.2(18)IXG	This command was introduced.
12.4(15)SW2	
12.2(33)IRB	

Usage Guidelines

You can configure the MAP version with multiple version values in one command line by separating the versions with a space. This command may be applied to any gsm-map operations that support multiple map-versions.

This command will fail if either:

- You reconfigure the map-version without removing the original configuration.
- You configure the map-version while multi-message-dialogue or allow-multi-message-dialogue is configured.

Examples

The following example shows how to specify map-version 1 and map-version 2 as the filter:

```
cs7 instance 0 mlr ruleset sms-rs1
rule 1 gsm-map sms-mo
map-version 1 2
```

Related Commands

Command	Description
rule (cs7 mlr ruleset)	Specifies the rules for a routing trigger within a multilayer ruleset table and enables cs7 mlr ruleset rule configuration mode.

match access-group

To enable access list packet classification on a linkset, use the **match access-group** cs7 linkset submode command. To remove the configuration, use the **no** form of this command.

match access-group

no match access-group

Syntax Description This command has no arguments or keywords.

Defaults None.

Command Modes cs7 linkset submode

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

This command should be used on input linksets with legacy SS7 links. The **match access-group** command enables the mapping of CS7 access list match criteria to the access list applied to the QoS classes.

Examples

The following example shows how to enable access list packet classification. Incoming packets with service indicator 3 (SCCP) will be assigned QoS class 5.

```
access list 2701 permit si 3

cs7 qos class 5
  qos-ip-precedence 3
  qos-access-group 2701

cs7 linkset to-washington 3.3.3
  match access-group
```

Related Commands

Command	Description
access-list	Defines an access list.
cs7 qos class	Specifies a QoS class.

match any (cs7 asp)

To assign a QoS class number to all inbound traffic, use the **match any** cs7 asp submode command. To remove the configuration, use the **no** form of this command.

match any qos-class *class* [*instance-number*]

no match any qos-class *class* [*instance-number*]

Syntax Description	qos-class	Specifies a QoS class.
	<i>class</i>	QoS class ID. Valid range is 1 to 7.
	<i>instance-number</i>	Required if multiple instances are configured. The valid range is 0 to 7. The default instance is 0.

Defaults	Matches all map-versions.

Command Modes	cs7 asp submode

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples	The following example shows how to assign QoS class 4 to all incoming packets from ASP1:
	cs7 asp ASP1
	match any qos-class 4

Related Commands	Command	Description
	cs7 asp	Specifies an application server process (ASP) and enables cs7 asp submode.
	cs7 qos class	Specifies a QoS class.

match any (cs7 linkset)

To enable input packet classification on a linkset, use the **match any** cs7 linkset submode command. To remove the configuration, use the **no** form of this command.

match any qos-class *class*

no match any qos-class *class*

Syntax Description

qos-class	Specifies a QoS class.
<i>class</i>	QoS class ID. Valid range is 1 to 7.

Defaults

None.

Command Modes

cs7 linkset submode

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

This command should be used on input linksets with legacy SS7 links.

Examples

The following example shows how to configure input linkset packet classification and assign QoS class 4 to the incoming packets:

```
cs7 linkset to-washington 3.3.3
 match any qos-class 4
```

Related Commands

Command	Description
cs7 qos class	Specifies a QoS class.

match si (cs7 asp)

To assign a QoS class number to any inbound packet that has a specific service indicator, use the **match si** command in cs7 asp configuration mode. To remove the configuration, use the **no** form of this command.

match si *si* **qos-class** *class* [*instance-number*]

no match si *si* **qos-class** *class* [*instance-number*]

Syntax Description	<i>si</i>	Service indicator. Valid range is 0 to 15.
	qos-class	Specifies a QoS class.
	<i>class</i>	QoS class ID. Valid range is 1 to 7.
	<i>instance-number</i>	Required if multiple instances are configured. The valid range is 0 to 7. The default instance is 0.

Defaults The default instance is 0.

Command Modes cs7 asp configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples The following example shows how to assign QoS class 3 to all ISUP (si=5) incoming packets from ASP1:

```
cs7 asp ASP1
match si 5 qos-class 3
```

Related Commands	Command	Description
	cs7 asp	Specifies an application server process (ASP) and enables cs7 asp submode.
	cs7 qos class	Specifies a QoS class.

match si (cs7 linkset)

To enable service indicator packet classification on a linkset, use the **match si** command in cs7 linkset configuration mode. To remove the configuration, use the **no** form of this command.

match si *si* **qos-class** *class*

no match si *si* **qos-class** *class*

Syntax Description

<i>si</i>	Service indicator. Valid range is 0 to 15.
qos-class	Specifies a QoS class.
<i>class</i>	QoS class ID. Valid range is 1 to 7.

Defaults

None.

Command Modes

cs7 linkset configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

This command should be used on input linksets with legacy SS7 links.

Examples

The following example shows how to configure service indicator packet classification. Service indicator 5 (ISUP) packets are assigned QoS class 3.

```
cs7 linkset to-washington 3.3.3
 match si 5 qos-class 3
```

Related Commands

Command	Description
cs7 qos class	Specifies a QoS class.

match-unknown-ton-np (cs7 mlr ruleset rule)

To match incoming messages to the corresponding rule parameter regardless of the rule's configured ton/np values, use the **match-unknown-ton-np** command in cs7 mlr ruleset rule configuration mode. Incoming messages containing parameters with an unknown type-of-number (ton=0) or an unknown numbering plan (np=0) will match the rule parameter. To remove the specification, use the **no** form of this command.

match-unknown-ton-np

no match-unknown-ton-np

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Command Modes	cs7 mlr ruleset rule configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	The match-unknown-ton-np command applies to address parameters (such as dest-sme, orig-sme, dest-smsc, and orig-smsc) within the rule.
	Use of the match-unknown-ton-np command is related to the evolution of ITP configuration for matching rule parameter nature-of-address (noa) values—also known as type-of-number (ton) values—and rule parameter numbering plan (np) values with the noa/ton/np values in corresponding parameters of incoming messages. With regard to unknown noa/np values, one effect of the match-unknown-ton-np command is to preserve the pre-12.2(25)SW3 noa/np matching rules.

In ITP releases earlier than release 12.2(25)SW3 no configuration matched a rule parameter of type noa 0 (unknown noa) to *only* those messages that had an unknown noa value in the corresponding parameter. With release 12.2(25)SW3, that type of match can be configured. The following usage guidelines describe the rule-matching implementation through 12.2(25)SW2, the implementation changes in 12.2(25)SW3, and the configuration changes that are automatically generated in a software update to release 12.2(25)SW3.

MLR/SMS rule-matching implementations before ITP release 12.2(25)SW3

In ITP releases earlier than 12.2(25)SW3, MLR/SMS configuration allows matching of a rule parameter noa value with an incoming message as follows:

- If **noa 0** (noa unknown) is specified in a rule parameter, then MLR matches that rule to incoming messages containing the corresponding parameter, regardless of the corresponding parameter's noa value.

- If an incoming message contains a parameter with noa unknown, then MLR matches that message to a rule for the corresponding parameter, regardless of the rule parameter's noa specification.

MLR/SMS rule-matching implementations in ITP release 12.2(25)SW3

Starting with ITP release 12.2(25)SW3, MLR/SMS configuration allows matching of a rule parameter type of number/numbering plan (ton/np) value with an incoming message as follows:

- A new **ton** keyword replaces the **noa** keyword. The keywords **ton** and **np** are optional and mutually independent.
- If **ton/np** is specified on a rule parameter, then MLR matches that rule to only those incoming messages containing the exact ton/np value in the corresponding parameter.
- If **ton/np** is not specified on a rule parameter, then MLR matches that rule to incoming messages containing the corresponding parameter, regardless of the ton/np value received.

Updating from a pre-12.2(25)SW3 release

To maintain consistent MLR/SMS functionality when you update from a pre-12.2(25)SW3 release, MLR/SMS configurations are automatically updated (NVgened) as follows:

- In the pre-12.2(25)SW3 release, a rule parameter configured with **noa 0 np 0** means match that rule to incoming messages containing the corresponding address parameter, regardless of the address *noa* or *np* value. Therefore, in an updated configuration, no **ton/np** specification is NVgened because the behavior is the same as if **ton** and **np** are not used at all in the matching algorithm. The update also does not need to NVgen the **match-unknown-ton-np** command for this rule.
- In the pre-12.2(25)SW3 release, if a rule parameter is configured with any **noa noa np np** values other than the default value 0, then the new configuration will NVgen the equivalent **ton/np** values for the rule parameter. In addition, the update will NVgen the **match-unknown-ton-np** command for the rule because the pre-12.2(25)SW3 MLR action is to match that rule to incoming messages containing unknown ton and np values in the corresponding parameters.

Examples

The following example shows the changes that are NVgened in a configuration that is updated from a pre-12.2(25)SW3 release to release 12.2(25)SW or later:

12.2(25)SW2

```
cs7 mlr ruleset ruleset1
rule 100 sms-mo
  dest-sme 9192 noa 0 np 0
  result as AS1
rule 200 sms-mo
  dest-sme 91934 noa 1 np 0
  result as AS2
```

NVgened Configuration Update to 12.2(25)SW3

```
cs7 mlr ruleset ruleset1
rule 100 sms-mo
  dest-sme 9192
  result as AS1
rule 200 sms-mo
  match-unknown-ton-np
  dest-sme 91934 ton 1
  result as AS2
```

Related Commands	Command	Description
	dest-sme (cs7 mlr ruleset rule)	Specifies the address of the destination short message entity (SME).
	dest-sme-table (cs7 mlr ruleset rule)	Specifies an MLR table of destination SME addresses.
	dest-smsc (cs7 mlr ruleset rule)	Specifies a destination service center address.
	orig-sme (cs7 mlr ruleset rule)	Specifies the address of the origin SME within an MLR operation.
	orig-sme-table (cs7 mlr ruleset rule)	Specifies a table of origin SME addresses to be used to find the desired routing destination.
	rule (cs7 mlr ruleset)	Specifies a rule and the order in which the table is searched within a multilayer ruleset table.

match-unknown-ton-np (cs7 sms set rule)

To match incoming messages to the corresponding rule parameter regardless of the rule's configured ton/np values, use the **match-unknown-ton-np** command in cs7 sms set rule configuration mode. Incoming messages containing parameters with an unknown type-of-number (ton=0) or an unknown numbering plan (np=0) will match the rule parameter. To remove the specification, use the **no** form of this command.

match-unknown-ton-np

no match-unknown-ton-np

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Command Modes	cs7 sms set rule configuration

Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.2(18)IXA</td> <td rowspan="3">This command was introduced.</td> </tr> <tr> <td>12.4(11)SW</td> </tr> <tr> <td>12.2(33)IRA</td> </tr> </tbody> </table>	Release	Modification	12.2(18)IXA	This command was introduced.	12.4(11)SW	12.2(33)IRA
Release	Modification						
12.2(18)IXA	This command was introduced.						
12.4(11)SW							
12.2(33)IRA							

Usage Guidelines	The match-unknown-ton-np command applies to address parameters (such as dest-sme, orig-sme, dest-smsc, and ogig-smsc) within the rule. Use of the match-unknown-ton-np command is related to the evolution of ITP configuration for matching rule parameter nature-of-address (noa) values—also known as type-of-number (ton) values—and rule parameter numbering plan (np) values with the noa/ton/np values in corresponding parameters of incoming messages. With regard to unknown noa/np values, one effect of the match-unknown-ton-np command is to preserve the pre-12.2(25)SW3 noa/np matching rules.

In ITP releases earlier than release 12.2(25)SW3 no configuration matched a rule parameter of type noa 0 (unknown noa) to *only* those messages that had an unknown noa value in the corresponding parameter. With release 12.2(25)SW3, that type of match can be configured. The following usage guidelines describe the rule-matching implementation through 12.2(25)SW2, the implementation changes in 12.2(25)SW3, and the configuration changes that are automatically generated in a software update to release 12.2(25)SW3.

MLR/SMS rule-matching implementations before ITP release 12.2(25)SW3

In ITP releases earlier than 12.2(25)SW3, MLR/SMS configuration allows matching of a rule parameter noa value with an incoming message as follows:

- If **noa 0** (noa unknown) is specified in a rule parameter, then SMS matches that rule to incoming messages containing the corresponding parameter, regardless of the corresponding parameter's noa value.

- If an incoming message contains a parameter with noa unknown, then SMS matches that message to a rule for the corresponding parameter, regardless of the rule parameter's noa specification.

MLR/SMS rule-matching implementations in ITP release 12.2(25)SW3

Starting with ITP release 12.2(25)SW3, MLR/SMS configuration allows matching of a rule parameter type of number/numbering plan (ton/np) value with an incoming message as follows:

- A new **ton** keyword replaces the **noa** keyword. The keywords **ton** and **np** are optional and mutually independent.
- If **ton/np** is specified on a rule parameter, then SMS matches that rule to only those incoming messages containing the exact ton/np value in the corresponding parameter.
- If **ton/np** is not specified on a rule parameter, then SMS matches that rule to incoming messages containing the corresponding parameter, regardless of the ton/np value received.

Updating from a pre-12.2(25)SW3 release

To maintain consistent MLR/SMS functionality when you update from a pre-12.2(25)SW3 release, MLR/SMS configurations are automatically updated (NVgened) as follows:

- In the pre-12.2(25)SW3 release, a rule parameter configured with **noa 0 np 0** means match that rule to incoming messages containing the corresponding address parameter, regardless of the address *noa* or *np* value. Therefore, in an updated configuration, no **ton/np** specification is NVgened because the behavior is the same as if **ton** and **np** are not used at all in the matching algorithm. The update also does not need to NVgen the **match-unknown-ton-np** command for this rule.
- In the pre-12.2(25)SW3 release, if a rule parameter is configured with any **noa noa np np** other than the default value 0, then the new configuration will NVgen the equivalent **ton/np** values for the rule parameter. In addition, the update will NVgen the **match-unknown-ton-np** command for the rule because the pre-12.2(25)SW3 SMS action is to match that rule to incoming messages containing unknown ton and np values in the corresponding parameters.

Examples

The following example shows the changes that are NVgened in a configuration that is updated from a pre-12.2(25)SW3 release to release 12.2(25)SW or later:

12.2(25)SW2

```
cs7 sms ruleset ruleset1
rule 100 sms-mo
  dest-sme 9192 noa 0 np 0
  result as AS1
rule 200 sms-mo
  dest-sme 91934 noa 1 np 0
  result as AS2
```

NVgened Configuration Update to 12.2(25)SW3

```
cs7 sms ruleset ruleset1
rule 100 sms-mo
  dest-sme 9192
  result as AS1
rule 200 sms-mo
  match-unknown-ton-np
  dest-sme 91934 ton 1
  result as AS2
```

Related Commands	Command	Description
	dest-sme (cs7 sms set rule)	Specifies the address of the destination Short Message Entity (SME).
	dest-sme-table (cs7 sms set rule)	Specifies an SMS table of destination SME addresses.
	dest-smsc (cs7 sms set rule)	Specifies a destination service center address.
	orig-sme (cs7 sms set rule)	Specifies the address of the origin SME.
	orig-sme-table (cs7 sms set rule)	Specifies a table of origin SME addresses to be used to find the desired routing destination.
	ruleset (cs7 sms ansi41 smsnot)	Specifies a rule and the order in which the table is searched.

max-inbound-streams (cs7 m3ua)

To configure the maximum number of inbound streams allowed for the local port, use the **max-inbound-streams** cs7 m3ua submode command. To remove the configuration, use the **no** form of this command.

max-inbound-streams *max-streams*

no max-inbound-streams *max-streams*

Syntax Description	<i>max-streams</i>	The maximum number of inbound streams allowed for the local port. The range is 2 to 25. The default is 17 streams.

Defaults	17 streams

Command Modes	cs7 m3ua submode

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples	The following command shows how to allow a maximum of 10 streams on the local port:

```
cs7 m3ua 2905
 local-ip 4.4.4.4
 max-inbound-streams 10
```

Related Commands	Command	Description
	cs7 m3ua	Specifies the local port number for M3UA and enters cs7 m3ua submode.
	show cs7 m3ua	Displays M3UA statistics.

max-inbound-streams (cs7)

To configure the maximum number of inbound streams allowed for the local port, use the **max-inbound-streams** *cs7* submode command. To remove the configuration, use the **no** form of this command.

max-inbound-streams *max-streams*

no max-inbound-streams *max-streams*

Syntax Description	<i>max-streams</i> The maximum number of inbound streams allowed for the local port. The range is 2 to 25. The default is 17 streams.	
Defaults	17 streams	
Command Modes	cs7 submode	
Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	
Examples	The following command shows how to allow a maximum of 10 streams on the local port: cs7 5000 local-ip 4.4.4.4 max-inbound-streams 10	
Related Commands	Command	Description
	cs7 sgmp	Specifies the local port number for and enters cs7 submode.
	show cs7 sgmp	Displays statistics.

max-inbound-streams (cs7 sua)

To configure the maximum number of inbound streams allowed for the local port, use the **max-inbound-streams** cs7 sua submode command. To remove the configuration, use the **no** form of this command.

max-inbound-streams *max-streams*

no max-inbound-streams *max-streams*

Syntax Description	<i>max-streams</i>	The maximum number of inbound streams allowed for the local port. The range is 2 to 25. The default is 17 streams.

Defaults	17 streams

Command Modes	cs7 sua submode

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples The following command shows how to allow a maximum of 10 streams on the local port:

```
cs7 sua 15000
 local-ip 4.4.4.4
 max-inbound-streams 10
```

Related Commands	Command	Description
	cs7 sua	Specifies the local port number for SUA and enters cs7 sua submode.
	show cs7 sua	Displays SUA statistics.

modify-failure (mlr options)

To specify the desired action when MLR packet modification fails, use the **modify-failure** command in `cs7 mlr options` configuration mode. To remove the specification, use the **no** form of this command.

modify-failure { **discard** | **resume** | **sccp-error** *sccp-error* }

no modify-failure { **discard** | **resume** | **sccp-error** *sccp-error* }

Syntax Description

discard	Discards packet (default).
resume	Resumes sending the original packet to the original destination.
sccp-error	Sends a UDTS to the originator with the configured SCCP error code if return-on-error was set in the UDT.
<i>sccp-error</i>	SCCP UDTS return cause values.

Defaults

The packet is discarded.

Command Modes

`cs7 mlr options` configuration

Related Commands

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The **modify-failure** command allows you to specify which action should be taken when an MLR packet cannot be modified. By default, the packet is discarded. MLR modification failures include exceeding the maximum MSU or address size when inserting new data, failures when attempting to modify the destination GT, and failures when executing a **modify-profile** command.

Examples

The following example shows how to specify the **modify-profile** command:

```
cs7 mlr options
  modify-failure sccp-error 7
```

modify-failure (pam)

To specify the desired action when the PAM table packet modification fails, use the **modify-failure** command in CS7 PAM configuration submode. To remove the specification, use the **no** form of this command.

modify-failure { **discard** | **resume** | **sccp-error** *sccp-error* }

no modify-failure { **discard** | **resume** | **sccp-error** *sccp-error* }

Syntax Description

discard	Discards packet (default).
resume	Resumes sending the original packet to the original destination.
sccp-error	Sends a UDTS to the originator with the configured SCCP error code if return-on-error was set in the UDT.
<i>sccp-error</i>	SCCP UDTS return cause values.

Defaults

The packet is discarded.

Command Modes

CS7 PAM configuration submode

Related Commands

Release	Modification
12.4(15)SW5 12.2(33)IRE	This command was introduced.

Usage Guidelines

The **modify-failure** command allows you to specify which action should be taken when an error occurs during a packet modification.

Examples

The following example shows how to configure a PAM table with the **modify-failure** command to resume sending the original packet to the original destination:

```
cs7 instance 0 pam alpha
  cgpa gt prefix tt 0 pc 1.2.3 ssn 12
  cdpa gt prefix 15 123456789abcdef tt 250 gti 4 np 15 nai 127 pc 1.123.4 ssn 255\n
1.2.3
dpc 2.3.4
modify-failure resume
```

Related Commands

■ **modify-failure (pam)**

cs7 pam	Identifies a packet address modification (PAM) table and enters the CS7 PAM submode.
cgpa (cs7 pam)	Configures one cgpa entry in the PAM table.
cdpa (cs7 pam)	Configures one cdpa entry in the PAM table.
dpc	Configures a dpc entry in the PAM table.
cs7 gws action-set	Defines gateway screening action sets that may include a PAM table.
gta asname	Creates or modifies a GTA entry that translates to an M3UA or SUA application server name. The GTA entry may include a PAM table.

modify-profile (cs7 mlr ruleset rule)

To specify SCCP and MAP addresses to modify in messages that are routed using MLR, use the **modify-profile** command in cs7 mlr ruleset rule configuration submode. Only one modification profile may be specified in a rule.

To disable the settings, use the **no** form of this command.

modify-profile [*profile-name*]

no modify-profile [*profile-name*]

Syntax Description	<i>profile-name</i>	Identifies a name to be associated with a defined MLR modification profile. The name is specified as a string with a maximum of 12 characters.
Defaults	None.	
Command Modes	cs7 mlr ruleset rule configuration	
Command History	12.2(18)IXC	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	
	12.2(18)IXE	The configuration submode was introduced.
Usage Guidelines	The protocol and operation of the associated rule and modification profile must be compatible for the modification to occur. This command is not valid for the all-operations rule operation type and protocol has not been defined for the ruleset.	
Examples	The following uses the modify-profile command: <pre>cs7 mlr modify-profile SRISM gsm-map sri-sm orig-smsc prefix 2 351 cgpa gt prefix 2 351 cs7 mlr ruleset FROM_MMSC rule 10 gsm-map sri-sm default orig-smsc 397777777 modify-profile SRISM result route</pre>	

 `modify-profile (cs7 mlr ruleset rule)`

Related Commands	Command	Description
	cs7 mlr ruleset	Specifies the rules for a routing trigger within a multilayer ruleset table and enables cs7 mlr ruleset rule configuration mode.
	rule (cs7 mlr ruleset)	Specifies the rules for a routing trigger within a multilayer ruleset table.
	cs7 mlr modify-profile	Specifies an MLR modify profile.

msc-proxy-addr (cs7 sms smsmo)

To enable the SMS MO Proxy feature and specify a MAP MSC Proxy address, use the **msc-proxy-addr** command in cs7 sms smsmo configuration mode. To remove the address, use the **no** form of this command.

msc-proxy-addr [**use** {**international** | **national**}] **tt** *tt* **gti** *gti* [**np** *np* **nai** *nai*]

no msc-proxy-addr

Syntax Description		
tt		Configure the translation type.
<i>tt</i>		Translation type, in the range 0 to 255.
gti		Specifies a global title indicator.
<i>gti</i>		Global title indicator. Valid numbers are 2 (primarily used in the ANSI domain) or 4 (used in the ITU domain).
np		In ITU domain, specifies a numbering plan.
<i>np</i>		Numbering plan. Valid range is 0 to 15.
nai		In ITU domain, specifies a nature of address indicator. Required for a <i>gti</i> value of 4. Optional for a <i>gti</i> value of 2.
<i>nai</i>		Nature of address indicator. Valid range is 0 to 127.
use		Indicates setting for national use bit in the address indicator.
international		Address has international scope (default for ITU/CHINA).
national		Address has national scope (default for ANSI).

Defaults None.

Command Modes cs7 sms smsmo configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines

The **msc-proxy-addr** command specifies how servicing MSC addresses are translated in the proxied dialog toward the SMSC.

The **msc-proxy-addr** command specifies a MAP MSC Proxy address. The address is used to form the SCCP CgPA for a proxied MO dialog.

The **msc-proxy-addr** command enables cs7 sms smsso msc proxy configuration mode.

Examples

The following example shows how to configure an SMS route table and how to specify a CDR service, GSM MAP routing, and a MAP MSC Proxy address:

```
cs7 sms route-table
cdr-service
gsm-map sms-mo
msc-proxy-addr use international tt 4
```

Related Commands

Command	Description
gsm-map (cs7 sms route table)	Specifies the GSM MAP operation.

mtp2

To configure CS7 link profile parameters for MTP2, use the **mtp2** cs7 profile submode command. To disable the settings, use the **no** form of this command.

mtp2

no mtp2

Syntax Description	This command has no arguments or keywords.

Defaults	The command is disabled.

Command Modes	cs7 profile submode

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples	The following example shows how to define a profile named timers. The profile supports MTP2, configures the t1 and t2 settings, and applies to all the links in the linkset named itpa.

```
cs7 profile timers
 mtp2
  timer t1 45000
  timer t2 9000
.
.
.
cs7 linkset itpa
 profile timers
```

Related Commands	Command	Description
	cs7 profile	Defines a profile that you can apply to all the links in a linkset.
	variant jt1	Configures a CS7 link profile variant.

mtp2-timer

Traditional SS7 links use serial interfaces. ITP interfaces are configured to use encapsulation MTP2. You can tune several MTP2 timers.

To tune MTP2 encapsulation timers, use the **mtp2-timer** cs7 link submode command with one of the timers. To reset the timers, use the **no** form of this command.

```
mtp2-timer {t1 msec | t2 msec | t3 msec | t4e msec | t4n msec | t5 msec | t6 msec | t7 msec | ttc timer msec}
```

```
no mtp2-timer {t1 msec | t2 msec | t3 msec | t4e msec | t4n msec | t5 msec | t6 msec | t7 msec | ttc timer msec}
```



Note

Ranges are ANSI or ITU defined.

Syntax Description

t1	Alignment ready timer. ANSI default is 13000 milliseconds. ITU default is 40000 milliseconds.
t2	Not aligned timer. ANSI default is 11500 milliseconds. ITU default is 5000 milliseconds.
t3	Aligned timer. ANSI default is 11500 milliseconds. ITU default is 1500 milliseconds.
t4e	Emergency proving period timer. ANSI default is 600 milliseconds. ITU default is 500 milliseconds.
t4n	Normal proving period timer. ANSI default is 2300 milliseconds. ITU default is 8200 milliseconds.
t5	Sending SIB timer. ANSI default is 80 milliseconds. ITU default is 100 milliseconds.
t6	Remote congestion timer. ANSI default is 1000 milliseconds. ITU default is 3000 milliseconds.
t7	Excessive delay of acknowledgment timer. ANSI default is 1000 milliseconds. ITU default is 1000 milliseconds.
ttc	ttc ta msec: TTC timer for sending SIE. Valid range is 10 to 250 milliseconds. Default is 20 milliseconds. ttc te msec: TTC timer for error monitoring. Valid range is 10 to 250 milliseconds. Default is 20 milliseconds. ttc tf msec: TTC timer for sending FISU. Valid range is 10 to 250 milliseconds. Default is 20 milliseconds. ttc to msec: TTC timer for sending SIO. Valid range is 10 to 250 milliseconds. Default is 20 milliseconds. ttc ts msec: TTC timer for sending SIOS. Valid range is 10 to 250 milliseconds. Default is 20 milliseconds.

Defaults

t1: ANSI = 13000; ITU = 40000

t2: ANSI = 11500; ITU = 5000

t3: ANSI = 11500; ITU = 1500

t4E: ANSI = 600; ITU = 500
 t4N: ANSI = 2300; ITU = 8200
 t5: ANSI = 80; ITU = 100
 t6: ANSI = 1000; ITU = 3000
 t7: ANSI= 1000; ITU = 1000
 ta: 20 ms
 te: 20 ms
 tf: 20 ms
 to: 20 ms
 ts: 20 ms

Command Modes cs7 link submode

Command History	Release	Modification
	12.2(18)IXA	This command replaced the cs7 mtp2 interface configuration command.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines MTP2 parameters can also be specified in a CS7 profile.

Examples The following example shows how to set the T1 timer for 25000 milliseconds:

```

cs7 linkset ITP2 6.100.5
 link 0 serial0/0:0
 mtp2-timer t1 25000

```

The following example shows how to set the TTC te timer for 100 milliseconds:

```

cs7 linkset ITP2 6.100.5
 link 0 sctp 192.68.1.2 7000 7000
 mtp2-timer ttc te 100

```

Related Commands	Command	Description
	bundling (cs7 link)	Enables and configures message bundling.
	cs7 profile	Defines a profile of MTP2 parameters that you can apply to all the links in a linkset.
	mtp2-timer ttc enable	Enables the use of TTC timers.
	show cs7 mtp2	Displays ITP MTP2 status.
	tx-queue-depth (cs7 link)	Configures the MTP2 transmit queue depth.

mtp2-timer ttc enable

The MTP/TTC variant allows configuration of TTC Signal Unit (SU) transmission timer values. To enable the use of MTP2 TTC timers, use the **mtp2-timer ttc enable** cs7 link submode command with one of the timers. To disable the timers, use the **no** form of this command.

mtp2-timer ttc enable

no mtp2-timer ttc enable

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Command Modes	cs7 link submode

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	After enabling the use of MTP2 TTC timers, you can set the timer values.

Examples	The following example shows how to enable the use of TTC timers:

```
cs7 linkset ITP2 6.100.5
link 0 serial0/0:0
  mtp2-timer ttc enable
```

Related Commands	Command	Description
	mtp2-timer	Tunes MTP2 encapsulation timers.
	show cs7 mtp2	Displays ITP MTP2 status.

multiplicity

To specify a method for selecting a destination in the application group, use the **multiplicity** in **cs7 gtt** application group submode. To restore the default multiplicity (share), use the **no** form of this command.

multiplicity {cost | share | cgpa | wrr}

no multiplicity

Syntax Description	cost	Uses the destination with the least cost if available.
	share	Shares equally among all destinations.
	cgpa	Uses the SCCP calling party address (CGPA) field, which results in a weighted factor selection number for choosing the next destination from the available items in the application group.
	wrr	Applies weighted round robin load balancing (WRR) to SCCP class 0 and SCCP class 1 traffic.

Defaults The default multiplicity is to share.

Command Modes cs7 gtt application group submode

Command History	Release	Modification
	12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.
	12.4(15)SW4 12.2(33)IRD	The keyword wrr was introduced.

Examples The following example shows how to configure an application group of three items. The first item is used approximately twice as many times as the other two items. These items handle equal amounts of traffic.

```
cs7 gtt application-group group1
multiplicity cgpa
pc 1.1.1 ssn 8 50 pcssn
pc 1.1.2 ssn 8 25 pcssn
pc 1.1.3 ssn 8 25 pcssn
```

Related Commands	Command	Description
	cs7 gtt application-group	Specifies a GTT application group.
	cs7 gtt map	Configures a Global Title Mated Application (MAP) entry.
	pc (cs7 gtt application group)	Adds or changes a point code and optional subsystem number in the application group.

■ multiplicity

Command	Description
asname (cs7 gtt application group)	Assigns an M3UA or SUA AS directly to a global title
cs7 sccp-class1-wrr	Configures the WRR option for GTT application groups.

nai

To specify a new nature of address (na) to be applied for the whole GTT address conversion table, use the **nai** cs7 gtt address conversion submode command. To disable the configuration, use the **no** form of this command.

nai *nai*

no **nai**

Syntax Description

<i>nai</i>	Nature of address value. The range is 0 to 127.

Defaults

None.

Command Modes

cs7 gtt address conversion submode

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Examples

The following example shows how to convert the *nai* value to 4 for all addresses that are converted:

```
cs7 gtt address-conversion e212e214
nai 4
```

Related Commands

Command	Description
cs7 gtt address-conversion	Configures a GTT address conversion table.

network-appearance

To define the value used in the network appearance parameter in M3UA and SUA messages, use the **network-appearance** command in cs7 as configuration mode. To remove the definition and use the actual instance number instead, use the **no** form of this command.

network-appearance *number*

no network-appearance *number*

Syntax Description	<i>number</i>	A value in the range 1 to 4294967295 to be used in the network appearance parameter in M3UA and SUA messages.

Defaults	None.

Command Modes	cs7 as configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	If network-appearance is not configured, the actual instance number is used instead. If network-appearance is already configured on another AS, it is valid only if the other AS has the same instance.

When you configure a network appearance value, the value must be unique among all instances of ITP. ITP cannot share a network appearance value between instances. If you try to configure a network appearance value between 1 and 7 inside an AS, and that value instance is already configured, ITP displays a warning indicating that network appearance is reserved for that instance. For example, if you configure a network appearance value of 3 on instance 1, while instance 3 is already configured on ITP, ITP displays a warning that network appearance value of 3 is reserved for instance 3.

Examples	The following example shows how to define the network appearance parameter as 100:

```
network-appearance 100
```

Related Commands	Command	Description
	cs7 mtp3 tuning rx-congestion-threshold	Enables multiple instances of a variant and network indicator combination.

new-name

To rename an existing GTT selector, use the **new-name** `cs7 gtt selector submode` command. To disable the configuration, use the **no** form of this command.

new-name *selector-name*

no new-name

Syntax Description

<i>selector-name</i>	New name for the GTT selector.

Defaults

None.

Command Modes

cs7 gtt selector submode

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

Since the GTT data is not stored in NVRAM, commands such as **show running config** will not display the GTT data. To display the current running configuration regarding GTT use the **show cs7 gtt config** command.

Examples

The following example shows how to rename the existing GTT selector to test1:

```
new-name test1
```

Related Commands

Command	Description
cs7 gtt selector	Configures a new GTT selector or enters the submode for modifying the attributes of a selector.
show cs7 gtt config	Displays the running configuration of GTT.

next-table

To add a next table entry to an existing GTT selector, use the **next-table** *cs7 gtt* selector submode command. To disable the configuration, use the **no** form of this command.

next-table *selector-name* [**ntt** *ntt*]

no next-table *selector-name* [**ntt** *ntt*]

Syntax Description

next-table	Configures a next table for the default GTT selector.
<i>selector-name</i>	Name of the GTT selector that the master table points to as the next table. The name is specified as a character string from 1 to 12 characters.
ntt	Specifies the value of the TT which will be modified in the MSU when it is forwarded to the next ITP instance.
<i>ntt</i>	The value of the TT. The range is between 0 and 255.

Defaults

None.

Command Modes

cs7 gtt selector submode

Command History

Release	Modification
12.4(15)SW5	This command was introduced.
12.2(33)IRE	

Usage Guidelines

This command configures the default GTT entry in a GTT table to point to another GTT table (next table). The next table needs to be in the same instance or have the same NI and SS7 variants. Multiple tables can refer to a single next table. The next table is also accessible directly for GTT operations.

Since the GTT data is not stored in NVRAM, commands such as **show running config** will not display the GTT data. To display the current running configuration regarding GTT use the **show cs7 gtt config** command.

Examples

The following example shows how to configure the GTT selector named alpha as the next table:

```
next-table alpha
```

Related Commands

Command	Description
cs7 gtt selector	Configures a new GTT selector or enters the submode for modifying the attributes of a selector.
show cs7 gtt config	Displays the running configuration of GTT including information on any configured next-table commands.

np

To specify a new numbering plan to be applied for the whole table, use the **np** *cs7* gtt address conversion submode command. To disable the configuration, use the **no** form of this command.

np *np*

no np

Syntax Description

<i>np</i>	Numbering plan value. The range is 0 to 15.

Defaults

None.

Command Modes

cs7 gtt address conversion submode

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Examples

The following example shows how to convert the *np* value to 6 for all addresses that are converted:

```
cs7 gtt prefix-conversion e212e214
np 6
```

Related Commands

Command	Description
cs7 gtt address-conversion	Configures a GTT address conversion table.

opc

To configure an originating point code (OPC) entry in the PAM table, use the **opc** command in CS7 PAM configuration submode. To remove the specification, use the **no** form of this command.

opc *point-code*

no opc *point-code*

Syntax Description	<i>point-code</i>	The signaling point code in the point code format.
Defaults	None.	
Command Modes	CS7 PAM configuration submode	
Command History	Release	Modification
	12.4(15)SW5 12.2(33)IRE	This command was introduced.
Usage Guidelines	None.	
Examples	The following example shows the opc signaling point code entry 1.2.3 in the point code format. It is configured for the PAM table named alpha: <pre>cs7 instance 0 pam alpha cgpa gt prefix tt 0 pc 1.2.3 ssn 12 cdpa gt prefix 15 123456789abcdef tt 250 gti 4 np 15 nai 127 pc 1.123.4 ssn 255\n opc 1.2.3 dpc 2.3.4 modify-failure resume</pre>	

orig-imsi (cs7 mlr ruleset rule)

Command	Description
cs7 pam	Identifies a packet address modification (PAM) table and enters the CS7 PAM submode.
cgpa (cs7 pam)	Configures a cgpa entry in the PAM table.
cdpa (cs7 pam)	Configures a cdpa entry in the PAM table.
dpc	Configures a dpc entry in the PAM table.
modify-failure (pam)	Specifies the desired action when the PAM table packet modification fails.
cs7 gws action-set	Defines gateway screening action sets that may include a PAM table.
gta asname	Creates or modifies a GTA entry that translates to an M3UA or SUA application server name. The GTA entry may include a PAM table.

To specify an origin IMSI, use the **orig-imsi** command in cs7 mlr ruleset rule configuration mode. To remove the configuration, use the **no** form of this command.

orig-imsi { * | *imsi-addr* | **unknown** } [**exact**] [**min-digits** *min*] [**max-digits** *max*]

no orig-imsi

Syntax Description

<i>imsi-addr</i>	IMSI address up to 16 hexadecimal digits.
unknown	Unknown origin IMSI.
exact	Configured address must match origin IMSI exactly.
min-digits	(Optional) Specifies the minimum number of digits in the address string.
<i>min</i>	Minimum number of digits in the address string. The default is 1.
max-digits	(Optional) Specifies the maximum number of digits in the address string.
<i>max</i>	Maximum number of digits in the address string. The default is the length of the address string.

Defaults

The maximum number of digits in the address string is 1.

Command Modes

cs7 mlr ruleset rule configuration

Command History

Release	Modification
12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.
12.2(18)IXG 12.4(15)SW2 12.2(33)IRB	This command supports UpdateLocation MSUs.

Usage Guidelines

In release 12.2(18)IXG 12.4(15)SW1 and later, this command supports UpdateLocation MSUs. This support helps identify specific subscribers by the originator IMSI and block specific fraudulent activity.

Examples

The following example shows how to specify a ruleset named ruleset1, a rule index of 20, and an origin IMSI address of 1111:

```
cs7 sms ruleset1
rule 20 sms-mo
  orig-imsi 1111
  result group grp1
```

The following example shows how to block the origin IMSI address of 861381234567:

```
rule 4 updLocation
orig-imsi 861381234567
result block
```

Related Commands

Command	Description
rule (cs7 mlr ruleset)	Specifies the rules for a routing trigger within a multilayer ruleset table and enables cs7 mlr ruleset rule configuration mode.

orig-imsi (cs7 sms set rule)

To specify an origin IMSI, use the **orig-imsi** command in cs7 sms set rule configuration mode. To remove the configuration, use the **no** form of this command.

orig-imsi { * | *imsi-addr* | **unknown** } [**exact**] [**min-digits** *min*] [**max-digits** *max*]

no orig-imsi

Syntax Description

<i>imsi-addr</i>	IMSI address up to 16 hexadecimal digits.
unknown	Unknown origin IMSI.
exact	Configured address must match origin IMSI exactly.
min-digits	(Optional) Specifies the minimum number of digits in the address string.
<i>min</i>	Minimum number of digits in the address string. The default is 1.
max-digits	(Optional) Specifies the maximum number of digits in the address string.
<i>max</i>	Maximum number of digits in the address string. The default is the length of the address string.

Defaults

The maximum number of digits in the address string is 1.

Command Modes

cs7 sms set rule configuration

Command History

Release	Modification
12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.
12.2(18)IXG 12.4(15)SW2 12.2(33)IRB	The orig-imsi and orig-imsi-table commands became valid under the updLoc operation.

Examples

The following example shows how to specify an SMS ruleset named SMS-RULES, a rule index of 20, and an origin IMSI address of 1111:

```
cs7 sms ruleset SMS-RULES
rule 20 sms-mo
  orig-imsi 1111
result group smsgrp
```

Related Commands

Command	Description
dest-sme (cs7 mlr ruleset rule)	Specifies an application destination port number.
dest-sme (cs7 sms set rule)	Specifies a destination short message entity (SME).

Command	Description
dest-sme-table (cs7 sms set rule)	Specifies an SMS table of destination SME addresses.
dest-smsc (cs7 sms set rule)	Specifies a destination SMSC.
orig-imsi-table (cs7 sms set rule)	Specifies an SMS table of origin IMSI addresses (address-table).
orig-sme (cs7 sms set rule)	Specifies an origin SME.
orig-sme-table (cs7 sms set rule)	Specifies an SMS table of origin SME addresses (address-table).
pid (cs7 sms set rule)	Specifies a protocol identifier (TP-PID).
result (cs7 sms set rule)	Specifies a result.
ruleset (cs7 sms ansi41 smsnot)	Specifies a rule within a ruleset.

orig-imsi-table (cs7 mlr ruleset rule)

To specify an SMS table of origin IMSI addresses, use the **orig-imsi-table** command in cs7 mlr ruleset rule configuration mode. To remove the configuration, use the **no** form of this command.

orig-imsi-table *table-name*

no orig-imsi-table *table-name*

Syntax Description	<i>table-name</i>	Address table name.

Defaults	None.

Command Modes	cs7 mlr ruleset rule configuration

Command History	Release	Modification
	12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.
	12.2(18)IXG 12.4(15)SW2 12.2(33)IRB	The orig-imsi and orig-imsi-table rule commands became valid under the updLoc operation.

Usage Guidelines This command supports UpdateLocation MSUs. This support helps identify specific subscribers by the originator IMSI and block specific fraudulent activity.

The **dest-sme-table**, **orig-imsi-table**, and **orig-sme-table** rule commands accept either an SMS address table name *or* an MLR address table name. This ability is primarily for customers who want the SMS-MO Proxy functionality. The address table names are unique between DSMR and MLR. You can enter an MLR address table name for an SMS rule parameter. However, MLR cannot reference SMS address tables.

If an incoming message matches an SMS rule that references an MLR address table, then any MLR address table result is mapped to an SMS result:

- BLOCK, PC, and PCSSN results map from MLR to SMS.
 - For result groups, the MLR result group name is mapped to an SMS result group name.
 - If the SMS result group is not configured, then the result specified on the rule is used.
- AS and CONTINUE results are not valid in SMS. For these cases, the result specified on the rule is used. If no result is specified, the result on the rule is used (the same as with MLR).

If multiple rule parameters are configured for a rule, then the rule result will be used (rather than a result specified in the address table).

If the result type specified within the table is valid, it is used. Otherwise, the result in the rule is used.

For all tables, the noa and np values must match before the table is accessed.

Examples

The following example shows how to specify an MLR ruleset named ruleset1, a rule index of 20, and an SMS table of origin IMSI addresses named SHORTLIST:

```
cs7 mlr ruleset ruleset1
rule 20 sms-mo
  orig-imsi-table SHORTLIST
  result block
```

The following example shows how to block the origin IMSI table named test:

```
rule 5 updLocation
orig-imsi-table test
result block
```

Related Commands

Command	Description
rule (cs7 mlr ruleset)	Specifies the rules for a routing trigger within a multilayer ruleset table and enables cs7 mlr ruleset rule configuration mode.

orig-imsi-table (cs7 sms set rule)

To specify an SMS table of origin IMSI addresses, use the **orig-imsi-table** command in cs7 sms set rule configuration mode. To remove the configuration, use the **no** form of this command.

orig-imsi-table *table-name* [**noa** *noa-value* **np** *np-value*]

no orig-imsi-table *table-name*

Syntax Description

<i>table-name</i>	Address table name.
noa	Specifies a nature of address.
<i>noa-value</i>	Valid range is 0 to 7.
np	Specifies a numbering plan identification value.
<i>np-value</i>	Valid range is 0 to 15.

Defaults

None.

Command Modes

cs7 sms set rule configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The **dest-sme-table**, **orig-imsi-table**, and **orig-sme-table** rule commands accept either an SMS address table name *or* an MLR address table name. This ability is primarily for customers who want the SMS-MO Proxy functionality. The address table names are unique between FDA and MLR. You can enter an MLR address table name for an SMS rule parameter. However, MLR cannot reference SMS address tables.

If an incoming message matches an SMS rule that references an MLR address table, then any MLR address table result is mapped to an SMS result:

- BLOCK, PC, and PCSSN results map from MLR to SMS.
 - For result groups, the MLR result group name is mapped to an SMS result group name.
 - If the SMS result group is not configured, then the result specified on the rule is used.
- AS and CONTINUE results are not valid in SMS. For these cases, the result specified on the rule is used. If no result is specified, the result on the rule is used (the same as with MLR).

If multiple rule parameters are configured for a rule, then the rule result will be used (rather than a result specified in the address table).

If the result type specified within the table is valid, it is used. Otherwise, the result in the rule is used.

For all tables, the noa and np values must match before the table is accessed.

Examples

The following example shows how to specify an SMS ruleset named SMS-RULES, a rule index of 20, and an SMS table of origin IMSI addresses named SHORTLIST:

```
cs7 sms ruleset SMS-RULES
rule 20 sms-mo
  orig-imsi-table SHORTLIST
  result block
```

orig-sme (cs7 mlr ruleset rule)

Command	Description
cgpa (cs7 mlr trigger)	Tests the availability of the CDR service queue as the input condition of the rule.
cs7 sms ruleset	Specifies a ruleset.
dest-sme (cs7 mlr ruleset rule)	Specifies an application destination port number.
dest-sme (cs7 mlr ruleset rule)	Specifies a destination short message entity (SME).
dest-sme-table (cs7 sms set rule)	Specifies an SMS table of destination SME addresses.
dest-smsc (cs7 sms set rule)	Specifies a destination SMSC.
orig-imsi (cs7 sms set rule)	Specifies an origin IMSI.
orig-sme (cs7 sms set rule)	Specifies an origin SME.
orig-sme-table (cs7 sms set rule)	Specifies an SMS table of origin SME addresses (address-table).
pid (cs7 sms set rule)	Specifies a protocol identifier (TP-PID).
result (cs7 sms set rule)	Specifies a result.
ruleset (cs7 sms ansi41 smsnot)	Specifies a rule within a ruleset.

To specify the address of the origin short message entity (SME) within an SMS operation, use the **orig-sme** command in cs7 mlr ruleset rule configuration mode. To remove the specification, use the **no** form of this command.

orig-sme {*** | *address*} [**exact**] [**min-digits** *min*] [**max-digits** *max*] [*orig-sme-addr-type*]

no orig-sme

Syntax Description

*	Matches all addresses.
<i>address</i>	When the rule operation is sms-mo, <i>address</i> is an address string of 1 to 20 hexadecimal characters. When the rule operation is sms-mt, <i>address</i> is an address string of 1 to 16 hexadecimal characters. The string is not input in BCD-String format, but in normal form. The string always carries an implicit wildcard (*) at the end of the string, allowing only the prefix of a range of addresses to be specified.
exact	(Optional) The previously specified <i>address</i> should be matched only if the number of digits and the digit values match exactly. If exact is not specified, <i>address</i> carries an implicit wildcard (*) at the end of the string, allowing a match on the string as a prefix (range of addresses).
min-digits	(Optional) Specifies the minimum number of digits in the address string.
<i>min</i>	Minimum number of digits in the address string. The default is 1.
max-digits	(Optional) Specifies the maximum number of digits in the address string.

<i>max</i>	Maximum number of digits in the address string. The default is the length of the address string.
<i>orig-sme-addr-type</i>	(Optional) Parameters that identify attributes of the SME address being used to match a rule. <i>orig-sme-addr-type</i> is composed of the following keywords: • [ton <i>ton</i>] The ton keyword specifies the type of number value associated with the SME address. The <i>ton</i> argument is an integer value in the range 0 to 7. • [np <i>np</i>] The np keyword specifies the numbering plan identification value associated with the SME address. The <i>np</i> argument is an integer value in the range 0 to 15.

Defaults

The maximum number of digits in the address string is 1.

Command Modes

cs7 mlr ruleset rule configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines**MLR/SMS rule-matching implementations earlier than ITP release 12.2(25)SW3**

In ITP releases earlier than 12.2(25)SW3, MLR/SMS configuration allows matching of a rule parameter *noa* value with an incoming message as follows:

- If **noa 0** (noa unknown) is specified in a rule parameter, then MLR matches that rule to incoming messages containing the corresponding parameter, regardless of the corresponding parameter's *noa* value.
- If an incoming message contains a parameter with *noa* unknown, then MLR matches that message to a rule for the corresponding parameter, regardless of the rule parameter's *noa* specification.

MLR/SMS rule-matching implementations in ITP release 12.2(25)SW3

Starting with ITP release 12.2(25)SW3, MLR/SMS configuration allows matching of a rule parameter type of number/numbering plan (*ton/np*) value with an incoming message as follows:

- A new **ton** keyword replaces the **noa** keyword. The keywords **ton** and **np** are optional and mutually independent.
- If **ton/np** is specified on a rule parameter, then MLR matches that rule to only those incoming messages containing the exact *ton/np* value in the corresponding parameter.
- If **ton/np** is not specified on a rule parameter, then MLR matches that rule to incoming messages containing the corresponding parameter, regardless of the *ton/np* value received.

For the **sms-mo** operation, **orig-sme** identifies from the SM-RP-OA field within the GSM MAP layer.

For the **sms-mt** operation, **orig-sme** identifies the SM-TP-OA field within the SMS user information field.

Table 33 **Orig-SME by Operation**

	Length in hex digits	No <i>orig-sme-addr-type</i>	<i>orig-sme-addr-type</i> specified
sms-mo	1–20	Defaults to digit string matching only.	specific np/ton
sms-mt	1–20	Defaults to digit string matching only.	specific np/ton
smdpp	1–20	Priority digit string matching based on the following order: SMS_OriginalOriginationAddress SMS_OriginationAddress MIN IMSI SCCP CgPA (RI=GT only)	min = MIN parameter only imsi = IMSI parameter only np/ton = full address matching based on the parameter order: SMS_OriginalOriginationAddress SMS_OriginationAddress

Examples

The following example shows how to specify the address of the origin SME:

```
cs7 mlr ruleset ruleset1
rule 10 sms-mo
  dest-sme 1234
  orig sme 60920025
  result gt 9991117777
```

Related Commands

Command	Description
match-unknown-ton-np (cs7 mlr ruleset rule)	Specifies that messages with unknown ton/np values match the corresponding address parameters, regardless of the rule's configured ton/np values.
rule (cs7 mlr ruleset)	Specifies the rules for a routing trigger within a multilayer ruleset table and enables cs7 mlr ruleset rule configuration mode.

orig-sme (cs7 sms set rule)

To specify an origin short message entity (SME), use the **orig-sme** command in cs7 sms set rule configuration mode. To remove the configuration, use the **no** form of this command.

orig-sme { * | *address* } [**exact**] | [**min-digits** *min*] | [**max-digits** *max*] [*orig-sme-addr-type*]

no orig-sme

Syntax Description	
*	Matches all addresses.
<i>address</i>	SMSC Address or MSISDN, 1 to 16 hexadecimal digits.
exact	Configured address must match orig-imsi exactly.
min-digits	(Optional) Specifies the minimum number of digits in the address string.
<i>min</i>	Minimum number of digits in the address string. The default is 1.
max-digits	(Optional) Specifies the maximum number of digits in the address string.
<i>max</i>	Maximum number of digits in the address string. The default is the length of the address string.
<i>orig-sme-addr-type</i>	(Optional) Parameters that identify attributes of the SME address being used to match a rule. The <i>orig-sme-addr-type</i> is composed of the following keywords: [ton <i>ton</i>] The ton keyword specifies the type of number value associated with the SME address. The <i>ton</i> argument is an integer value in the range 0 to 7. [np <i>np</i>] The np keyword specifies the numbering plan identification value associated with the SME address. The <i>np</i> argument is an integer value in the range 0 to 15.

Defaults None.

Command Modes cs7 sms set rule configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines **MLR/SMS rule-matching implementations earlier than ITP release 12.2(25)SW3**
 In ITP releases earlier than 12.2(25)SW3, MLR/SMS configuration allows matching of a rule parameter noa value with an incoming message as follows:

- If **noa 0** (noa unknown) is specified in a rule parameter, then SMS matches that rule to incoming messages containing the corresponding parameter, regardless of the corresponding parameter's noa value.
- If an incoming message contains a parameter with noa unknown, then SMS matches that message to a rule for the corresponding parameter, regardless of the rule parameter noa specification.

MLR/SMS rule-matching implementations in ITP release 12.2(25)SW3

Starting with ITP release 12.2(25)SW3, MLR/SMS configuration allows matching of a rule parameter type of number/numbering plan (ton/np) value with an incoming message as follows:

- A new **ton** keyword replaces the **noa** keyword. The keywords **ton** and **np** are optional and mutually independent.
- If **ton/np** is specified on a rule parameter, then SMS matches that rule to only those incoming messages containing the exact ton/np value in the corresponding parameter.
- If **ton/np** is not specified on a rule parameter, then SMS matches that rule to incoming messages containing the corresponding parameter, regardless of the ton/np value received.

Examples

The following example shows how to specify an SMS ruleset named SMS-RULES, a rule index of 20, and an origin SME matching all addresses:

```
cs7 sms ruleset SMS-RULES
rule 20 sms-mo
  orig-sme *
  result block
```

Related Commands

Command	Description
cgpa (cs7 mlr trigger)	Tests the availability of CDR service queue as the input condition of the rule.
cs7 sms ruleset	Specifies a ruleset.
dest-sme (cs7 mlr ruleset rule)	Specifies an application destination port number.
dest-sme (cs7 sms set rule)	Specifies a destination short message entity.
dest-sme-table (cs7 sms set rule)	Specifies an SMS table of destination SME addresses.
dest-smsc (cs7 sms set rule)	Specifies a destination SMSC.
match-unknown-ton-np (cs7 sms set rule)	Specifies that messages with unknown TON/NP will be a match to the corresponding address parameters regardless of the rule's configured TON/NP.
orig-imsi (cs7 sms set rule)	Specifies an origin IMSI.
orig-imsi-table (cs7 sms set rule)	Specifies an SMS table of origin IMSI addresses (address-table).
orig-sme-table (cs7 sms set rule)	Specifies an SMS table of origin SME addresses (address-table).
pid (cs7 sms set rule)	Specifies a protocol identifier (TP-PID).

Command	Description
result (cs7 sms set rule)	Specifies a result.
ruleset (cs7 sms ansi41 smsnot)	Specifies a rule within a ruleset.

orig-sme-table (cs7 mlr ruleset rule)

To specify a table of origin SME addresses that will be used to find the desired routing destination, use the **orig-sme-table** command in cs7 mlr ruleset rule configuration mode. To remove the configuration, use the **no** form of this command.

orig-sme-table *table-name* [**ton** *ton-value*] [**np** *np-value*]

no orig-sme-table *table-name* [**ton** *ton-value*] [**np** *np-value*]

Syntax Description

<i>table-name</i>	Identifies the name of a previously defined MLR address table to be used when searching with the orig-sme-table routing command. The name is specified as a character string with a maximum of 12 characters.
ton	Specifies a type of number.
<i>ton-value</i>	Valid range is 0 to 7.
np	Specifies a numbering plan identification value.
<i>np-value</i>	Valid range is 0 to 15.

Defaults

None.

Command Modes

cs7 mlr ruleset rule configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

MLR/SMS rule-matching implementations earlier than ITP release 12.2(25)SW3

In ITP releases earlier than 12.2(25)SW3, MLR/SMS configuration allows matching of a rule parameter noa value with an incoming message as follows:

- If **noa 0** (noa unknown) is specified in a rule parameter, then MLR matches that rule to incoming messages containing the corresponding parameter, regardless of the corresponding parameter's noa value.
- If an incoming message contains a parameter with noa unknown, then MLR matches that message to a rule for the corresponding parameter, regardless of the rule parameter's noa specification.

MLR/SMS rule-matching implementations in ITP release 12.2(25)SW3

Starting with ITP release 12.2(25)SW3, MLR/SMS configuration allows matching of a rule parameter type of number/numbering plan (ton/np) value with an incoming message as follows:

- A new **ton** keyword replaces the **noa** keyword. The keywords **ton** and **np** are optional and mutually independent.

- If **ton/np** is specified on a rule parameter, then MLR matches that rule to only those incoming messages containing the exact ton/np value in the corresponding parameter.
- If **ton/np** is not specified on a rule parameter, then MLR matches that rule to incoming messages containing the corresponding parameter, regardless of the ton/np value received.

The **orig-sme-table** command is valid for smdpp, sms-mo, and sms-mt rule operations. If the address-table lookup finds a match and returns a result, it may only be used if no other routing parameters are defined on this rule. If more than one parameter is configured in a rule, then the result specified under the rule is used.

The **dest-sme-table**, **orig-imsi-table**, and **orig-sme-table** rule commands accept either an SMS address table name *or* an MLR address table name. This ability is primarily for customers who want the SMS-MO Proxy functionality. The address table names are unique between FDA and MLR. You can enter an MLR address table name for an SMS rule parameter. However, MLR cannot reference SMS address tables.

If an incoming message matches an SMS rule that references an MLR address table, then any MLR address table result is mapped to an SMS result:

- BLOCK, PC, and PCSSN results map from MLR to SMS.
 - For result groups, the MLR result group name is mapped to an SMS result group name.
 - If the SMS result group is not configured, then the result specified on the rule is used.
- AS and CONTINUE results are not valid in SMS. For these cases, the result specified on the rule is used. If no result is specified, the result on the rule is used (the same as with MLR).

If multiple rule parameters are configured for a rule, then the rule result will be used (rather than a result specified in the address table).

If the result type specified within the table is valid, it is used. Otherwise, the result in the rule is used.

For all tables, the ton and np must match before the table is accessed.

Examples

The following example shows how to specify an SMS ruleset named ruleset1, a rule index of 20, and a table of origin SME addresses named tbl1:

```
cs7 mlr ruleset ruleset1
rule 20 sms-mo
  orig-sme-table tbl1
  result block
```

Related Commands

Command	Description
match-unknown-ton-np (cs7 mlr ruleset rule)	Specifies that messages with unknown TON/NP will be a match to the corresponding address parameters regardless of the rule's configured TON/NP.
rule (cs7 mlr ruleset)	Specifies the rules for a routing trigger within a multilayer ruleset table and enables cs7 mlr ruleset rule configuration mode.

orig-sme-table (cs7 sms set rule)

To specify an SMS table of origin SME addresses, use the **orig-sme-table** command in cs7 sms set rule configuration mode. To remove the configuration, use the **no** form of this command.

orig-sme-table *table-name* [**ton** *ton-value*] [**np** *np-value*]

no orig-sme-table *table-name* [**ton** *ton-value*] [**np** *np-value*]

Syntax Description

<i>table-name</i>	Address table name.
ton	Specifies a type of number.
<i>ton-value</i>	Valid range is 0 to 7.
np	Specifies a numbering plan identification value.
<i>np-value</i>	Valid range is 0 to 15.

Defaults

None.

Command Modes

cs7 sms set rule configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

MLR/SMS rule-matching implementations earlier than ITP release 12.2(25)SW3

In ITP releases earlier than 12.2(25)SW3, MLR/SMS configuration allows matching of a rule parameter noa value with an incoming message as follows:

- If **noa 0** (noa unknown) is specified in a rule parameter, then SMS matches that rule to incoming messages containing the corresponding parameter, regardless of the corresponding parameter's noa value.
- If an incoming message contains a parameter with noa unknown, then SMS matches that message to a rule for the corresponding parameter, regardless of the rule parameter's noa specification.

MLR/SMS rule-matching implementations in ITP release 12.2(25)SW3

Starting with ITP release 12.2(25)SW3, MLR/SMS configuration allows matching of a rule parameter type of number/numbering plan (ton/np) value with an incoming message as follows:

- A new **ton** keyword replaces the **noa** keyword. The keywords **ton** and **np** are optional and mutually independent.
- If **ton/np** is specified on a rule parameter, then SMS matches that rule to only those incoming messages containing the exact ton/np value in the corresponding parameter.

- If **ton/np** is not specified on a rule parameter, then SMS matches that rule to incoming messages containing the corresponding parameter, regardless of the ton/np value received.

The **dest-sme-table**, **orig-imsi-table**, and **orig-sme-table** rule commands accept either an SMS address table name *or* an MLR address table name. This ability is primarily for customers who want the SMS-MO Proxy functionality. The address table names are unique between DSMR and MLR. You can enter an MLR address table name for an SMS rule parameter. However, MLR cannot reference SMS address tables.

If an incoming message matches an SMS rule that references an MLR address table, then any MLR address table result is mapped to an SMS result:

- BLOCK, PC, and PCSSN results map from MLR to SMS.
 - For result groups, the MLR result group name is mapped to an SMS result group name.
 - If the SMS result group is not configured, then the result specified on the rule is used.
- AS and CONTINUE results are not valid in SMS. For these cases, the result specified on the rule is used. If no result is specified, the result on the rule is used (the same as with MLR).

If multiple rule parameters are configured for a rule, then the rule result will be used (rather than a result specified in the address table).

If the result type specified within the table is valid, it is used. Otherwise, the result in the rule is used.

For all tables, the ton and np must match before the table is accessed.

Examples

The following example shows how to specify an SMS ruleset named SMS-RULES, a rule index of 20, and an SMS table of origin SME addresses named BLACKLIST:

```
cs7 sms ruleset SMS-RULES
rule 20 sms-mo
  orig-sme-table BLACKLIST
  result block
```

Related Commands

Command	Description
cgpa (cs7 mlr trigger)	Tests the availability of the CDR service queue as the input condition of the rule.
cs7 sms ruleset	Specifies a ruleset.
dest-sme (cs7 mlr ruleset rule)	Specifies an application destination port number.
dest-sme (cs7 sms set rule)	Specifies a destination short message entity (SME).
dest-sme-table (cs7 sms set rule)	Specifies an SMS table of destination SME addresses.
dest-smsc (cs7 sms set rule)	Specifies a destination SMSC.
match-unknown-ton-np (cs7 sms set rule)	Specifies that messages with unknown TON/NP will be a match to the corresponding address parameters regardless of the rule's configured TON/NP.
orig-imsi (cs7 sms set rule)	Specifies an origin IMSI.
orig-imsi-table (cs7 sms set rule)	Specifies an SMS table of origin IMSI addresses (address-table).
orig-sme (cs7 sms set rule)	Specifies an origin SME.

Command	Description
pid (cs7 sms set rule)	Specifies a protocol identifier (TP-PID).
result (cs7 sms set rule)	Specifies a result.
ruleset (cs7 sms ansi41 smsnot)	Specifies a rule within a ruleset.

orig-smsc (cs7 mlr ruleset rule)

To specify the originating service center address, use the **orig-smsc** command in cs7 mlr ruleset rule configuration mode. To remove the specification, use the **no** form of this command.

```
orig-smsc { * | address } [exact] | [min-digits min] | [max-digits max] [addr-type]
```

```
no orig-smsc
```

Syntax Description

*	Matches all addresses.
<i>address</i>	Address of 1 to 20 hexadecimal digits.
<i>addr-type</i>	(Optional) Parameters that identify attributes of the SMSC address being used to match a rule. If not specified, the address defaults to an SMSC address string specifying an E.164/telephony address with international scope. <i>addr-type</i> is composed of the following keywords: - The noa keyword specifies the nature of address value associated with the SMSC address. Messages received with an unknown (0) value will match any nonzero noa value specified. - The <i>noa</i> argument is an integer value in the range 0 to 7. - The np keyword specifies the numbering plan identification value associated with the SMSC address. Messages received with an unknown (0) value will match any nonzero np value specified. - The <i>np</i> argument is an integer value in the range 0 to 15.
exact	(Optional) Configured address must match dest-sme exactly.
min-digits	(Optional) Specifies the minimum number of digits in the address string.
<i>min</i>	Minimum number of digits in the address string. The default is 1.
max-digits	(Optional) Specifies the maximum number of digits in the address string.
<i>max</i>	Maximum number of digits in the address string. The default is the length of the address string.

Defaults

If not specified, the *addr-type* address defaults to an E.164/telephony address with international scope. The maximum number of digits in the address string is 1.

Command Modes

cs7 mlr ruleset rule configuration

Command History

Release	Modification
12.2(18)SW	This command was introduced.

Usage Guidelines

The **orig-smsc** command is used to specify the address of the originating service center (SM-RP-OA field within GSM) within an SMS-MT operation. This parameter is part of the rule used to match this route.

**Note**

The originating SMSC address might also be present in the SCCP CgPA. If so, the routing trigger might already contain the destination SMSC address; the address need not be specified on the rule.

For the **sri-sm** operation, **orig-smsc** matches the originating service center address found within the GSM MAP layer.

Examples

The following example shows how to specify the originating service center address:

```
cs7 mlr ruleset ruleset1
rule 20 sms-mt
  orig-smsc 1111
result block
```

Related Commands

Command	Description
rule (cs7 mlr ruleset)	Specifies the rules for a routing trigger within a multilayer ruleset table and enables cs7 mlr ruleset rule configuration mode.

orig-smsc (cs7 mlr modify-profile)

To modify the originating service center address, use the **orig-smsc** command in cs7 mlr modify-profile configuration mode. To remove the specification, use the **no** form of this command.

orig-smsc [**prefix** {*prefix-remove-num* | *}]{*prefix-add-digits* | *}] [**ton** *new-ton*] [**np** *new-np*]

no orig-smsc [**prefix** {*prefix-remove-num* | *}]{*prefix-add-digits* | *}] [**ton** *new-ton*] [**np** *new-np*]

Syntax Description		
prefix		Specifies that prefix modification is to be performed on the address.
<i>prefix-remove-num</i>		An integer in the range of 1 to 38 that defines the number of prefix digits to remove from the address. If no prefix digits are to be removed, then the asterisk (*) should be specified. To replace the entire address, specify that all of the digits are to be removed.
<i>prefix-add-digits</i>		A string of 1 to 38 hexadecimal digits to add to the beginning of the address. If no digits are added, then the asterisk (*) should be specified in this field. If the number of digits in the modified address exceeds 38 digits, then the address modification cannot be performed. In this case, the action taken is based on the configured modify-failure command. By default, the packet is discarded.
ton		Indicates a type of number (ton) replacement.
<i>new-ton</i>		An integer in the range of 0 to 7 that defines the new type of number (ton) value for the modified address.
np		Indicates a numbering plan (np) replacement.
<i>new-np</i>		An integer in the range of 0 to 15 that defines the new numbering plan (np) value for the modified address.

Command Modes cs7 mlr modify-profile configuration

Command History

12.2(18)IXC	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines Using **orig-smsc**, you can modify the address digits, the type of number (ton), and the numbering plan (np).

You can configure prefix-based address modification or a replacement address. For prefix-based address translation, you configure the number of prefix digits that will be removed from the address and the digit string that should be prefixed to the address. Specifying an asterisk (*) for the number of prefix digits indicates that no prefix digits should be removed. Specifying an asterisk (*) for the digit string indicates that no prefix digits are prefixed to the address string. To replace the entire address, you should specify the maximum value for the number of prefix digits to remove. If the resulting modified address exceeds the maximum allowed number of digits, then MLR does not modify the packet and discards it by default. You can optionally configure the desired action for failed modifications using the **modify-failure** command within the MLR options submenu.

Examples

The following example shows how to modify the originating service center address:

```
cs7 mlr modify-profile SRISM gsm-map sri-sm
  orig-smsc prefix 2 351
  cgpa gt prefix 2 351
```

Related Commands

Command	Description
cs7 mlr modify-profile	Specifies an MLR modification profile.
modify-failure (mlr options)	Specifies the desired action when MLR packet modification fails.

outbound (config-gws-as)

To configure a screening of outbound messages, use the **outbound** command in gws as configuration mode. To remove the configuration, use the **no** form of this command.

```
outbound [logging type {allow | block | rate-limit | both} {silent | file [verbose] | console
[verbose] | file [verbose] console [verbose]}] result {action action-set-name | table
table-name}
```

```
no outbound
```

Syntax Description	
logging	(Optional) Enables logging.
type	Specifies logging type.
allow	Messages allowed for further processing.
block	Messages blocked.
rate-limit	Logs the number of MSUs discarded because of a configured rate limit.
both	Allowed and blocked messages.
silent	Messages are screened without logging.
file	Log is copied to a file.
verbose	(Optional) The packet (up to 40 bytes) is printed to the file and/or displayed on the console.
console	Log is displayed on the console.
result	Specifies the next step.
action	Specifies that the next step is an action set.
<i>action-set-name</i>	Name of the action set in the next step. Valid names may not exceed 12 alphanumeric characters.
table	Specifies that the next step is a table.
<i>table-name</i>	Name of the table in the next step.

Defaults The default screening is silent.

Command Modes gws as configuration

Command History	Release	Modification
	12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.
	12.2(33)IRG 12.4(15)SW7	The rate-limit keyword was added.

Examples

The following example shows how to configure outbound screening on an AS named as2:

```
cs7 instance 0 gws as name as2
outbound result action ALLOW
```

The following example shows how to configure inbound and outbound default screening for all ASes:

```
cs7 instance 0 gws as default
inbound logging type block file console verbose result table SIO0
outbound result action BLOCK
```

Related Commands

Command	Description
show cs7 gws as	Displays ITP gateway screening information for the AS.

outbound (config-gws-ls)

To configure screening of outbound messages, use the **outbound** command in gws linkset configuration mode. To remove the configuration, use the **no** form of this command.

```
outbound [logging type {allow | block | rate-limit | both} {silent | file [verbose] | console
[verbose] | file [verbose] console [verbose]}] result {action action-set-name | table
table-name}
```

```
no outbound
```

Syntax Description	
logging	(Optional) Enables logging.
type	Specifies logging type.
allow	Messages allowed for further processing.
block	Messages blocked.
rate-limit	Logs the number of MSUs discarded because of a configured rate limit.
both	Allowed and blocked messages.
silent	Messages are screened without logging.
file	Log is copied to a file.
verbose	(Optional) The packet (up to 40 bytes) is printed to the file and/or displayed on the console.
console	Log is displayed on the console.
result	Specifies the next step.
action	Specifies that the next step is an action set.
<i>action-set-name</i>	Name of the action set in the next step. Valid names may not exceed 12 alphanumeric characters.
table	Specifies that the next step is a table.
<i>table-name</i>	Name of the table in the next step.

Defaults The default screening is silent.

Command Modes gws linkset configuration

Command History	Release	Modification
	12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.
	12.2(33)IRG 12.4(15)SW7	The rate-limit keyword was added.

Examples

The following example shows how to configure inbound and outbound screening:

```
cs7 instance 0 gws linkset name to_morehead1
inbound result table opcttc1
outbound result action ALLOW
```

Related Commands

Command	Description
show cs7 gws linkset	Displays ITP gateway screening information for the linkset.

pam (cs7 mlr ruleset rule)

To configure a reference to an existing PAM table for an MLR ruleset rule, use the **pam** command in the cs7 mlr ruleset rule configuration mode. To remove the configuration, use the **no** form of this command.

pam *pam-name*

no pam *pam-name*

Syntax Description	pam	The keyword indicating a PAM table is being referenced.
	<i>pam-name</i>	The identifying name of an existing PAM table.

Defaults	None.

Command Modes	cs7 mlr ruleset rule configuration

Command History	Release	Modification
	12.4(15)SW5 12.2(33)IRE	This command was introduced.

Usage Guidelines	None.

Examples Using the **show cs7 mlr config** command, the following example shows the configuration of a reference to the PAM table beta under the MLR ruleset alpha.

```
cs7 instance 0 mlr ruleset alpha
rule 1 gsm-map sms-mo default
pam beta
```

Using the **show cs7 mlr ruleset** command, the following example also displays the PAM table beta under the MLR ruleset alpha.

```
Name:      alpha      Instance:0  Protocol: n/a
Rule       Operation   Protocol   Matches   pam
-----
1  sms-mo             gsm-map           0    beta
```

Related Commands	Command	Description
	cgpa (cs7 pam)	Configures one cgpa entry in the PAM table.
	cdpa (cs7 pam)	Configures one cdpa entry in the PAM table.
	opc	Configures an originating point code entry in the PAM table.

Command	Description
dpc	Configures a destination point code entry in the PAM table.
modify-failure (pam)	Specifies the desired action when the PAM table packet modification fails.
cs7 gws action-set	Defines gateway screening action sets that may include a PAM table.
gta asname	Creates or modifies a GTA entry that translates to an M3UA or SUA application server name. The GTA entry may include a PAM table.

path-retransmit (cs7 asp)

To configure the maximum number of path retransmissions on a remote address for the association, use the **path-retransmit** *cs7 asp* submode command. To disable the configuration, use the **no** form of this command.

path-retransmit *max-retries*

no path-retransmit *max-retries*

Syntax Description	<i>max-retries</i>	Maximum number of packet and keepalive retries before the corresponding destination address is marked inactive. The range is 2 to 10 retries. The default number is the value specified under the local port instance.

Defaults	The maximum number of retries is the value specified under the local port instance.

Command Modes	cs7 asp submode

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples	The following example shows how to set the number of path retransmit retries to 10:

```
cs7 asp ASP1
  path-retransmit 10
```

Related Commands	Command	Description
	cs7 asp	Specifies an application server process (ASP) and enables cs7 asp submode.
	show cs7 asp	Displays ASP statistics.

path-retransmit (cs7 link)

To configure path retransmissions on a remote peer address, use the **path-retransmit** cs7 link submode command. To disable the configuration, use the **no** form of this command.

path-retransmit *max-retries*

no path-retransmit *max-retries*

Syntax Description	<i>max-retries</i> Maximum number of packet and keepalive retries before the corresponding destination address is marked inactive. The range is 2 to 10 retries. The default is 4 retries.							
Defaults	4 retries							
Command Modes	cs7 link submode							
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>12.2(18)IXA</td><td rowspan="3">This command was introduced.</td></tr><tr><td>12.4(11)SW</td></tr><tr><td>12.2(33)IRA</td></tr></table>		Release	Modification	12.2(18)IXA	This command was introduced.	12.4(11)SW	12.2(33)IRA
Release	Modification							
12.2(18)IXA	This command was introduced.							
12.4(11)SW								
12.2(33)IRA								
Usage Guidelines	The path-retransmit command specifies the number of packet retries before the destination address is deemed unreachable. The number of path-retransmits multiplied by the retransmission timer ultimately controls how fast an alternate address becomes the primary path for multihomed nodes. This relationship suggests the RTO parameters and the path-retransmit command should be considered together. Configuring the default RTO values and a default path retransmit value of 4 allows a multihomed node to switch to an alternate destination address within 4 seconds.							
Examples	The following example shows how to set the number of path retransmit retries to 10: <pre>cs7 linkset michael 10.1.1 link 0 sctp 172.18.44.147 7000 7000 path-retransmit 10</pre>							
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>show cs7 m2pa</td><td>Displays M2PA statistics.</td></tr></table>		Command	Description	show cs7 m2pa	Displays M2PA statistics.		
Command	Description							
show cs7 m2pa	Displays M2PA statistics.							

path-retransmit (cs7 m2pa profile)

To configure path retransmissions on a remote peer address, use the **path-retransmit** cs7 m2pa profile command. To disable the configuration, use the **no** form of this command.

path-retransmit *max-retries*

no path-retransmit *max-retries*

Syntax Description	<i>max-retries</i>	Maximum number of packet and keepalive retries before the corresponding destination address is marked inactive. The range is 2 to 10 retries. The default is 4 retries.

Defaults	4 retries

Command Modes	cs7 m2pa profile configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	The path-retransmit command specifies the number of packet retries before the destination address is deemed unreachable. The number of path-retransmits multiplied by the retransmission timer ultimately controls how fast an alternate address becomes the primary path for multihomed nodes. This relationship suggests the RTO parameters and the path-retransmit command should be considered together. Configuring the default RTO values and a default path retransmit value of 4 allows a multihomed node to switch to an alternate destination address within 4 seconds.

Examples	The following example shows how to define a profile named m2parfc. The profile supports M2PA RFC, specifies the path-retransmit command, and applies to all the links in the linkset named to_nyc.

```
cs7 profile m2parfc
 m2pa
  path-retransmit 10
.
.
.
cs7 linkset to_nyc
 profile m2parfc
```

Related Commands	Command	Description
	m2pa	Specifies M2PA parameters in a CS7 profile.

path-retransmit (cs7 m3ua)

To configure the maximum number of path retransmissions on a remote ASP/ mated-SG address to be used when a new SCTP association is started with the local port, use the **path-retransmit** cs7 m3ua submode command. To disable the configuration, use the **no** form of this command.

path-retransmit *max-retries*

no path-retransmit *max-retries*

Syntax Description	<i>max-retries</i> Maximum number of path retries. The range is 2 to 10 retries. The default is 4 retries.							
Defaults	4 retries							
Command Modes	cs7 m3ua submode							
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>12.2(18)IXA</td><td rowspan="3">This command was introduced.</td></tr><tr><td>12.4(11)SW</td></tr><tr><td>12.2(33)IRA</td></tr></table>		Release	Modification	12.2(18)IXA	This command was introduced.	12.4(11)SW	12.2(33)IRA
Release	Modification							
12.2(18)IXA	This command was introduced.							
12.4(11)SW								
12.2(33)IRA								
Examples	The following example shows how to set the number of path retransmit retries to 10: <pre>cs7 m3ua 2905 local-ip 4.4.4.4 path-retransmit 10</pre>							
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>cs7 m3ua</td><td>Specifies the local port number for M3UA and enables cs7 m3ua submode.</td></tr></table>		Command	Description	cs7 m3ua	Specifies the local port number for M3UA and enables cs7 m3ua submode.		
Command	Description							
cs7 m3ua	Specifies the local port number for M3UA and enables cs7 m3ua submode.							

path-retransmit (cs7 mated-sg)

To configure the maximum number of path retransmissions on a remote address for the association, use the **path-retransmit** *cs7 mated-sg* submode command. To disable the configuration, use the **no** form of this command.

path-retransmit *max-retries*

no path-retransmit *max-retries*

Syntax Description	<i>max-retries</i>	Maximum number of packet and keepalive retries before the corresponding destination address is marked inactive. The range is 2 to 10 retries. The default is the value specified under the local port instance.

Defaults	The default maximum number of retries is the value specified under the local port instance.

Command Modes	cs7 mated-sg submode

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples	The following example shows how to set the number of path retransmit retries to 10:

```
cs7 mated-sg BLUE 2905
  path-retransmit 10
```

Related Commands	Command	Description
	cs7 mated-sg	Configures a connection to a mated SG and enables cs7 mated-sg submode.
	show cs7 mated-sg	Displays mated-SG statistics.

path-retransmit (cs7)

To configure the maximum number of path retransmissions on a remote ASP/ mated-SG address to be used when a new SCTP association is started with the local port, use the **path-retransmit cs7** submode command. To disable the configuration, use the **no** form of this command.

path-retransmit *max-retries*

no path-retransmit *max-retries*

Syntax Description	<i>max-retries</i> Maximum number of path retries. The range is 2 to 10 retries. The default is 4 retries.	
Defaults	4 retries	
Command Modes	cs7 submode	
Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	
Examples	The following example shows how to set the number of path retransmit retries to 10: cs7 5000 local-ip 4.4.4.4 path-retransmit 10	
Related Commands	Command	Description
	cs7 sgmp	Specifies the local port number for and enables cs7 submode.

path-retransmit (cs7 sua)

To configure the maximum number of path retransmissions on a remote ASP/ mated-SG address to be used when a new SCTP association is started with the local port, use the **path-retransmit** cs7 sua submode command. To disable the configuration, use the **no** form of this command.

path-retransmit *max-retries*

no path-retransmit *max-retries*

Syntax Description	<i>max-retries</i>	Maximum number of path retries. The range is 2 to 10 retries. The default is 4 retries.

Defaults	4 retries

Command Modes	cs7 sua submode

Command History	Release	Modification
	12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.

Examples The following example shows how to set the number of path retransmit retries to 10:

```
cs7 sua 15000
local-ip 4.4.4.4
path-retransmit 10
```

Related Commands	Command	Description
	cs7 sua	Specifies the local port number for SUA and enables cs7 sua submode.

pc (cs7 gtt application group)

To add or change a point code and optional subsystem number in the application group, use the **pc** command in cs7 gtt application group submode. To remove the point code and optional subsystem number, use the **no** form of this command.

```
[instance instance-number] pc pc [ssn ssn] {cost {gt [ntt ntt] | pcssn} [rate-limit rate] | wf {gt [ntt ntt] | pcssn}} [sccp-allow-pak-conv number]
```

```
no [instance instance-number] pc pc [ssn ssn]
```

Syntax Description		
instance		Specifies an instance.
<i>instance-number</i>		Instance number.
<i>pc</i>		Point code, in the form zone.region.sp. The specified point code must represent a real point code, not an alias point code.
ssn		Specifies a subsystem number.
<i>ssn</i>		Subsystem number. Valid range is 2 to 255.
<i>cost</i>		Index value (1–64) specifying the priority of the AS name within the application group.
gt		Sets the routing indicator to route on the global title.
ntt		Configures a new translation type value to be set within the called party address global title selector data. The keyword is valid only when the gt keyword is specified.
<i>ntt</i>		New translation type value in the range 0 to 255.
pcssn		Sets the routing indicator to route on the point code and subsystem number.
rate-limit		Specifies the traffic-rate limitation to this PC/SSN. The over-flow traffic will be routed to higher cost DPC/ASNAME. If not specified, the PC does not have a rate-limit.
<i>rate</i>		An integrate value specifying the traffic rate. Valid range is 1 to 4294967296 MSU/sec.
<i>wf</i>		Weighing factor. Any items added to the group require a cost if the destination for the multiplicity command is specified as cgpa or wrr .
sccp-allow-pak-conv		Enables conversion of SCCP packet between XUDT/XUDTS and UDT/UDTS.
<i>number</i>		1 specifies XUDT/XUDTS to UDT/UDTS conversion 2 specifies UDT/UDTS to XUDT/XUDTS conversion 3 specifies NO CONVERSION

Defaults None.

Command Modes cs7 gtt application group submode

Command History	Release	Modification
	12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.
	12.4(15)SW4 12.2(33)IRD	The rate limit keyword and <i>rate</i> argument were introduced.
	12.4(15)SW9 12.2(33)IRI	The sccp-allow-pak-conv keyword was added.

Usage Guidelines

The destination in a GTT application group uses the *wf* argument when the **multiplicity** command is configured with the **cgpa** or **wrr** keyword.

The rate-limit parameter is only valid for multiplicity cost mode.

Examples

The following example shows how to specify point code 2.2.2, subsystem number 3, with a cost of 4. The routing indicator is set to route on the point code and subsystem number.

```
pc 1.2.3 ssn 3 4 pcssn
```

Related Commands

Command	Description
cs7 gtt application-group	Specifies a GTT application group.
multiplicity	Specifies a method for selecting a destination in the application group.

pc (cs7 mlr result)

To specify the destination point code, use the **pc** command in cs7 mlr result configuration mode. To remove the specification, use the **no** form of this command.

[instance instance] pc dest-pc [ssn ssn] [order order] [weight weight]

no [instance instance] pc dest-pc [ssn ssn] [order order] [weight weight]

Syntax Description	
instance	(Optional) Indicates the PC/PCSSN result in local or other instance.
<i>instance</i>	(Optional) Instance number. The valid range is 0 to 7. The default instance is 0.
<i>dest-pc</i>	A destination point code in variant-specific point-code format. The specified point code must represent a real point code, not an alias point code.
ssn	(Optional) Specifies a subsystem number to be used along with the point code.
<i>ssn</i>	Subsystem number. Valid range is 2 to 255.
order	Specifies the order in which the results are stored in the result group. Required for (and only present in the CLI for) results in a dest-sme-binding mode. Results in a wrp result group are not able to configure an order parameter.
<i>order</i>	An integer value in the range of 1 to 1000.
weight	(Optional) Specifies the load-balancing weight.
<i>weight</i>	For dest-sme-binding mode, an integer value in the range 1 to 2147483647. The weight value should reflect the relative capacity of the result (smc). This value is used by the dynamic B-address routing algorithm to select a deterministic result (SMSC) based on the message B-address. If not configured, the default <i>weight</i> value is 1. For wrp mode, an integer value in the range of 0 to 10. A value of 10 indicates the resource should be selected 10 times more than a resource assigned a weight of 1. A weight of 0 indicates that the resource should only be used in the event that all nonzero-weighted resources are unavailable. If multiple zero-weighted resources exist, then messages are equally distributed between them if all nonzero-weighted resources fail. If not specified, a default weight of 1 is used.

Defaults

The default load-balancing weight is 1 and the default instance is 0.

Command Modes

cs7 mlr result configuration

Command History	Release	Modification
	12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.
	12.2(18)IXG 12.4(15)SW2 12.2(33)IRB	The instance keyword was added.

Usage Guidelines If multiple zero-weighted resources exist, then messages are equally distributed between them if all nonzero-weighted resources fail. If not specified, a default weight of 1 is used.

Examples The following example shows how to specify three resources in the result group SMS-WEIGHTED. The three resources are identified by point codes and assigned weighted round-robin (WRR) values.

```
cs7 mlr result SMS-WEIGHTED
  pc 3.3.2 weight 1
  pc 3.3.1 weight 2
  pc 3.3.3 weight 5
```

The following example shows how to specify the instance number as 1:

```
cs7 instance 0 mlr result ttt
instance 1 pc 1.11.1 ssn 11
```

Related Commands	Command	Description
	cs7 mlr result	Specifies the name of the MLR result group. The result group contains the list of resources that process traffic to be routed based on multilayer information.
	show cs7 mlr result	Displays multilayer SMS routing result information.

pc-range

To specify a point code range entry in a pc table, use the **pc-range** command in gateway screening table configuration mode. To delete a point code entry, use the **no** form of this command.

pc-range *pc-start* [*pc-end*] **result** { **action** *action-set-name* | **table** *table-name* }

no pc-range *pc-start* [*pc-end*]

Syntax Description

<i>pc-start</i>	Starting pc in the range.
<i>pc-end</i>	(Optional) Ending pc in the range.
result	Specifies the next step.
action	Screens the result by action set.
<i>action-set-name</i>	Action set name. Valid names may not exceed 12 alphanumeric characters.
table	Screens the result by table.
<i>table-name</i>	Table name. Valid names may not exceed 12 alphanumeric characters.

Defaults

None.

Command Modes

gateway screening table configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The **pc-range** command is valid for the following table types: aff-dest, dpc, opc.
Wildcards can be used. Refer to [Table 13 on page 205](#).

Examples

The following example shows how to specify a **pc-range** entry for the OPC1 table:

```
cs7 instance 0 gws table OPC1 type opc action allowed
pc-range 6.6.6 result table PCSSN1
```

Related Commands

Command	Description
cs7 gws table	Configures a gateway screening table.

pc-range ssn

To specify a point code range entry in a pc-ssn table, use the **pc-range ssn** command in gateway screening table configuration mode. To delete a point code, use the **no** form of this command.

pc-range *pc-start* [*pc-end*] **ssn** *ssn* **result** { **action-set** *action-set-name* | **table** *table-name* }

no pc-range ssn *pc-start* [*pc-end*] **ssn** *ssn*

Syntax Description	<i>pc-start</i>	Starting pc in the range.
	<i>pc-end</i>	(Optional) Ending pc in the range.
	ssn	Specifies the subsystem number.
	<i>ssn</i>	Subsystem number. Valid range is 1 to 255.
	result	Specifies the next step.
	action	Screens the result by action set.
	<i>action-set-name</i>	Action set name. Valid names may not exceed 12 alphanumeric characters.
	table	Screens the result by table.
	<i>table-name</i>	Table name. Valid names may not exceed 12 alphanumeric characters.

Defaults None.

Command Modes gateway screening table configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines The **pc-range ssn** command is valid for the following table types: aff-pc-ssn, cdpa-pc-ssn, cgpa-pc-ssn. Wildcards are allowed.

Examples The following example shows how to specify a **pc-range** entry for the OPC1 table:

```
cs7 instance 0 gws table OPC1 type opc action allowed
pc-range 6.6.6 result table PCSSN1
```

Related Commands	Command	Description
	cs7 gws table	Configures a gateway screening table.

peer-timer (cs7 link)

To set the peer timer, use the **peer-timer** command in cs7 link configuration mode. To disable the timer, use the **no** form of this command.

peer-timer {*lssu msec* | **t01** *msec* | **t2** *msec* | **t3** *msec* | **t4e** *msec* | **t4n** *msec* | **t06** *msec* | **t7** *msec*}

no peer-timer {*lssu msec* | **t01** *msec* | **t2** *msec* | **t3** *msec* | **t4e** *msec* | **t4n** *msec* | **t06** *msec* | **t7** *msec*}

Syntax Description		
lssu		LSSU rate timer, the rate at which link status messages are sent. The range is 500 to 30000 milliseconds. The default is 5000 milliseconds. Applies to M2PA RFC links only.
t01 msec		Alignment ready timer. The range is 500 to 60000 milliseconds. The default is 5000 milliseconds if the link is defined as M2PA draft2, and 45000 milliseconds if the link is defined as an M2PA RFC link.
t2		Not aligned timer. The range is 500 to 150000 milliseconds. The default is 60000 milliseconds. Applies to M2PA RFC links only.
t3		Aligned timer. The range is 500 to 60000 milliseconds. The default is 2000 milliseconds. Applies to M2PA RFC links only.
t4e		Emergency proving period timer, the rate at which the emergency proving link status messages are sent. The range is 100 to 5000 milliseconds. The default is 500 milliseconds. Applies to M2PA RFC links only.
t4n		Normal proving period timer, the rate at which the normal proving link status messages are sent. The range is 500 to 60000 milliseconds. The default is 8000 milliseconds. Applies to M2PA RFC links only.
t06		Remote congestion timer. The range is 500 to 12000 milliseconds. The default is 4000 milliseconds.
t7		Excessive delay of acknowledgment timer. The range is 0 to 30000 milliseconds. The default is 0 milliseconds. Applies to M2PA RFC links only.

Defaults See Syntax Description.

Command Modes cs7 link configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples The following example shows how to set the t06 timer to 2000 milliseconds for link 0 in the linkset named to_nyc:

```
cs7 linkset to_nyc 10.1.1
link 0 sctp 172.18.44.147 7000 7000
peer-timer t06 2000
```

Related Commands

Command	Description
cs7 profile	Specifies a set of parameters that can be applied to a linkset.
link (cs7 linkset)	Specifies a link.
show cs7 m2pa	Displays M2PA statistics.

peer-timer (cs7 m2pa profile)

To set the peer timer, use the **peer-timer** command in cs7 m2pa profile configuration mode. To disable the timer, use the **no** form of this command.

peer-timer {*lssu msec* | **t01 msec** | **t2 msec** | **t3 msec** | **t4e msec** | **t4n msec** | **t06 msec** | **t7 msec**}

no peer-timer {*lssu msec* | **t01 msec** | **t2 msec** | **t3 msec** | **t4e msec** | **t4n msec** | **t06 msec** | **t7 msec**}

Syntax Description		
lssu		LSSU rate timer, the rate at which link status messages are sent. The range is 500 to 30000 milliseconds. The default is 5000 milliseconds. Applies to M2PA RFC links only.
t01 msec		Alignment ready timer. The range is 500 to 60000 milliseconds. The default is 5000 milliseconds if the link is defined as M2PA draft2, and 45000 milliseconds if the link is defined as an M2PA RFC link.
t2		Not aligned timer. The range is 500 to 150000 milliseconds. The default is 60000 milliseconds. Applies to M2PA RFC links only.
t3		Aligned timer. The range is 500 to 60000 milliseconds. The default is 2000 milliseconds. Applies to M2PA RFC links only.
t4e		Emergency proving period timer, the rate at which the emergency proving link status messages are sent. The range is 100 to 5000 milliseconds. The default is 500 milliseconds. Applies to M2PA RFC links only.
t4n		Normal proving period timer, the rate at which the normal proving link status messages are sent. The range is 500 to 60000 milliseconds. The default is 8000 milliseconds. Applies to M2PA RFC links only.
t06		Remote congestion timer. The range is 500 to 12000 milliseconds. The default is 4000 milliseconds.
t7		Excessive delay of acknowledgment timer. The range is 0 to 30000 milliseconds. The default is 0 milliseconds. Applies to M2PA RFC links only.

Defaults See Syntax Description.

Command Modes cs7 m2pa profile configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples The following example shows how to define a profile named m2parfc. The profile supports M2PA RFC, configures **peer-timer** settings and **hold-transport** settings, and applies to all the links in the linkset named to_nyc.

```
cs7 profile m2parfc
  m2pa
    peer-timer t1 15000
    peer-timer t2 9000
  .
  .
  .
cs7 linkset to_nyc
  profile m2parfc
```

Related Commands

Command	Description
cs7 profile	Specifies a set of parameters that can be applied to a linkset.
link (cs7 linkset)	Specifies a link.
show cs7 m2pa	Displays M2PA statistics.

pid (cs7 mlr ruleset rule)

To specify a particular protocol identifier (PID) value for an SMS-MO or SMS-MT rule, use the **pid** command in cs7 mlr ruleset rule configuration mode. To remove the specification, use the **no** form of this command.

pid *protocol-id*

no pid *protocol-id*

Syntax Description

<i>protocol-id</i>	An integer in the range 0 to 255.

Defaults

None.

Command Modes

cs7 mlr ruleset rule configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The value of the PID maps to the values specified for the TP-PID SMS parameter. For a complete set of PID values, refer to GSM 03.40.

Examples

The following example shows how to specify a protocol identifier (PID) value:

```
cs7 mlr ruleset ruleset1
rule 10 gsm-map sms-mo
pid 1
dest-sme 1234
orig sme 60920025
result gt 9991117777
```

Related Commands

Command	Description
rule (cs7 mlr ruleset)	Specifies the rules for a routing trigger within a multilayer ruleset table and enables cs7 mlr ruleset rule configuration mode.

pid (cs7 sms set rule)

To specify a protocol identifier (TP-PID), use the **pid** command in cs7 sms set rule configuration mode. To remove the configuration, use the **no** form of this command.

pid *pid-value*

no pid

Syntax Description	<i>pid-value</i>	Protocol identifier integer value. Valid range is 0 to 255.

Defaults	None.

Command Modes	cs7 sms set rule configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples	The following example shows how to specify an SMS ruleset named SMS-RULES, a rule index of 20, and a PID of 25:

```
cs7 sms ruleset SMS-RULES
rule 20 sms-mo
pid 25
result block
```

Related Commands	Command	Description
	cgpa (cs7 mlr trigger)	Tests the availability of the CDR service queue as the input condition of the rule.
	cs7 sms ruleset	Specifies a ruleset.
	dest-sme (cs7 mlr ruleset rule)	Specifies an application destination port number.
	dest-sme (cs7 sms set rule)	Specifies a destination short message entity (SME).
	dest-sme-table (cs7 sms set rule)	Specifies an SMS table of destination SME addresses.
	dest-smsc (cs7 sms set rule)	Specifies a destination SMSC.
	orig-imsi (cs7 sms set rule)	Specifies an origin IMSI.
	orig-imsi-table (cs7 sms set rule)	Specifies an SMS table of origin IMSI addresses (address-table).
	orig-sme (cs7 sms set rule)	Specifies an origin SME.

Command	Description
orig-sme-table (cs7 sms set rule)	Specifies an SMS table of origin SME addresses (address-table).
result (cs7 sms set rule)	Specifies a result.
ruleset (cs7 sms ansi41 smsnot)	Specifies a rule within a ruleset.

ping cs7

To verify that you can reach ITP nodes, use the **ping cs7** EXEC command. To stop the ping, use the **ping cs7** command with the **stop** keyword.

ping cs7 [*instance-number*] [**-opc** *origination-point-code*] [**-duration** *seconds*] [**-ni** *network-indicator*] [**-rate** *MSU-per-second*] [**-size** *bytes*] [**-sls** *value* | **round-robin**] {*destination-point-code* | *host*}

ping cs7 [*instance-number*] **stop** *destination-point-code*

Syntax Description

<i>instance-number</i>	(Optional) ITP instance.
-opc	(Optional) Specifies the secondary pc or the capability pc as the originating pc of the ping. If -opc is not specified, the primary pc is the default originating pc.
<i>origination-point-code</i>	Originating point code. You can specify a secondary pc or a capability pc.
-duration	(Optional) Specifies a ping test duration, in seconds.
<i>seconds</i>	Duration of the ping, in seconds. The default is 1 second.
-ni	(Optional) Specifies a network indicator.
<i>network-indicator</i>	The network indicator. The default is 2.
-rate	(Optional) Specifies a ping message rate in MSU per second.
<i>MSU-per-second</i>	MSU per second.
-size	(Optional) Specifies a test message size, in bytes.
<i>bytes</i>	Ping test message size. The default size is 40 bytes.
-sls	(Optional) Signaling link selector.
<i>value</i>	Signaling link selector value. Valid numbers are 1 to 15. The default is 0.
round-robin	Performs the ping in round-robin order.
<i>destination-point-code</i>	The point code.
<i>host</i>	The hostname.
stop	Stops the ping.

Defaults

The primary point code is the default originating point code. The default of the duration of the ping is 1 second. The network indicator default is 2. The signaling link selector default value is 0.

EXEC

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Examples

The following example shows how to start a 10-second ping to point code 10.44.156:

```
Router# ping cs7 -duration 10 10.44.156
%CS7PING-6-RTT:Q.755 Test 10.44.156:MTP Traffic test rtt 200/200/200
%CS7PING-6-TERM:Q.755 Test 10.44.156:MTP Traffic test terminated
```

The following example shows how to start a ping from the secondary point code 10.10.10 to 10.44.156:

```
ping cs7 -opc 10.10.10 10.44.156
```

The following example shows how to stop a ping to point code 10.44.156:

```
ping cs7 stop 10.44.156
```

Related Commands

Command	Description
cs7 host	Displays the hostname.
show cs7 linkset	Displays linkset information.
show cs7 ping	Displays output from a ping test.

ping-interval

To set the interval between two consecutive ICMP Echo requests, use the **ping-interval** cs7 dcs submode command. To stop the ping, use the **no** form of this command.

ping-interval *sec*

no ping-interval *sec*

Syntax Description	<i>sec</i>	(Optional) Length of time in seconds that defines the interval between pings to the DCS nodes' IP addresses. The time interval range is 0 to 30 seconds. The default interval is 5 seconds.

Defaults	5 seconds

Command Modes	cs7 dcs submode

Command History	Release	Modification
	12.2(18)IXH	This command was introduced.
	12.4(15)SW3	
	12.2(33)IRC	

Usage Guidelines	The source address of ICMP packets is based on the determination by the router. Normally, the source address of ICMP packets is the address of the closest interface to the destination address. This behavior conforms to the selection of source addresses when the customer issues ping commands with the CLI. A <i>sec</i> value of 0 indicates no ping is sent, and that the DCS is shown as always available.

Examples	The following example shows how to configure a ping interval of 5 seconds between the remote IP address and the local IP address:

```
cs7 dcs dcs5
 remote-ip 209.165.201.29 209.165.201.28 3033
 local-ip 1209.165.20127 3033
 ping-interval 5
 timeout-count 3
 udp-checksum
```

Related Commands	Command	Description
	pmp (cs7 linkset)	Turns probeless monitoring on for a linkset.
	pmp (cs7 as)	Turns probeless monitoring on for an AS.
	cs7 dcs-group	Identifies a name to be associated with a DCS group.

Command	Description
cs7 pmp hold-queue	Sets the integer range of a PMP hold queue threshold.
cs 7 dcs	Identifies a name to be associated with a DCS node.
show cs7 pmp	Displays errors and information about the PMP.
show cs7 dcs-group	Displays information about the DCS group.
show cs7 dcs	Displays information about the DCS node.

plan-capacity-rcvd

To configure link receive planning capacity, use the **plan-capacity-rcvd** cs7 link submode command. To remove the configuration, use the **no** form of this command.

plan-capacity-rcvd *bps*

no plan-capacity-rcvd *bps*

Syntax Description

bps Planned capacity in bits per second. The range is 56000 to 2147483647.

Defaults

For links based on Serial or ATM (HSL) technologies, the planned capacity is the physical speed of the link.

Command Modes

cs7 link submode

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

Planned capacity is the maximum amount of expected data to be transmitted on a link. This value is expressed in bits per second. For links based on Serial or ATM (HSL) technologies, the planned capacity is the physical speed of the link. You do not need to specify a planned capacity for these types of links. When a planned capacity is not specified for these types of links, the ifSpeed (from the IF-MIB) is used as the planned capacity.

In the case of SCTP/IP-based links, you cannot directly determine the expected amount of traffic. The design of the IP cloud must consider the traffic from all SS7 links and allocate resources accordingly. To monitor link utilization on these types of links, a planned capacity must be specified.

Examples

The following example shows how to set the receive planning capacity on link 0 to 56000 bps:

```
cs7 linkset michael 10.1.1
link 0 sctp 172.18.44.147 7000 7000
plan-capacity-rcvd 56000
```

Related Commands

Command	Description
cs7 util-abate	Specifies the integer range utilization threshold.
cs7 util-threshold	Specifies the global threshold for link utilization.
plan-capacity-send	Specifies the link send planning capacity.

Command	Description
threshold-rcvd	Specifies the receive threshold for a link.
threshold-send	Specifies the send threshold for a link.

plan-capacity-send

To configure the link send planning capacity, use the **plan-capacity-send** cs7 link submode command. To remove the configuration, use the **no** form of this command.

plan-capacity-send *bps*

no plan-capacity-send *bps*

Syntax Description	<i>bps</i>	Planned capacity in bits per second. The range is 56000 to 2147483647.

Defaults	For links based on Serial or ATM (HSL) technologies, the planned capacity is the physical speed of the link.

Command Modes	cs7 link submode

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	Planned capacity is the maximum amount of expected data to be transmitted on a link. This value is expressed in bits per second. For links based on Serial or ATM (HSL) technologies, the planned capacity is the physical speed of the link. You do not need to specify a planned capacity for these types of links. When a planned capacity is not specified for these types of links, the ifSpeed (from the IF-MIB) is used as the planned capacity.
	In the case of SCTP/IP-based links, you cannot directly determine the expected amount of traffic. The design of the IP cloud must consider the traffic from all SS7 links and allocate resources accordingly. To monitor link utilization on these types of links, a planned capacity must be specified.

Examples	The following example shows how to set the send planning capacity on link 0 to 56000 bps:

```
cs7 linkset michael 10.1.1
link 0 sctp 172.18.44.147 7000 7000
plan-capacity-send 56000
```

Related Commands	Command	Description
	cs7 util-abate	Specifies the integer range utilization threshold.
	cs7 util-threshold	Specifies the global threshold for link utilization.
	plan-capacity-revd	Specifies the link receive planning capacity.

Command	Description
threshold-rcvd	Specifies the receive threshold for a link.
threshold-send	Specifies the send threshold for a link.

pmp (cs7 as)

The probeless monitoring protocol is a proprietary ITP UDP protocol that allows copying sent or received ITP MSUs and then sending them to a data collection server (DCS). To turn on probeless monitoring for an AS, use the **pmp** cs7 as submode command. To turn probeless monitoring off, use the **no** form of this command.

pmp

no pmp

Syntax Description	This command has no arguments or keywords.

Defaults	Probeless monitoring is off.

Command Modes	cs7 as submode

Command History	Release	Modification
	12.4(15)SW3 12.2(33)IRC	This command was introduced.

Usage Guidelines	When probeless monitoring is turned on for an AS, you still have to specify the DCS group under cs7 as submode. When probeless monitoring is turned off at the global configuration level, it overrides the probeless monitoring setting for the AS. When the global probeless monitoring option is on, the probeless monitoring setting for a particular AS governs whether probeless monitoring is on or off for that AS.

Examples	The following example shows how to turn PMP on for an AS:

```
cs7 instance 4 as as1 m3ua
  pmp
  routing-key 2333 444
  asp asp1
  contextid 2
  asp asp2
  contextid 3
  dcs-group dcs-group1 inbound
  dcs-group dcs-group2 outbound
```

Related Commands	Command	Description
	pmp (cs7 linkset)	Turns probeless monitoring on for a linkset.
	cs7 dcs-group	Identifies a name to be associated with a DCS group.

Command	Description
cs7 pmp hold-queue	Sets the integer range of a PMP hold queue threshold.
cs 7 dcs	Identifies a name to be associated with a DCS node.
show cs7 pmp	Displays errors and information about the PMP.
show cs7 dcs-group	Displays information about the DCS group.
show cs7 dcs	Displays information about the DCS node.

pmp (cs7 linkset)

The probeless monitoring protocol is a proprietary ITP UDP protocol that allows copying sent or received ITP MSUs and then sending them to a data collection server (DCS). To turn on probeless monitoring for a linkset, use the **pmp** cs7 linkset submode command. To turn probeless monitoring off, use the **no** form of this command.

pmp

no pmp

Syntax Description	This command has no arguments or keywords.

Defaults	Probeless monitoring is off.

Command Modes	cs7 linkset submode

Command History	Release	Modification
	12.4(15)SW3	This command was introduced.
	12.2(33)IRC	

Usage Guidelines	When probeless monitoring is turned on for a linkset, you still have to specify the DCS group under cs7 linkset submode. When probeless monitoring is turned off at the global configuration level, it overrides the probeless monitoring setting for the linkset. When the global probeless monitoring option is on, the probeless monitoring setting for a particular linkset governs whether probeless monitoring is on or off for that linkset.

Examples	The following example shows how to turn PMP on for a linkset:

```
cs7 instance 0 linkset tojupiter 2.54.0
  accounting
  pmp
  gtt-accounting
  dcs-group polystar all
  link 0 sctp 10.0.90.30 2905 2905
  contextid 1
```

Related Commands	Command	Description
	pmp (cs7 AS)	Turns probeless monitoring on for an AS.
	cs7 dcs-group	Identifies a name to be associated with a DCS group.
	cs7 pmp hold-queue	Sets the integer range of a PMP hold queue threshold.

Command	Description
cs 7 dcs	Identifies a name to be associated with a DCS node.
show cs7 pmp	Displays errors and information about the PMP.
show cs7 dcs-group	Displays information about the DCS group.
show cs7 dcs	Displays information about the DCS node.

point-code (mtp3)

To configure the billing pc-table entry when the pc-table type is MTP3, use the **point-code si** command in billing pc-table submode. To remove the configuration, use the **no** form of this command.

point-code *point-code* **si** *si-number*

no point-code *point-code* **si** *si-number*

Syntax Description	<i>point-code</i>	Point code of table entry
	si	Service indicator
	<i>si-number</i>	Service indicator number

Defaults	None.

Command Modes	billing pc-table submode

Command History	Release	Modification
	12.4(15)SW4	This command was introduced.
	12.2(33)IRD	

Usage Guidelines	This command configures the point code and service indicator to meet the accounting criteria.

Examples	The following example shows how to configure a point code of 1.1.1 and a service indicator of 11:
	<pre>cs7 instance 0 billing pc-table PCTBL_01 mtp3 point-code 1.1.1 si 11</pre>

Command	Description
show cs7 billing configuration	Shows the billing configuration.z
cs7 billing pc-table	Configures a pc-table for the billing account.
cs7 billing options	Configures options for billing.
cs7 billing load	Specifies the billing configuration file to load.

point-code (sccp)

To configure the billing pc-table entry when the pc-table type is SCCP, use the **point-code** command in billing pc-table submenu. To remove the configuration, use the **no** form of this command.

point-code *point-code* [**ssn** *ssn-number*] [**gta** *gta-number* **tt** *tt-number* **gti** *gti-number*] [**np** *np-number*] [**nai** *nai-number*]

no point-code *point-code* [**ssn** *ssn-number*] [**gta** *gta-number* **tt** *tt-number* **gti** *gti-number*] [**np** *np-number*] [**nai** *nai-number*]

Syntax Description

<i>point-code</i>	Point code of table entry
<i>ssn-number</i>	Sub-System Number (0-255)
<i>gta-number</i>	Global Title Address number (1 to 15 hex digits)
<i>tt-number</i>	Translation Type number (0-255)
<i>gti-number</i>	Global Title Indicator number (2 or 4)
<i>np-number</i>	National Plan number (0-15)
<i>nai-number</i>	Nature of Address Indicator number (0-127)

Defaults

None.

Command Modes

billing pc-table submenu

Command History

Release	Modification
12.4(15)SW4	This command was introduced.
12.2(33)IRD	

Usage Guidelines

This command configures the point code and service indicator to meet the accounting criteria.

Examples

The following example shows how to configure a point code of 1.1.1 and a service indicator of 11:

```
cs7 instance 0 billing pc-table PCTBL_02 sccp
point-code 2.2.2 ssn 8 gta 67890 tt 0 gti 4 np 4 nai 2
```

Related Commands

Command	Description
cs7 billing pc-table	Configures a pc-table for the billing account.

Command	Description
cs7 billing options	Configures options for billing.
cs7 billing load	Specifies the billing configuration file to load.

post-gtt-address-conversion

After you have defined a GTT address conversion table, you can apply the table on a GTT selector basis. To specify the global title address conversion table to apply after performing local global title translation, use the **post-gtt-address-conversion** *cs7 gtt selector submode* command. To remove the statement, use the **no** form of this command.

post-gtt-address-conversion *table-name*

no post-gtt-address-conversion *table-name*

Syntax Description	<i>table-name</i> Name of an already-defined address conversion table.							
Defaults	None.							
Command Modes	cs7 gtt selector submode							
Command History	<table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>12.2(18)IXA</td><td rowspan="3">This command was introduced.</td></tr><tr><td>12.4(11)SW</td></tr><tr><td>12.2(33)IRA</td></tr></tbody></table>		Release	Modification	12.2(18)IXA	This command was introduced.	12.4(11)SW	12.2(33)IRA
Release	Modification							
12.2(18)IXA	This command was introduced.							
12.4(11)SW								
12.2(33)IRA								
Examples	The following example shows how to specify a conversion table named table1: <pre>cs7 gtt selector SELECTOR1 tt 1 gti 2 post-gtt-address-conversion table1</pre>							
Related Commands	<table><thead><tr><th>Command</th><th>Description</th></tr></thead><tbody><tr><td>cs7 gtt selector</td><td>Creates a GTT selector.</td></tr><tr><td>pre-gtt-address-conversion</td><td>Specifies the global title address conversion table to apply before performing local global title translation.</td></tr></tbody></table>		Command	Description	cs7 gtt selector	Creates a GTT selector.	pre-gtt-address-conversion	Specifies the global title address conversion table to apply before performing local global title translation.
Command	Description							
cs7 gtt selector	Creates a GTT selector.							
pre-gtt-address-conversion	Specifies the global title address conversion table to apply before performing local global title translation.							

power enable unsequence

By default, all SAMIs download the image at the same time, as configured by the **power enable unsequence** command in global configuration mode. To configure ITP so that both SAMIs download the image one at a time, use the **no** form of this command.

```
power enable unsequence
no power enable unsequence
```

Defaults All SAMIs download the image at the same time.

Command Modes Global configuration mode (config)

Command History	Release	Modification
	12.2(33)IRG	This command was introduced.

Examples

The following example shows how to configure the SAMIs to download the image at the same time:

```
power enable unsequence
```

The following example shows how to configure the SAMIs to download the image one at a time:

```
no power enable unsequence
```

Related Commands

pre-gtt-address-conversion

To specify the global title address conversion table to apply before performing local global title translation, use the **pre-gtt-address-conversion** *cs7 gtt selector* submode command. To remove the statement, use the **no** form of this command.

pre-gtt-address-conversion *table-name*

no pre-gtt-address-conversion *table-name*

Syntax Description	<i>table-name</i> Name of an already-defined prefix-conversion table.							
Defaults	None.							
Command Modes	cs7 gtt selector submode							
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>12.2(18)IXA</td><td rowspan="3">This command was introduced.</td></tr><tr><td>12.4(11)SW</td></tr><tr><td>12.2(33)IRA</td></tr></table>		Release	Modification	12.2(18)IXA	This command was introduced.	12.4(11)SW	12.2(33)IRA
Release	Modification							
12.2(18)IXA	This command was introduced.							
12.4(11)SW								
12.2(33)IRA								
Examples	The following example shows how to specify a conversion table named table2: <pre>cs7 gtt selector name tt np nai pre-gtt-address-conversion table2</pre>							
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>cs7 gtt selector</td><td>Creates a GTT selector.</td></tr><tr><td>post-gtt-address-conversion</td><td>Specifies the global title address conversion table to apply after performing local global title translation.</td></tr></table>		Command	Description	cs7 gtt selector	Creates a GTT selector.	post-gtt-address-conversion	Specifies the global title address conversion table to apply after performing local global title translation.
Command	Description							
cs7 gtt selector	Creates a GTT selector.							
post-gtt-address-conversion	Specifies the global title address conversion table to apply after performing local global title translation.							

preserve-opc (cs7 mlr ruleset)

To preserve the original originating point code (OPC) when an MLR is selected in this instance, use the **preserve-opc** command in cs7 mlr ruleset configuration mode. To remove the specification, use the **no** form of this command.

preserve-opc

no preserve-opc

Syntax Description

This command has no arguments or keywords.

Defaults

The command is disabled. The OPC is modified by the MLR to the ITP local PC.

Command Modes

cs7 mlr ruleset configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The default mode of MLR operation is for the ITP to place its local PC into the OPC field and insert the original OPC into the SCCP calling party address PC field, if possible. This behavior is consistent with an SCCP relay function, which MLR most closely resembles.

When the **preserve-opc** command is specified, the ITP routes the packet without modifying the original OPC in any way. The SCCP calling party address is also not modified.

Examples

The following example shows how to specify that, when a rule is matched, the ITP routes the packet without modifying the original OPC:

```
cs7 mlr ruleset ruleset1
 preserve-opc
```

Related Commands

Command	Description
cs7 mlr ruleset	Specifies an MLR ruleset and application layer protocol filter for the ruleset.
preserve-opc (cs7 mlr options)	Specifies an MLR result option command and enables cs7 mlr options configuration mode.

preserve-opc (cs7 mlr options)

To preserve the original originating point code (OPC) when an MLR is selected in this instance, use the **preserve-opc** command in cs7 mlr options configuration mode. To remove the specification, use the **no** form of this command.

preserve-opc

no preserve-opc

Syntax Description

This command has no keywords or arguments.

Defaults

The command is disabled. The OPC is modified by the MLR to the ITP local PC.

Command Modes

cs7 mlr options configuration

Command History

Release	Modification
12.2(18)IXC	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The default mode of MLR operation is for the ITP to place its local PC into the OPC field and insert the original OPC into the SCCP calling party address PC field, if possible. This behavior is consistent with an SCCP relay function, which MLR most closely resembles.

When the **preserve-opc** command is specified, the ITP routes the packet without modifying the original OPC in any way. The SCCP calling party address is also not modified. This **preserve-opc** command applies to all messages that are routed using MLR.

Related Commands

Commands	Description
cs7 mlr options	Specifies MLR global options.
preserve-opc (cs7 mlr ruleset)	Specifies an MLR ruleset and application layer protocol filter for the ruleset.

preventive-txp

To enable preventive transfer prohibited route management messages, use the **preventive-txp** cs7 linkset submode command. To disable preventive transfer prohibited messages, use the **no** form of this command.

preventive-txp

no preventive-txp

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

cs7 linkset submode

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA12	

Usage Guidelines

A preventive transfer prohibited message is normally sent to an adjacent node to indicate that the adjacent node will be used for signaling traffic to a concerned destination. The purpose of the message is to avoid a routing loop by preventing the adjacent node from sending signaling traffic to a node that will route the signaling traffic back to the adjacent node.

This command should only be used to disable preventive transfer prohibited messages to adjacent nodes when the possibility for a routing loop does not exist. Extreme care should be taken when this command is used to disable preventive transfer prohibited messages.

Examples

The following example shows how to disable the broadcast of route management messages on linkset1:

```
cs7 linkset linkset1
no preventive-txp
```

Related Commands

Command	Description
cs7 linkset	Specifies a linkset and enables cs7 linkset submode.
show cs7 linkset	Displays linkset information and status.

qos-access-group

To apply an access list to a QoS class, use the **qos-access-group** *cs7 qos* submode command. To remove the access list from the QoS class, use the **no** form of this command.

qos-access-group *access-list-number*

no qos-access-group *access-list-number*

Syntax Description	<i>access-list-number</i>	Number of a Cisco SS7 access list. The range is a decimal number from 2700 to 2999.

Defaults	None.

Command Modes	cs7 qos submode

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	The qos-access-group command allows you to assign an ITP access list to a QoS class definition.

Examples	The following example shows how to assign access list 2700 to QoS class 3. Packets that match access list 2700 are assigned QoS class 3.

```
access list 2700 permit dpc 1.100.0 0.0.255
```

```
cs7 qos class 3
  qos-access-group 2700
```

Related Commands	Command	Description
	access-list	Defines an access list.
	cs7 qos class	Defines a QoS class.
	show cs7 access-lists	Displays information about defined ITP access lists.

qos-class (cs7 as)

To configure a QoS class for the packets sent to the ASPs in this AS, use the **qos-class** cs7 as submode command. To remove the configuration, use the **no** form of this command.

qos-class *class*

no qos-class *class*

Syntax Description	<i>class</i>	QoS class ID. Valid range is 1 to 7.

Defaults	None.

Command Modes	cs7 as submode

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	The QoS class must be defined before the class is assigned.
	After being configured, this QoS class is applied to all ASPs listed under this AS. The QoS class goes into effect for only the subsequent ASP connections.
	The QoS class defined under the ASP overrides the QoS class defined under the AS.

Examples	The following example shows how to configure QoS class 4 for AS1:

```
cs7 as as1 m3ua
  qos-class 4
```

Related Commands	Command	Description
	cs7 as	Defines an application server (AS).

qos-class (cs7 asp)

To configure a QoS class for the packets sent to this ASP, use the **qos-class** cs7 asp submode command. To remove the configuration, use the **no** form of this command.

qos-class *class* [*instance-number*]

no qos-class *class* [*instance-number*]

Syntax Description	<i>class</i>	QoS class ID in the range 0 to 7.
	<i>instance-number</i>	Required if multiple instances are configured. The valid range is 0 to 7. The default instance is 0.

Defaults	The default instance is 0.

Command Modes	cs7 asp submode

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines

The QoS class must be defined before the class is assigned.

The QoS class goes into effect for only the subsequent ASP connections.

The QoS class defined under the ASP overrides the QoS class defined under the AS.

Examples

The following example shows how to configure QoS class 4 for ASP1:

```
cs7 asp ASP1 2904 2905 m3ua
  remote-ip 1.1.1.1
  qos-class 4
```

Related Commands	Command	Description
	cs7 asp	Specifies an application server process (ASP) and enables cs7 asp submode.
	cs7 qos class	Defines a QoS class.
	show cs7 qos	Displays QoS class information.

qos-class (cs7 gtt selector)

To configure a QoS class for a selector, use the **qos-class** cs7 gtt selector submode command. To remove the configuration, use the **no** form of this command.

qos-class *class*

no qos-class *class*

Syntax Description

<i>class</i>	QoS class ID. Valid range is 0 to 7.

Defaults

None.

Command Modes

cs7 gtt selector submode

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

If the QoS class entered for a selector is not defined, SCCP packets for the selector are routed using the default class peer link members.

Examples

The following example shows how to configure QoS class 4 for the GTT selector named c7gsp:

```
cs7 gtt selector c7gsp 3 2
qos-class 4
```

Related Commands

Command	Description
cs7 qos class	Defines a QoS class.
show cs7 qos	Displays QoS class information.

qos-class (cs7 link)

To configure a QoS class for a peer link, use the **qos-class** cs7 link submode command. To remove the configuration, use the **no** form of this command.

qos-class *class*

no qos-class *class*

Syntax Description	<i>class</i> QoS class ID. Valid range is 1 to 7.	
Defaults	None.	
Command Modes	cs7 link submode	
Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	
Usage Guidelines	ITP QoS requires at least one default class peer link member. ITP QoS does not permit a QoS class to be assigned to the default class peer link member.	
	The QoS class must be defined before the class is assigned to a peer link.	
Examples	The following example shows how to configure QoS class 4 for peer link 2: cs7 linkset michael 10.1.1 link 2 sctp 172.18.44.147 7000 7000 qos-class 4	
Related Commands	Command	Description
	cs7 qos class	Defines a QoS class.
	show cs7 qos	Displays QoS class information.

qos-class (cs7 mated-sg)

To configure a QoS class for the packets sent to the SG mate, use the **qos-class** cs7 mated-sg submode command. To remove the configuration, use the **no** form of this command.

qos-class *class* [*instance-number*]

no qos-class *class* [*instance-number*]

Syntax Description	<i>class</i>	QoS class ID. Valid range is 1 to 7.
	<i>instance-number</i>	Required if multiple instances are configured. The valid range is 0 to 7. The default instance is 0.

Defaults	The default instance is 0.

Command Modes	cs7 mated-sg submode

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	The QoS class must be defined before the class is assigned to a peer link.
	The QoS class goes into effect for only the subsequent mated-SG connection.

Examples	The following example shows how to configure QoS class 4 for the mated SG named BLUE:

```
cs7 mated-sg BLUE 2905
remote-ip 5.5.5.5
qos-class 4
```

Related Commands	Command	Description
	cs7 qos class	Defines a QoS class.
	show cs7 qos	Displays QoS class information.

qos-ip-dscp

To define the differentiated services code point (DSCP) setting for a QoS class, use the **qos-ip-dscp** *cs7* qos submode command. To set the DSCP setting to the default, use the **no** form of this command.

qos-ip-dscp *ip-tos*

no qos-ip-dscp *ip-tos*

Syntax Description

<i>ip-tos</i>	DSCP setting for the IP TOS byte, in decimal notation. Valid range is 0 to 63. The default is 0.

Defaults

The IP TOS default is 0.

Command Modes

cs7 qos submode

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The TOS byte in the IP header is set with the value of **qos-ip-dscp** on peer links that are members of the specified QoS class. The **ip-dscp** *cs7* link submode command overrides the **qos-ip-dscp** TOS settings assigned through a QoS class.

Examples

The following example shows how to set the IP type of service to DSCP 56 for QoS class 2:

```
cs7 qos class 2
  qos-ip-dscp 56
```

Related Commands

Command	Description
cs7 linkset	Specifies a linkset.
ip-dscp (cs7 m2pa profile)	Configures DSCP TOS setting for a link.
link (cs7 linkset)	Configures a link.

qos-ip-precedence

To define the IP precedence setting for a QoS class, use the **qos-ip-precedence** *cs7* qos submode command. To set the IP precedence to the default setting, use the **no** form of this command.

qos-ip-precedence *ip-tos*

no qos-ip-precedence *ip-tos*

Syntax Description	<i>ip-tos</i>	IP precedence setting, in decimal notation. Valid range is 0 to 7. The default setting is 0.

Defaults	The IP ToS default is 0.

Command Modes	cs7 qos submode

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	The ToS byte in the IP header is set with the value of qos-ip-precedence on peer links that are members of the specified QoS class. The ip-precedence <i>cs7</i> link submode command overrides the qos-ip-precedence ToS settings assigned through a QoS class.

Examples	The following example shows how to set the IP type of service to 3 for QoS class 1: <pre>cs7 qos class 1 qos-ip-precedence 3</pre>

Related Commands	Command	Description
	cs7 linkset	Specifies a linkset.
	ip-precedence (cs7 link)	Configures IP precedence ToS settings.
	link (cs7 linkset)	Configures a link.

rate-limit rate (cs7 gws as rate-limit-timer)

To enable the rate limit traffic rate on specified GWS AS for a message type, use the **rate-limit rate** command in the cs7 gws as rate-limit-timer configuration mode. To disable the configuration, use the **no** form of this command.

rate-limit rate *rate* [**onset-threshold** *othresh* [**abate-threshold** *athresh*]][**sccp-error** *sccp-error*]

no rate-limit

rate-limit rate	Enables the rate limit traffic rate feature.
<i>rate</i>	Specified traffic rate. The range is from 1 to 2147483648 MSUs.
onset-threshold	(Optional) Sets a configured rate limit to raise an alarm.
<i>othresh</i>	(Optional) Specifies the percentage of the configured rate limit that will raise the alarm. The range is from 11 to 100 percent.
abate-threshold	(Optional) Sets a configured rate limit to clear the alarm.
<i>athresh</i>	(Optional) Specifies the percentage of the configured rate limit that will clear the alarm. The range is from 1 to 99 percent.
sccp-error	(Optional) Sends a UDTS to the originator with the configured SCCP error code. This requires that the UDTS has a return-on-error configured.
<i>sccp-error</i>	The specified SCCP UDTS return cause value. (The usage guidelines section lists the error definitions.)

Defaults

The rate limit traffic rate feature is disabled by default.

If the onset threshold is not set, the default onset threshold is 90%. If the abate threshold is not set, the default abate threshold is 10% lesser than the onset value.

Command Modes

cs7 gws as rate-limit timer configuration submode

Release	Modification
12.4(15)SW6	This command was introduced.
12.2(33)IRF	

Usage Guidelines

The rate limit traffic rate feature is not related to the maximum number of MSUs supported on the physical interface. There is no check based on the number of Max MSU supported on the physical interface.

MSUs are silently discarded when the rate limit is reached. The traffic flow resumes at the beginning of the next time window. Message counting also resumes at the beginning of the next time window.

You can specify the sending of a return on error, when SCCP MSUs are discarded. The following table lists the SCCP UDTS return cause values:

Value	Description
0	No translation for an address of such nature
1	No translation for this specific address
2	Subsystem congestion
3	Subsystem failure
4	Unequipped User
5	MTP failure
6	Network Congestion
7	Unqualified
8	XUDTS Error in message transport
9	XUDTS Error in local processing
A	XUDTS Cannot perform reassembly
B	SCCP failure
C	SCCP Hop counter violation
D	Segmentation not supported
E	Segmentation failure
WORD	ITU SCCP Spare Error Codes in Hex {F..FF}

Examples

In this example, the Cisco ITP counts the ingress messages on GWS AS alpha during a five second period. When the number of packets crosses the configured 2000 message maximum, messages are discarded silently.

For discarded SCCP messages, a UDTs with the configured error-code 3 is sent to the originator.

An alarm is raised when the ingress traffic rate on the GWS alpha reaches 80% of the configured 2000 maximum. The alarm clears if during the next time period the traffic rate drops to 60% or less of the configured 2000 maximum:

```
cs7 instance 0 gws as name alpha
  rate-limit-timer 5
  rate-limit rate 2000 onset-threshold 80 abate-threshold 60 sccp-error 3
  inbound result action-set as1
```

Related Commands

Command	Description
inbound (config-gws-ls)	Configure screening of inbound message on a GWS linkset.
inbound (config-gws-as)	Configure screening of inbound message on a GWS AS.
rate-limit-timer (cs7 gws as)	Enables rate limiting for GWS AS.

■ rate-limit rate (cs7 gws as rate-limit-timer)

Command	Description
rate-limit-timer (cs7 gws linkset)	Enables rate limiting for GWS linksets.
show cs7 gws linkset	Shows the number of MSUs discarded silently or with an error due to the rate limit feature.

rate-limit rate (gws as egress-rate-lmt-timer)

To enable the rate limit traffic rate on specified action sets for a message type, use the **rate-limit rate** command in the gws as egress-rate-lmt-timer configuration mode. This feature limits the total outbound traffic rate on the given AS. To disable the configuration, use the **no** form of this command.

rate-limit rate *rate* [**onset-threshold** *othresh* [**abate-threshold** *athresh*]]

no rate-limit

rate-limit rate	Enables the rate limit traffic rate feature.
<i>rate</i>	Specified traffic rate. The range is from 1 to 2147483648 MSUs.
onset-threshold	(Optional) Sets a configured rate limit to raise an alarm.
<i>othresh</i>	(Optional) Percentage of the configured rate limit that will raise the alarm. The range is from 11 to 100.
abate-threshold	(Optional) Sets a configured rate limit to clear the alarm.
<i>athresh</i>	(Optional) Percentage of the configured rate limit that will clear the alarm. The range is from 1 to 99.

Defaults

Disabled.

If the onset threshold is not set, the default onset threshold is 90 percent. If the abate threshold is not set, the default abate threshold is 10 percent less than the onset value.

Command Modes

gws as egress-rate-lmt-timer configuration submode

Command History

Release	Modification
12.4(15)SW7	This command was introduced.
12.2(33)IRG	

Usage Guidelines

The rate limit traffic rate feature is not related to the maximum number of MSUs supported on the physical interface. There is no check based on the number of Max MSUs supported on the physical interface.

MSUs are discarded when the egress rate limit is reached, and an alarm is raised indicating that the threshold has been hit. Both traffic flow and message counting resume at the start of the next time window.

Examples

In the following example, the Cisco ITP counts the egress messages on an AS named “as-1” during a five-second period:

```
cs7 instance 0 gws as name as-1
  outbound result action-set as1
  egress-rate-lmt-timer 5
  rate-limit rate 2000 onset-threshold 80 abate-threshold 60
```

An alarm is raised when the egress traffic rate reaches 80 percent of the configured 2000 maximum. This alarm clears if, during the next time period, the traffic rate drops to 60 percent or less of the configured 2000 maximum.

Another alarm is raised when the egress traffic rate exceeds the configured 2000 maximum. Additional MSUs are discarded, and this alarm clears after expiration of the time period.

Related Commands

Command	Description
egress-rate-lmt-timer (config-gws-as)	Enables the rate limit feature on egress traffic of a given AS and sets its associated timer.
egress-rate-lmt-timer (config-gws-ls)	Enables the rate limit feature on egress traffic of a given linkset and sets its associated timer.
outbound (config-gws-as)	Configure screening of outbound messages on a GWS AS.
outbound (config-gws-ls)	Configure screening of outbound messages on a GWS linkset.
rate-limit-timer (cs7 gws as)	Enables rate limiting for GWS AS.
rate-limit-timer (cs7 gws linkset)	Enables rate limiting for GWS linksets.
show cs7 gws linkset	Shows the number of MSUs discarded silently or with an error because of the rate limit feature.

rate-limit rate (gws linkset egress-rate-lmt-timer)

To enable the rate limit traffic rate on specified linksets for a message type, use the **rate-limit rate** command in the gws linkset egress-rate-lmt-timer configuration mode. This feature limits the total outbound traffic rate on the given linkset. To disable the configuration, use the **no** form of this command.

rate-limit rate *rate* [**onset-threshold** *othresh* [**abate-threshold** *athresh*]]

no rate-limit

rate-limit rate	Enables the rate limit traffic rate feature.
<i>rate</i>	Specified traffic rate. The range is from 1 to 2147483648 MSUs.
onset-threshold	(Optional) Sets a configured rate limit to raise an alarm.
<i>othresh</i>	(Optional) Percentage of the configured rate limit that will raise the alarm. The range is from 11 to 100.
abate-threshold	(Optional) Sets a configured rate limit to clear the alarm.
<i>athresh</i>	(Optional) Percentage of the configured rate limit that will clear the alarm. The range is from 1 to 99.

Defaults

Disabled.

If the onset threshold is not set, the default onset threshold is 90 percent. If the abate threshold is not set, the default abate threshold is 10 percent less than the onset value.

Command Modes

gws linkset egress-rate-lmt-timer configuration submenu

Command History

Release	Modification
12.4(15)SW7	This command was introduced.
12.2(33)IRG	

Usage Guidelines

The rate limit traffic rate feature is not related to the maximum number of MSUs supported on the physical interface. There is no check based on the number of Max MSU supported on the physical interface.

MSUs are discarded when the egress rate limit is reached, and an alarm is raised indicating that the threshold has been hit. Both traffic flow and message counting resume at the start of the next time window.

Examples

In the following example, the Cisco ITP counts the egress messages on a linkset named “ls-1” during a five-second period:

```
cs7 instance 0 gws linkset name ls-1
  outbound result action-set as1
  egress-rate-lmt-timer 5
  rate-limit rate 2000 onset-threshold 80 abate-threshold 60
```

An alarm is raised when the egress traffic rate reaches 80 percent of the configured 2000 maximum. This alarm clears if, during the next time period, the traffic rate drops to 60 percent or less of the configured 2000 maximum.

Another alarm is raised when the egress traffic rate exceeds the configured 2000 maximum. Additional MSUs are discarded, and this alarm clears after expiration of the time period.

Related Commands

Command	Description
egress-rate-lmt-timer (config-gws-as)	Enables the rate limit feature on egress traffic of a given AS and sets its associated timer.
egress-rate-lmt-timer (config-gws-ls)	Enables the rate limit feature on egress traffic of a given linkset and sets its associated timer.
outbound (config-gws-as)	Configure screening of outbound messages on a GWS AS.
outbound (config-gws-ls)	Configure screening of outbound messages on a GWS linkset.
rate-limit-timer (cs7 gws as)	Enables rate limiting for GWS AS.
rate-limit-timer (cs7 gws linkset)	Enables rate limiting for GWS linksets.
show cs7 gws linkset	Shows the number of MSUs discarded silently or with an error because of the rate limit feature.

rate-limit rate (gws linkset rate-limit-timer)

To enable the rate limit traffic rate on specified linksets for a message type, use the **rate-limit rate** command in the cs7 gws linkset rate-limit-timer configuration mode. To disable the configuration, use the **no** form of this command.

rate-limit rate *rate* [**onset-threshold** *othresh* [**abate-threshold** *athresh*]][**sccp-error** *sccp-error*]

no rate-limit

rate-limit rate	Enables the rate limit traffic rate feature.
<i>rate</i>	Specified traffic rate. The range is from 1 to 2147483648 MSUs.
onset-threshold	(Optional) Sets a configured rate limit to raise an alarm.
<i>othresh</i>	(Optional) Specifies the percentage of the configured rate limit that will raise the alarm. The range is from 11 to 100 percent.
abate-threshold	(Optional) Sets a configured rate limit to clear the alarm.
<i>athresh</i>	(Optional) Specifies the percentage of the configured rate limit that will clear the alarm. The range is from 1 to 99 percent.
sccp-error	(Optional) Sends a UDTs to the originator with the configured SCCP error code. This requires that the UDTs has a return-on-error configured.
<i>sccp-error</i>	The specified SCCP UDTs return cause value. (The usage guidelines section lists the error definitions.)

Defaults

The rate limit traffic rate feature is disabled by default.

If the onset threshold is not set, the default onset threshold is 90%. If the abate threshold is not set, the default abate threshold is 10% lesser than the onset value.

Command Modes

cs7 gws linkset rate-limit timer configuration submode

Command History

Release	Modification
12.4(15)SW6	This command was introduced.
12.2(33)IRF	

Usage Guidelines

The rate limit traffic rate feature is not related to the maximum number of MSUs supported on the physical interface. There is no check based on the number of Max MSU supported on the physical interface.

MSUs are silently discarded when the rate limit is reached. The traffic flow resumes at the beginning of the next time window. Message counting also resumes at the beginning of the next time window.

You can specify the sending of a return on error, when SCCP MSUs are discarded. The following table lists the SCCP UDTs return cause values:

Value	Description
0	No translation for an address of such nature
1	No translation for this specific address
2	Subsystem congestion
3	Subsystem failure
4	Unequipped User
5	MTP failure
6	Network Congestion
7	Unqualified
8	XUDTS Error in message transport
9	XUDTS Error in local processing
A	XUDTS Cannot perform reassembly
B	SCCP failure
C	SCCP Hop counter violation
D	Segmentation not supported
E	Segmentation failure
WORD	ITU SCCP Spare Error Codes in Hex {F..FF}

Examples

In this example, the Cisco ITP counts the ingress messages on linkset alpha during a five second period. When the number of packets crosses the configured 2000 message maximum, messages are discarded silently.

For discarded SCCP messages, a UDTs with the configured error-code 3 is sent to the originator.

An alarm is raised when the ingress traffic rate on the linkset alpha reaches 80% of the configured 2000 maximum. The alarm clears if during the next time period the traffic rate drops to 60% or less of the configured 2000 maximum:

```
cs7 in 0 gws linkset name alpha
  rate-limit-timer 5
  rate-limit rate 2000 onset-threshold 80 abate-threshold 60 sccp-error 3
  inbound result action-set as1
```

Related Commands

Command	Description
inbound (config-gws-ls)	Configure screening of inbound message on a GWS linkset.
inbound (config-gws-as)	Configure screening of inbound message on a GWS AS.
rate-limit-timer (cs7 gws as)	Enables rate limiting for GWS AS.

Command	Description
rate-limit-timer (cs7 gws linkset)	Enables rate limiting for GWS linksets.
show cs7 gws linkset	Shows the number of MSUs discarded silently or with an error due to the rate limit feature.

rate-limit-timer (cs7 gws as)

To enable rate limiting for GWS AS and to configure the rate limit timer, use the **rate-limit-timer** command in the cs7 gws as configuration mode. To disable the configuration, use the **no** form of this command.

rate-limit-timer *timer*

no rate-limit-timer *timer*

Syntax Description

rate-limit-timer	Enables the rate-limit on a given AS and configures the rate limit timer.
<i>timer</i>	The length of the time period set for the Cisco ITP to count the received MSUs. The range is an integer value of 1 to 60 seconds.

Defaults

Rate limiting is disabled.

Command Modes

cs7 gws as configuration submode

Command History

Release	Modification
12.4(15)SW6	This command was introduced.
12.2(33)IRF	

Usage Guidelines

The rate limit timer screens the MSUs for the configured time and resets on expiration.

The rate-limit-timer is only valid for inbound traffic. The timer resets after each time period expires. The rate-limit-timer parameter is only valid for inbound traffic. This rate-limit option is not available in default or global mode. This feature can only be disabled when its sub mode options are deleted. Also to delete the inbound setting, the rate-limit option needs to be disabled.

Examples

The following example configures the Cisco ITP to count the ingress messages on the AS named alpha for periods of five seconds:

```
cs7 instance 0 gws as name alpha
  rate-limit-timer 5
```

Related Commands

Command	Description
inbound (config-gws-ls)	Configure screening of inbound message on a GWS linkset.
inbound (config-gws-as)	Configure screening of inbound message on a GWS AS.

Command	Description
rate-limit rate (cs7 gws as rate-limit-timer)	Enables the rate limit traffic rate.
rate-limit-timer (cs7 gws linkset)	Enables rate limiting for GWS linksets.
show cs7 gws linkset	Shows the number of MSUs discarded silently or with an error due to the rate limit feature.

rate-limit-timer (cs7 gws linkset)

To enable rate limiting for GWS linksets and to configure the rate limit timer, use the **rate-limit-timer** command in the cs7 gws linkset configuration mode. To disable the configuration, use the **no** form of this command.

rate-limit-timer *timer*

no rate-limit-timer *timer*

Syntax Description

rate-limit-timer	Enables the rate-limit on a given linkset and configures the rate limit timer.
<i>timer</i>	The length of the time period set for the Cisco ITP to count the received MSUs. The range is an integer value of 1 to 60 seconds.

Defaults

Rate limiting is disabled.

Command Modes

cs7 gws linkset configuration submode

Command History

Release	Modification
12.4(15)SW6	This command was introduced.
12.2(33)IRF	

Usage Guidelines

The rate limit timer screens the MSUs for the configured time and resets on expiration.

The rate-limit-timer is only valid for inbound traffic. The timer resets after each time period expires. The rate-limit-timer parameter is only valid for inbound traffic. This rate-limit option is not available in default or global mode. This feature can only be disabled when its sub mode options are deleted. Also to delete the inbound setting, the rate-limit option needs to be disabled.

Examples

The following example configures the Cisco ITP to count the ingress SCCP messages on linkset ls1 for periods of five seconds:

```
cs7 in 0 gws linkset name ls1
  rate-limit-timer 5
```

Related Commands

Command	Description
inbound (config-gws-ls)	Configure screening of inbound message on a GWS linkset.
inbound (config-gws-as)	Configure screening of inbound message on a GWS AS.

Command	Description
rate-limit rate (cs7 gws as rate-limit-timer)	Enables the rate limit traffic rate.
rate-limit-timer (cs7 gws as)	Enables rate limiting for GWS AS.
show cs7 gws linkset	Shows the number of MSUs discarded silently or with an error due to the rate limit feature.

receive-window (cs7 local peer)

To configure the local receive window size, use the **receive-window** cs7 local peer configuration command. To disable the configuration, use the **no** form of this command.

receive-window *size*

no receive-window *size*

Syntax Description	<i>size</i>	Receive window size in bytes. The range is 5000 to 20971520 bytes. The default receive window size is 64000 bytes.
Defaults	64000 bytes	
Command Modes	cs7 local peer configuration	
Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines

The size of the receive window can affect performance. SCTP adapts its transmission rate to suit the available network capacity by using a congestion-sensitive, sliding-window flow control mechanism described in RFC 2581. At any time, only a certain number of bytes can be outstanding through the network. Keeping the path full of packets requires that both the congestion window (cwnd) and receive window (rwnd) reach the effective size of the “pipe” represented by the bandwidth delay. You can calculate the capacity of the pipe using the following equation:

$$\text{capacity (bits)} = \text{bandwidth (bits/sec)} \times \text{round-trip-time(sec)}$$

The bandwidth delay can vary widely depending on the network speed and round-trip-time (rtt) between the two endpoints. Using the capacity equation, you can estimate the minimum buffer size given the bandwidth of the communication media and the round-trip time between the nodes. For example, if the nodes are connected by a 1,544,000-bits/sec T1 link with a round-trip time of 60 ms, the estimated minimum buffer size is 11,580 bytes. The **receive-window** command defaults to 64,000 bytes. The congestion control and windowing algorithms adjust to network conditions by controlling the number of bytes that can be outstanding through the network.

Examples

The following example shows how to set the receive-window size to 6000 bytes:

```
cs7 local-peer 7000
  receive-window 6000
```

Related Commands

Command	Description
show cs7 m2pa	Displays M2PA statistics.

receive-window (cs7 m3ua)

To configure the local receive window size for the local port, use the **receive-window** cs7 m3ua submode command. To disable the configuration, use the **no** form of this command.

receive-window *size*

no receive-window *size*

Syntax Description	<i>size</i>	Receive window size in bytes. The range is 5000 to 20971520 bytes. The default receive window size is 64000 bytes.

Defaults	64000 bytes

Command Modes	cs7 m3ua submode

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples	The following example shows how to set the receive window size to 6000 bytes:

```
cs7 m3ua 2905
 local-ip 4.4.4.4
 receive-window 6000
```

Related Commands	Command	Description
	cs7 m3ua	Specifies the local port number for M3UA and enters cs7 m3ua submode.

receive-window (cs7)

To configure the local receive window size for the local port, use the **receive-window cs7** submode command. To disable the configuration, use the **no** form of this command.

receive-window *size*

no receive-window *size*

Syntax Description	<i>size</i> Receive window size in bytes. The range is 5000 to 20971520 bytes. The default receive window size is 64000 bytes.		
Defaults	64000 bytes		
Command Modes	cs7 submode		
Command History	Release	Modification	
	12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.	
Examples	The following example shows how to set the receive window size to 6000 bytes: cs7 5000 local-ip 4.4.4.4 receive-window 6000		
Related Commands	Command		Description
	cs7 sgmp		Specifies the local port number for and enters cs7 submode.

receive-window (cs7 sua)

To configure the local receive window size for the local port, use the **receive-window** cs7 sua submode command. To disable the configuration, use the **no** form of this command.

receive-window *size*

no receive-window *size*

Syntax Description	<i>size</i> Receive window size in bytes. The range is 5000 to 20971520 bytes. The default receive window size is 64000 bytes.	
Defaults	64000 bytes	
Command Modes	cs7 sua submode	
Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	
Examples	The following example shows how to set the receive window size to 6000 bytes: cs7 sua 15000 local-ip 4.4.4.4 receive-window 6000	
Related Commands	Command	Description
	cs7 sua	Specifies the local port number for SUA and enters cs7 sua submode.

recovery-timeout

The AS recovery timeout is the amount of time after an AS becomes inactive that it will queue traffic waiting for an ASP to become active. If no ASP becomes active within this time, queued messages are lost.

To specify the recovery timeout value, use the **recovery-timeout** *cs7* as submode command. To disable the configuration, use the **no** form of this command.

recovery-timeout *msec*

no recovery-timeout *msec*

Syntax Description	<i>msec</i>	Recovery timeout value in milliseconds. The valid range is 0 to 2000 ms. The default is 2000 ms.

Defaults	2000 ms

Command Modes	<i>cs7</i> as submode

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples	The following example shows how to set the recovery timeout to 1000 ms: <pre>cs7 as BLUE m3ua recovery-timeout 1000</pre>

Related Commands	Command	Description
	cs7 as	Defines an AS.
	show cs7 asp detail	Displays ASP information.

remote-ip (cs7 asp)

To configure a remote IP address to associate incoming packets from an ASP to a configured ASP, use the **remote-ip** *cs7 asp* submode command. To remove the configuration, use the **no** form of this command.

remote-ip *remote-ip*

no remote-ip *remote-ip*

Syntax Description	<i>remote-ip</i> The remote IP address of the ASP.							
Defaults	None.							
Command Modes	cs7 asp submode							
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>12.2(18)IXA</td><td rowspan="3">This command was introduced.</td></tr><tr><td>12.4(11)SW</td></tr><tr><td>12.2(33)IRA</td></tr></table>		Release	Modification	12.2(18)IXA	This command was introduced.	12.4(11)SW	12.2(33)IRA
Release	Modification							
12.2(18)IXA	This command was introduced.							
12.4(11)SW								
12.2(33)IRA								
Usage Guidelines	With the remote-ip command, you can configure a remote IP address to associate incoming packets from an ASP to a configured ASP. The remote IP address configuration does not require you to configure all the possible IP addresses for multihoming, but the remote IP should be in the list of allowed IP addresses that is learned from the INIT and/or COOKIE SCTP control messages. You can configure up to four remote IP addresses by specifying additional remote-ip commands.							
Examples	The following example shows how to configure remote IP address 2.2.2.2 for M3UA ASP1: <pre>cs7 asp ASP1 5000 5000 m3ua remote-ip 2.2.2.2</pre>							
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>cs7 asp</td><td>Specifies an application server process (ASP) and enables cs7 asp submode.</td></tr></table>		Command	Description	cs7 asp	Specifies an application server process (ASP) and enables cs7 asp submode.		
Command	Description							
cs7 asp	Specifies an application server process (ASP) and enables cs7 asp submode.							

remote-ip (cs7 dcs)

To configure an IP address and port for a DCS node, use the **To** to disable the command, use the **no** form of this command.

remote-ip *ip_addr1* [*ip_addr2*] *port*

no remote-ip

Syntax Description	<i>ip_addr1</i>	An IPv4 address in the form xxx.xxx.xxx.xxx. It is the primary IP address used when sending PMP traffic.
	<i>ip_addr2</i>	(Optional) An IPv4 address in the form xxx.xxx.xxx.xxx. It is a redundant IP address used when the primary IP address fails.
	<i>port</i>	IP address port with an integer range of 1024 to 49151.

Defaults	None.

Command Modes	cs7 dcs configuration submode

Command History	Release	Modification
	12.4(15)SW3	This command was introduced.
	12.2(33)IRC	

Usage Guidelines

You must shut down the DCS node before deleting a remote IP address on that node. You can only modify the remote IP address if the DCS node is not part of any DCS group.

We recommend using 33500 for the port number. This port number is recognized by the @WIRESHARK dissector for PMP.

The **no remote-ip** command does not have any keywords or arguments; it deletes all ports and IP addresses.

Examples

The following example shows how to configure a DCS node with 209.165.201.31 as the primary address, 209.165.201.28 as the secondary address, and 33500 as the port on the CS7 DCS node named dcs1:

```
cs7 dcs dcs1
remote-ip 209.165.201.31 209.165.201.28 33500
local-ip 209.165.201.30 33500
ping-interval 5
timeout-count 3
udp-checksum
```

Related Commands

Command	Description
pmp (cs7 linkset)	Turns probeless monitoring on for a linkset.
pmp (cs7 AS)	Turns probeless monitoring on for an AS.
cs7 dcs-group	Identifies a name to be associated with a DCS group.
cs7 pmp hold-queue	Sets the integer range of a PMP hold queue threshold.
cs 7 dcs	Identifies a name to be associated with a DCS node.
show cs7 pmp	Displays errors and information about the PMP.
show cs7 dcs-group	Displays information about the DCS group.
show cs7 dcs	Displays information about the DCS node.

remote-ip (cs7 mated-sg)

To configure a remote IP address to associate incoming packets from the mate, use the **remote-ip** cs7 mated-sg submode command. To remove the configuration, use the **no** form of this command.

remote-ip *remote-ip*

no remote-ip *remote-ip*

Syntax Description	<i>remote-ip</i>	The remote IP address of the mate.

Defaults	None.

Command Modes	cs7 mated-sg submode

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	With the remote-ip command, you can configure a remote IP address to associate incoming packets from the mate. The remote IP address configuration does not require you to configure all the possible IP addresses for multihoming, but the remote IP should be in the list of allowed IP addresses that is learned from the INIT and/or COOKIE SCTP control messages. You can configure up to four remote IP addresses by specifying additional remote-ip commands.

Examples	The following example shows how to configure a remote IP address for the mated SG named BLUE: cs7 mated-sg BLUE 5000 remote-ip 5.5.5.5

Related Commands	Command	Description
	cs7 mated-sg	Configures a connection to a mated SG.

remove route (route table)

To remove the active MTP3 route table on the ITP, use the **remove route** route table submode configuration command.

remove route *point-code* [*mask* | */length*]

Syntax Description	<i>point-code</i>	Signaling point code of the destination.
	<i>mask</i>	Specifies the significant bits of the point code.
	<i>/length</i>	Alternate way of specifying the mask. For ANSI, the alternate specification of the default is /24. For ITU, the alternate specification of the default is /14.

Defaults	None.

Command Modes	route table submode configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	The remove route command is the functional equivalent of “no update.” The specified route is deleted from the active routing table.
	If the configuration contained an update route command for the specified point code, the update route command line is removed from the configuration.
	The remove route configuration appears in the ITP configuration until a new route-table is created using the cs7 save route-table privileged EXEC command.

Examples	The following example shows how to remove an active route table:

```
remove route 1.50.2 255.255.255 linkset nyc
```

Related Commands	Command	Description
	update route (route-table)	Updates a route.

response-timer (cs7 sms profile parms)

To specify the time lapse allowed between a UCP request and the corresponding UCP response, use the **response-timer** command in cs7 sms profile parameters configuration mode. To remove the specification, use the **no** form of this command.

response-timer *msec*

no response-timer *msec*

Syntax Description	<i>msec</i>	Time lapse allowed between an UCP request and the corresponding UCP response. Valid range is 1000 ms to 10000 ms. The default is 5000 ms.

Defaults	5000 ms

Command Modes	cs7 sms profile parameters configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples The following example shows how to configure an SMPP profile named mmprofile and set several parameters:

```
cs7 sms smpp profile mmprofile
bind-type any
inactivity-timer 5000
keepalive-timer 1000
response-timer 2000
send-window 50
session-init-timer 5000
```

Related Commands	Command	Description
	bind-type (cs7 sms profile parameters)	Specifies the SMPP bind type.
	inactivity-timer (cs7 sms profile parameters)	Specifies the session inactivity timer.
	keepalive-timer (cs7 sms profile parameters)	Specifies the session keepalive timer.

■ response-timer (cs7 sms profile parms)

Command	Description
send-window (cs7 sms profile parms)	Specifies the send window size.
session-init-timer (cs7 sms profile parms)	Specifies the session initiation time.

response-timer (cs7 sms session parms)

To specify the time lapse allowed between a UCP request and the corresponding UCP response, use the **response-timer** command in cs7 sms session parameters configuration mode. To remove the specification, use the **no** form of this command.

response-timer *msec*

no response-timer *msec*

Syntax Description	<i>time</i>	Time lapse allowed between an UCP request and the corresponding UCP response. Valid range is 1000 ms to 10000 ms. The default is 5000 ms.

Defaults	5000 ms

Command Modes	cs7 sms session parameters configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples	The following example shows how to create an SMPP connection and how to configure a destination and several parameters:

```
cs7 sms smpp 5000 local-ip 10.10.10.200 dynamic
destination offisland 10.10.20.2 6000
bind-type any
inactivity-timer 5000
keepalive-timer 1000
response-timer 2000
send-window 50
session-init-timer 5000
```

Related Commands	Command	Description
	bind-type (cs7 sms session parameters)	Specifies the SMPP bind type.
	inactivity-timer (cs7 sms session parameters)	Specifies the session inactivity timer.
	keepalive-timer (cs7 sms session parameters)	Specifies the session keepalive timer.

■ response-timer (cs7 sms session parms)

Command	Description
send-window (cs7 sms session parms)	Specifies the send window size.
session-init-timer (cs7 sms session parms)	Specifies the session initiation timer.

result (cs7 mlr ruleset rule)

To specify the processing that will be performed on a packet matching the specified trigger and rule, use the **result** command in cs7 mlr ruleset rule configuration mode. To cancel the processing, use the **no** form of this command.

```
result {gt addr-string [gt-addr-type] | [instance instance-number] pc dest_pc [ssn ssn] | asname
as-name | group result-group | block [sccp-error error | map-error {[default ecdef[subdef]]}[v1
ec1 [sub1]] [v2 ec2 [sub2]] [v3 ec3 [sub3]] } | continue | route}
```

no result

Syntax Description	gt	Routes the message using SCCP global title. The specified address is placed in the SCCP Called Party Address, the routing indicator is changed to RI=GT, and the message is routed based on the locally provisioned global title translation table.
	addr-string	Address string of 1 to 15 hexadecimal characters. The string is not input in BCD-String format, but in normal form.
	gt-addr-type	(Optional) Parameters that identify attributes of the global title address being used as a result. The parameters are variant-specific, and are identical to those parameters specified on a cs7 gtt selector command. If not specified, the default is the standard E.164 address type for the network variant being used. tt tt [gti gti] [np np nai nai] tt Identifies the translation type specified within the address. tt An integer value from 0 to 255. gti Identifies the global title indicator value for the specified address. Used only when the cs7 variant command specifies ITU or China. gti An integer value of 2 or 4. np Identifies the numbering plan of the specified address. Used only when the gti value is 4. np An integer value from 0 to 15. nai Identifies the nature of address indicator. Used only when the gti value is 4. nai Integer value from 0 to 127.
	instance	(Optional) Indicates the PC/PCSSN result in a local or other instance.
	instance-number	(Optional) Instance number. Valid range is 0 to 7. The default instance is 0.
	pc	Routes the message using the specified destination point code (DPC). The packet is routed in MTP3 with the specified DPC.
	dest-pc	DPC in variant-specific point-code format.
	ssn	Routes the message using the subsystem number.
	ssn	Subsystem number in decimal. Valid range is 2 to 255.
	asname	Routes the message to a particular destination M3UA or SUA application server.

<i>as-name</i>	Identifies an M3UA or SUA application server name. The name can be 1 to 12 characters in length.
group	Routes the message using a result group. A group is used to specify multiple destinations for a given rule match. The MLR result group must be defined before configuring the result command.
<i>result-group</i>	Identifies the name of the MLR result group containing the desired result possibilities. The name is specified as a character string with a maximum of 12 characters.
block sccp-error error	Drops messages matching this rule. Sends a UDTS for dropped packets to the originator with the configured sccp error code if return-on-error was set in the UDT.
block map-error	Performs MAP error handling. Defines the MAP error code for MLR/SMS-blocked MSUs based on operation type and version. If an MLR or SMS module matches the rule and the MSU is blocked, an error message is sent instead of dropping the MSU silently.
default	Returns a default MAP error code.
<i>ecdef</i>	The default return MAP error code.
<i>subdef</i>	Specifies a secondary default MAP error code.
v1	MAP version 1
v2	MAP version 2
v3	MAP version 3
<i>ec1</i>	Specifies the MAP error code for ec1.
<i>ec2</i>	Specifies the MAP error code for ec2.
<i>ec3</i>	Specifies the MAP error code for ec3.
<i>sub1</i>	Specifies a secondary MAP error code for sub1.
<i>sub2</i>	Specifies a secondary MAP error code for sub2.
<i>sub3</i>	Specifies a secondary MAP error code for sub3.
continue	Routes the original message as received.
route	Resumes original routing for the packet with the MLR-modified message.

Defaults

If not specified, the default global title address is the standard E.164 address type for the network variant being used.

Command Modes

cs7 mlr ruleset rule configuration

Command History	Release	Modification
	12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.
	12.2(18)IXG 12.4(15)SW2 12.2(33)IRB	The map-error keyword was added.
	12.2(18)IXG 12.4(15)SW2 12.2(33)IRB	The instance keyword was added.

Usage Guidelines

The MLR result group must be defined before configuring the **result** command.

One result must be specified.

If **sccp-error** *error* is configured and return-on-error is set in the UDT, a UDTS is sent back for dropped SCCP packets to the originating user with the configured error as the return cause. Currently, you can configure block results in MLR rules, triggers, and address table entries.

The **block map-error** MAP error code for a version takes precedence over a default MAP error code. If no MAP error is configured for the special version, the configured default error code is used. If no MAP error is configured, the MSU is blocked and dropped silently.

Examples

The following example shows how to route a packet that matches the configured trigger and rule routed for processing to the result group SMS-WEIGHTED:

```
cs7 mlr ruleset ruleset1
  rule 10 gsm-map sms-mo
    dest-sme 1234
    orig sme 60920025
    result group SMS-WEIGHTED
```

The following example shows how to configure MLR block map error handling for version 1 and the error code systemFailure:

```
cs7 mlr ruleset mapecset protocol gsm-map
  rule 10 sms-mo default
  result block map-error v1 systemFailure
```

The following example shows how to configure 1 as the instance in the **result** command:

```
cs7 instance 0 mlr ruleset tttt protocol gsm-map
  rule 1 sms-mo default
  result instance 1 pc 3.3.3 ssn 7
```

The following example shows how to route mobile initiated GSM-MAP messages containing USSD string *123*/## to DPC 1234:

```
cs7 ins 0 mlr options
  enable ussd-tree-type 2 ussd-timer 180

cs7 ins 0 mlr ruleset abc
  rule 1 gsm-map mobileUSSD
  ussd-string 123
  result pc 1234
```

■ result (cs7 mlr ruleset rule)

```
cs7 instance 0 gws action-set ussd_action mlr ruleset abc
cs7 instance 0 gws linkset name from_msc
    inbound result action ussd_action
cs7 instance 0 gws linkset name from_ussd
    inbound result action ussd_action
```

The following example shows how to filter mobile initiated GSM-MAP messages containing USSD string *123*/#:

```
cs7 ins 0 mlr options
    enable ussd-tree-type 2 ussd-timer 180

cs7 ins 0 mlr ruleset abc
    rule 1 gsm-map mobileUSSD
        ussd-string 123
        result block
```

Related Commands

Command	Description
cs7 mlr result	Specifies destination resources that process traffic to be routed based on multilayer information.
rule (cs7 mlr ruleset)	Specifies the rules for a routing trigger within a multilayer ruleset table and enables cs7 mlr ruleset rule configuration submode.
show cs7 mlr statistics	Displays global MLR statistics.

result (cs7 sms set rule)

To specify the result of a rule, use the **result** command in cs7 sms set rule configuration mode. To delete the result, use the **no** form of this command.

```
result {block | next-rule | group result-group | gt addr [tt tt] | pc dest-pc [ssn ssn] | rule index |
        deliver-mt | obtain-orig-imsi [validate] [next-rule] | validate-orig-msc [exit | gt-mismatch
        next-rule | negative-reply next-rule | no | pc-mismatch next-rule | timeout next-rule] }
```

no result

Syntax Description

block	Drops the message.
next-rule	Continues message processing with the next rule.
group	Routes the message using a result group and specifies the result group name.
<i>result-group</i>	Result group name.
gt	Routes the message using GT.
<i>addr</i>	Specifies the SCCP address, a string of 1 to 15 hexadecimal digits.
tt	(Optional) Specifies the translation type.
<i>tt</i>	Translation type, in the range 0 to 255.
pc	Routes the message using a point code and specifies the destination point code.
<i>dest-pc</i>	Destination point code.
ssn	(Optional) Specifies a subsystem number.
<i>ssn</i>	Subsystem number, in the range 2 to 255.
rule	Continues message processing at a specified rule.
<i>index</i>	Rule index, in the range 1 to 1000.
deliver-mt	Attempts a delivery to the destination SME as a mobile device. (Only valid for SMS-MO rule operations.)
obtain-origin-imsi	If the originator's IMSI was not provided on the SMS-MO request, then SMR attempts to obtain its IMSI.
validate	Specifies the SMR will obtain the originator's IMSI from the HLR and verify that the returned IMSI matches the origin IMSI received in the SMS-MO request or in a previous rule that obtained the origin IMSI. If the IMSI validation fails, an error is returned unless next-rule has been specified. If the origin IMSI was not previously received or obtained, then validation is successful if the originator's IMSI can be successfully obtained from the HLR.
next-rule	Executes the next rule in the ruleset sequence regardless of whether the origin IMSI was successfully retrieved.
result validate-orig-msc	Validates MO-SMS messages sent from MSC to SMSC or from SGSN to SMSC.
exit	Exits from cs7 sms result original msc/sgsn validation configuration submode.
gt-mismatch	GTA of GT-based CgPA does not match the MSC/SGSN number in the SRI-SM response.

instance	Indicates the PC/PCSSN result in a local or other instance.
negative-reply	HLR returns a negative response (reject, abort, cancel, error) for an SRI-SM request.
no	Negates a command or sets its defaults.
pc-mismatch	GTA generated by applying msc-proxy-addr on PC-based CgPA does not match the MSC/SGSN number in the SRI-SM response.
timeout	Timeout for HLR SRI-SM response.
next-rule	Continues message processing with the next rule.

Defaults

None.

Command Modes

cs7 sms set rule configuration

Command History

Release	Modification
12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.
12.2(18)IXH 12.4(15)SW3 12.2(33)IRC	The result validate-orig-msc keyword was added.

Usage Guidelines

If a valid result was returned from a rule parameter address table, then the table result overrules the rule result. Otherwise, the rule result is used.

This command with **result validate-orig-msc** keyword prevents a fraudulent party from submitting mobile originated short messages on behalf of an existing mobile subscriber. Its validation checks the originating MSC/SGSN address of an MO-SMS message to verify the true location of the mobile subscriber and prevent SMS MO spoofing.

Examples

The following example shows how to specify a ruleset named MO-RULES that includes rules and their results:

```
cs7 sms ruleset MO-RULES
rule 10 sms-mo
  result obtain-orig-imsi

rule 20 sms-mo
  orig-imsi-table IMSI-BLK
  result block

rule 30 sms-mo
  orig-imsi-table IMSI-OK
  result group POSTPAY
```


Related Commands

Command	Description
cs7 sms ruleset	Configures an SMS ruleset.
ruleset (cs7 sms ansi41 smsnot)	Specifies a rule and rule index.

retransmit-cwnd-rate (cs7 asp)

To configure the rate at which the SCTP congestion window size is reduced due to retransmission timer expiration, use the **retransmit-cwnd-rate** *cs7 asp* submode command. To disable the configuration, use the **no** form of this command.

retransmit-cwnd-rate *percent* [**sctp-fast-retransmit**]

no retransmit-cwnd-rate *percent* [**sctp-fast-retransmit**]

Syntax Description

<i>percent</i>	Rate at which the size of the SCTP congestion window is decreased due to retransmission timer expiration. Range is 0 to 100 percent. The default is 50 percent.
sctp-fast-retransmit	(Optional) Indicates that the setting of the SCTP congestion window should follow the rules as defined for an SCTP fast retransmission.

Defaults

The default rate is 50 percent.

Command Modes

cs7 asp submode

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The **retransmit-cwnd-rate** command allows the administrator to configure a rate at which the SCTP congestion window is decreased due to retransmission timer expiration. The administrator can select one of two methods for setting the congestion window as a result of the retransmission timer expiration: Either set the congestion window to the defaults as defined in RFC 2960 or RFC 4960 or set the congestion window in the same way as for a fast retransmission.



Caution

The behavior of the SCTP congestion control algorithms is not compliant with RFC 2960 or RFC 4960 when this command uses values other than the default rate. The rate should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples

The following example shows how to set the rate for reducing the congestion window to 70 percent due to a retransmission timer expiration:

```
cs7 asp ASP1 2905 2905 m3ua
  remote-ip 1.1.1
  retransmit-cwnd-rate 70
```

Related Commands

Command	Description
retransmit-timeout (cs7 asp)	Configures the minimum retransmission timeout value for the association.

retransmit-cwnd-rate (cs7 link)

To configure the rate at which the SCTP congestion window size is reduced due to retransmission timer expiration, use the **retransmit-cwnd-rate** cs7 link submode command. To disable the configuration, use the **no** form of this command.

retransmit-cwnd-rate *percent* [**sctp-fast-retransmit**]

no retransmit-cwnd-rate *percent* [**sctp-fast-retransmit**]

Syntax Description	<i>percent</i>	Rate at which the size of the SCTP congestion window is decreased due to retransmission timer expiration. Range is 0 to 100 percent. The default is 50 percent.
	sctp-fast-retransmit	(Optional) Indicates that the setting of the SCTP congestion window should follow the rules as defined for an SCTP fast retransmission.

Defaults The default rate is 50 percent.

Command Modes cs7 link submode

Command History	Release	Modification
	12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.

Usage Guidelines The **retransmit-cwnd-rate** command allows the administrator to configure a rate at which the SCTP congestion window is decreased due to retransmission timer expiration. The administrator can select one of two methods for setting the congestion window as a result of the retransmission timer expiration: Either set the congestion window to the defaults as defined in RFC 2960 or RFC 4960 or set the congestion window in the same way as for a fast retransmission.

The behavior of the SCTP congestion control algorithms is not compliant with RFC 2960 or RFC 4960 when this command is changed to values other than the default. This command should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples The following example shows how to set the rate for reducing the congestion window to 70 percent due to a retransmission timer expiration:

```
cs7 linkset michael 10.1.1
link 0 sctp 172.18.44.147 7000 7000

retransmit-cwnd-rate 70
```

Related Commands

Command	Description
retransmit-timeout (cs7 link)	Configures the minimum retransmission timeout value for the association.

retransmit-cwnd-rate (cs7 m2pa profile)

To configure the rate at which the SCTP congestion window size is reduced due to retransmission timer expiration, use the **retransmit-cwnd-rate** command in cs7 m2pa profile configuration mode. To disable the configuration, use the **no** form of this command.

retransmit-cwnd-rate *percent* [**sctp-fast-retransmit**]

no retransmit-cwnd-rate *percent* [**sctp-fast-retransmit**]

Syntax Description	<i>percent</i>	Rate at which the size of the SCTP congestion window is decreased due to retransmission timer expiration. Range is 0 to 100 percent. The default is 50 percent.
	sctp-fast-retransmit	(Optional) Indicates that the setting of the SCTP congestion window should follow the rules as defined for an SCTP fast retransmission.

Defaults The default rate is 50 percent.

Command Modes cs7 m2pa profile configuration

Command History	Release	Modification
	12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.

Usage Guidelines The **retransmit-cwnd-rate** command allows the administrator to configure a rate at which the SCTP congestion window is decreased due to retransmission timer expiration. The administrator can select one of two methods for setting the congestion window as a result of the retransmission timer expiration: Either set the congestion window to the defaults as defined in RFC 2960 or RFC 4960 or set the congestion window in the same way as for a fast retransmission.

The behavior of the SCTP congestion control algorithms is not compliant with RFC 2960 or RFC 4960 when this command is changed to values other than the default. This command should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples The following example shows how to define a profile named m2parfc. The profile supports M2PA RFC, specifies the **retransmit-cwnd-rate** command, and applies to all the links in the linkset named to_nyc.

```
cs7 profile m2parfc
 m2pa
  retransmit-cwnd-rate 70
.
.
.
cs7 linkset to_nyc
```

```
profile m2parfc
```

Related Commands

Command	Description
m2pa	Specifies M2PA parameters in a CS7 profile.

retransmit-cwnd-rate (cs7 m3ua)

To configure the rate at which the SCTP congestion window size is reduced due to retransmission timer expiration, use the **retransmit-cwnd-rate** *cs7 m3ua* submode command. To disable the configuration, use the **no** form of this command.

retransmit-cwnd-rate *percent* [**sctp-fast-retransmit**]

no retransmit-cwnd-rate *percent* [**sctp-fast-retransmit**]

Syntax Description

<i>percent</i>	Rate at which the size of the SCTP congestion window is decreased due to retransmission timer expiration. Range is 0 to 100 percent. The default is 50 percent.
sctp-fast-retransmit	(Optional) Indicates that the setting of the SCTP congestion window should follow the rules as defined for an SCTP fast retransmission.

Defaults

The default rate is 50 percent.

Command Modes

cs7 m3ua submode

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The **retransmit-cwnd-rate** command allows the administrator to configure a rate at which the SCTP congestion window is decreased due to retransmission timer expiration. The administrator can select one of two methods for setting the congestion window as a result of the retransmission timer expiration: Either set the congestion window to the defaults as defined in RFC 2960 or RFC 4960 or set the congestion window in the same way as for a fast retransmission.



Caution

The behavior of the SCTP congestion control algorithms is not compliant with RFC 2960 or RFC 4960 when this command is changed to values other than the default. This command should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples

The following example shows how to set the rate for reducing the congestion window to 70 percent due to a retransmission timer expiration:

```
cs7 m3ua 2905
  local-ip 4.4.4.4

    retransmit-cwnd-rate 70
```


Related Commands

Command	Description
retransmit-timeout (cs7 m3ua)	Configures the minimum retransmission timeout value for the association.

retransmit-cwnd-rate (cs7 mated-sg)

To configure the rate at which the SCTP congestion window size is reduced due to retransmission timer expiration, use the **retransmit-cwnd-rate** *cs7 mated-sg* submode command. To disable the configuration, use the **no** form of this command.

retransmit-cwnd-rate *percent* [**sctp-fast-retransmit**]

no retransmit-cwnd-rate *percent* [**sctp-fast-retransmit**]

Syntax Description	<i>percent</i>	Rate at which the size of the SCTP congestion window is decreased due to retransmission timer expiration. Range is 0 to 100 percent. The default is 50 percent.
	sctp-fast-retransmit	(Optional) Indicates that the setting of the SCTP congestion window should follow the rules as defined for an SCTP fast retransmission.

Defaults The default rate is 50 percent.

Command Modes *cs7 mated-sg* submode

Command History	Release	Modification
	12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.

Usage Guidelines The **retransmit-cwnd-rate** command allows the administrator to configure a rate at which the SCTP congestion window is decreased due to retransmission timer expiration. The administrator can select one of two methods for setting the congestion window as a result of the retransmission timer expiration: Either set the congestion window to the defaults as defined in RFC 2960 or RFC 4960 or set the congestion window in the same way as for a fast retransmission.

The behavior of the SCTP congestion control algorithms is not compliant with RFC 2960 or RFC 4960 when this command is changed to values other than the default. This command should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples The following example shows how to set the rate for reducing the congestion window to 70 percent due to a retransmission timer expiration:

```
cs7 mated-sg BLUE 5000
remote-ip 5.5.5.5

retransmit-cwnd-rate 70
```

Related Commands

Command	Description
retransmit-timeout (cs7 mated-sg)	Configures the minimum retransmission timeout value for the association.

retransmit-cwnd-rate (cs7)

To configure the rate at which the SCTP congestion window size is reduced due to retransmission timer expiration, use the **retransmit-cwnd-rate cs7** submode command. To disable the configuration, use the **no** form of this command.

retransmit-cwnd-rate *percent* [**sctp-fast-retransmit**]

no retransmit-cwnd-rate *percent* [**sctp-fast-retransmit**]

Syntax Description	<i>percent</i>	Rate at which the size of the SCTP congestion window is decreased due to retransmission timer expiration. Range is 0 to 100 percent. The default is 50 percent.
	sctp-fast-retransmit	(Optional) Indicates that the setting of the SCTP congestion window should follow the rules as defined for an SCTP fast retransmission.

Defaults The default rate is 50 percent.

Command Modes cs7 submode

Command History	Release	Modification
	12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.

Usage Guidelines The **retransmit-cwnd-rate** command allows the administrator to configure a rate at which the SCTP congestion window is decreased due to retransmission timer expiration. The administrator can select one of two methods for setting the congestion window as a result of the retransmission timer expiration: Either set the congestion window to the defaults as defined in RFC 2960 or RFC 4960 or set the congestion window in the same way as for a fast retransmission.

The behavior of the SCTP congestion control algorithms is not compliant with RFC 2960 or RFC 4960 when this command is changed to values other than the default. This command should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples The following example shows how to set the rate for reducing the congestion window to 70 percent due to a retransmission timer expiration:

```
cs7 5000
local-ip 4.4.4.4

retransmit-cwnd-rate 70
```

Related Commands

Command	Description
retransmit-timeout (cs7)	Configures the minimum retransmission timeout value for the association.

retransmit-cwnd-rate (cs7 sua)

To configure the rate at which the SCTP congestion window size is reduced due to retransmission timer expiration, use the **retransmit-cwnd-rate** *cs7 sua* submode command. To disable the configuration, use the **no** form of this command.

retransmit-cwnd-rate *percent* [**sctp-fast-retransmit**]

no retransmit-cwnd-rate *percent* [**sctp-fast-retransmit**]

Syntax Description	<i>percent</i>	Rate at which the size of the SCTP congestion window is decreased due to retransmission timer expiration. Range is 0 to 100 percent. The default is 50 percent.
	sctp-fast-retransmit	(Optional) Indicates that the setting of the SCTP congestion window should follow the rules as defined for an SCTP fast retransmission.

Defaults The default rate is 50 percent.

Command Modes *cs7 sua* submode

Command History	Release	Modification
	12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.

Usage Guidelines The **retransmit-cwnd-rate** command allows the administrator to configure a rate at which the SCTP congestion window is decreased due to retransmission timer expiration. The administrator can select one of two methods for setting the congestion window as a result of the retransmission timer expiration: Either set the congestion window to the defaults as defined in RFC 2960 or RFC 4960 or set the congestion window in the same way as for a fast retransmission.

The behavior of the SCTP congestion control algorithms is not compliant with RFC 2960 or RFC 4960 when this command is changed to values other than the default. This command should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples The following example shows how to set the rate for reducing the congestion window to 70 percent due to a retransmission timer expiration:

```
cs7 sua 15000
  local-ip 4.4.4.4

  retransmit-cwnd-rate 70
```

Related Commands

Command	Description
retransmit-timeout (cs7 sua)	Configures the minimum retransmission timeout value for the association.

retransmit-timeout (cs7 asp)

To configure the minimum retransmission timeout value for the association, use the **retransmit-timeout** cs7 asp submode command. To disable the timeout value, use the **no** form of this command.

retransmit-timeout *rto-min rto-max*

no retransmit-timeout

Syntax Description	<i>rto-min</i>	Retransmission timeout minimum value in milliseconds. Range is 40 to 60000 milliseconds. The default is the value specified under the local port instance.
	<i>rto-max</i>	Retransmission timeout maximum value in milliseconds. Range is 40 to 60000 milliseconds. The default is 1000 milliseconds.

Defaults	The default <i>rto-min</i> value is 1000 milliseconds.
	The default <i>rto-max</i> value is 1000 milliseconds.

Command Modes	cs7 asp submode

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	The retransmission timeout (RTO) should be adjusted for round-trip delay between nodes. Preferably, the retransmission timeout should be greater than the round-trip delay between nodes. You will have to compromise between allowing a long delay and having responsive discovery of lost frames. You can calculate a general estimate of round-trip times (rtt) for various packet sizes (ignoring propagation delay and latencies in transmission equipment) using the following equation:

$$\text{estimated rtt} = ((\text{packet size} * \text{bits per byte}) / \text{link speed}) * 2$$

For example, if a packet has a 20-byte IP header, a 32-byte SCTP header, 100 bytes of user data, and a 1,544,000-bits/sec link between two nodes, the estimated rtt is 1.5 ms.

SCTP computes RTO values based on rtt measurements. When packet retransmission occurs, the timeout value is doubled for each retransmission, with an upper limit of *rto-max*. Multihomed nodes have to compromise between allowing a long delay and having responsive switching to an alternate IP address, which is important for multihomed nodes. The maximum RTO value for multihomed nodes should be set equal to or just slightly higher than the minimum RTO value. The number of outstanding bytes allowed decreases with each retransmission timeout. The trade-off of bounding the maximum RTO close to the minimum RTO is the frequency of retransmissions versus increasing transmit delays for packets on the transmit queue. During periods of retransmissions multihomed nodes send duplicate packets until

the alternate address becomes the primary path. The alternate address becomes the primary path when the number of retries exceeds the path-retransmit parameter. The default value for minimum and maximum RTO is 1 second. Propagation delays and latencies vary in networks, so select an RTO value carefully.

Examples

The following example shows how to set the minimum value of the retransmit timeout to 300 milliseconds and the maximum value to 3000 milliseconds:

```
cs7 asp ASP1 2904 2905 m3ua
remote-ip 1.1.1.1
retransmit-timeout 300 3000
```

Related Commands

Command	Description
cs7 asp	Specifies an application server process (ASP) and enables cs7 asp submode.

retransmit-timeout (cs7 link)

To configure the retransmission timeout value on a link, use the **retransmit-timeout** cs7 link submode command. To disable the timeout value, use the **no** form of this command.

retransmit-timeout *rto-min rto-max*

no retransmit-timeout

Syntax Description

<i>rto-min</i>	Retransmission timeout minimum value in milliseconds. Range is 40 to 60000 milliseconds. The default is 1000 milliseconds.
<i>rto-max</i>	Retransmission timeout maximum value in milliseconds. Range is 40 to 60000 milliseconds. The default is 1000 milliseconds.

Defaults

The default *rto-min* value is 1000 milliseconds.

The default *rto-max* value is 1000 milliseconds.

Command Modes

cs7 link submode

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The retransmission timeout (RTO) should be adjusted for round-trip delay between nodes. Preferably, the retransmission timeout should be greater than the round-trip delay between nodes. You will have to compromise between allowing a long delay and having responsive discovery of lost frames. You can calculate a general estimate of round-trip times (rtt) for various packet sizes (ignoring propagation delay and latencies in transmission equipment) using the following equation:

$$\text{estimated rtt} = ((\text{packet size} * \text{bits per byte}) / \text{link speed}) * 2$$

For example, if a packet has a 20-byte IP header, a 32-byte SCTP header, 100 bytes of user data, and a 1,544,000-bits/sec link between two nodes, the estimated rtt is 1.5 ms.

SCTP computes RTO values based on rtt measurements. When packet retransmission occurs, the timeout value is doubled for each retransmission, with an upper limit of *rto-max*. Multihomed nodes have to compromise between allowing a long delay and having responsive switching to an alternate IP address, which is important for multihomed nodes. The maximum RTO value for multihomed nodes should be set equal to or just slightly higher than the minimum RTO value. The number of outstanding bytes allowed decreases with each retransmission timeout. The trade-off of bounding the maximum RTO close to the minimum RTO is the frequency of retransmissions versus increasing transmit delays for packets on the transmit queue. During periods of retransmissions multihomed nodes send duplicate packets until the alternate address becomes the primary path. The alternate address becomes the primary path when

the number of retries exceeds the path-retransmit parameter. The default value for minimum and maximum RTO is 1 second. Propagation delays and latencies vary in networks, so select an RTO value carefully.

Examples

The following example shows how to set the value of the minimum retransmit timeout to 300 milliseconds and the maximum value to 30000 milliseconds:

```
cs7 linkset michael 10.1.1
link 0 sctp 172.18.44.147 7000 7000
  retransmit-timeout 300 30000
```

Related Commands

Command	Description
show cs7 m2pa	Displays M2PA statistics.

retransmit-timeout (cs7 m2pa profile)

To configure the retransmission timeout value on a link, use the **retransmit-timeout** command in cs7 m2pa profile configuration mode. To disable the timeout value, use the **no** form of this command.

retransmit-timeout *rto-min rto-max*

no retransmit-timeout

Syntax Description	<i>rto-min</i>	Retransmission timeout minimum value in milliseconds. Range is 40 to 60000 milliseconds. The default is 1000 milliseconds.
	<i>rto-max</i>	Retransmission timeout maximum value in milliseconds. Range is 40 to 60000 milliseconds. The default is 1000 milliseconds.

Defaults	The default <i>rto-min</i> value is 1000 milliseconds.
	The default <i>rto-max</i> value is 1000 milliseconds.

Command Modes	cs7 m2pa profile configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	The retransmission timeout (RTO) should be adjusted for round-trip delay between nodes. Preferably, the retransmission timeout should be greater than the round-trip delay between nodes. You will have to compromise between allowing a long delay and having responsive discovery of lost frames. You can calculate a general estimate of round-trip times (rtt) for various packet sizes (ignoring propagation delay and latencies in transmission equipment) using the following equation:

$$\text{estimated rtt} = ((\text{packet size} * \text{bits per byte}) / \text{link speed}) * 2$$

For example, if a packet has a 20-byte IP header, a 32-byte SCTP header, 100 bytes of user data, and a 1,544,000-bits/sec link between two nodes, the estimated rtt is 1.5 ms.

SCTP computes RTO values based on rtt measurements. When packet retransmission occurs, the timeout value is doubled for each retransmission, with an upper limit of *rto-max*. Multihomed nodes have to compromise between allowing a long delay and having responsive switching to an alternate IP address, which is important for multihomed nodes. The maximum RTO value for multihomed nodes should be set equal to or just slightly higher than the minimum RTO value. The number of outstanding bytes allowed decreases with each retransmission timeout. The trade-off of bounding the maximum RTO close to the minimum RTO is the frequency of retransmissions versus increasing transmit delays for packets on the transmit queue. During periods of retransmissions multihomed nodes send duplicate packets until the alternate address becomes the primary path. The alternate address becomes the primary path when

the number of retries exceeds the path-retransmit parameter. The default value for minimum and maximum RTO is 1 second. Propagation delays and latencies vary in networks, so select an RTO value carefully.

Examples

The following example shows how to define a profile named m2parfc. The profile supports M2PA RFC, specifies the **retransmit-timeout** command, and applies to all the links in the linkset named to_nyc.

```
cs7 profile m2parfc
  m2pa
    retransmit-timeout 300 30000
  .
  .
  .
cs7 linkset to_nyc
  profile m2parfc
```

Related Commands

Command	Description
m2pa	Specifies M2PA parameters in a CS7 profile.

retransmit-timeout (cs7 m3ua)

To configure the minimum retransmission timeout value used when a new SCTP association is started, use the **retransmit-timeout** cs7 m3ua submode command. To disable the timeout value, use the **no** form of this command.

retransmit-timeout *rto-min rto-max*

no retransmit-timeout

Syntax Description

<i>rto-min</i>	Retransmission timeout minimum value in milliseconds. Range is 40 to 60000 milliseconds. The default is 1000 milliseconds.
<i>rto-max</i>	Retransmission timeout maximum value in milliseconds. Range is 40 to 60000 milliseconds. The default is 1000 milliseconds

Defaults

The default *rto-min* value is 1000 milliseconds.

The default *rto-max* value is 1000 milliseconds.

Command Modes

cs7 m3ua submode

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The retransmission timeout (RTO) should be adjusted for round-trip delay between nodes. Preferably, the retransmission timeout should be greater than the round-trip delay between nodes. You will have to compromise between allowing a long delay and having responsive discovery of lost frames. You can calculate a general estimate of round-trip times (rtt) for various packet sizes (ignoring propagation delay and latencies in transmission equipment) using the following equation:

$$\text{estimated rtt} = ((\text{packet size} * \text{bits per byte}) / \text{link speed}) * 2$$

For example, if a packet has a 20-byte IP header, a 32-byte SCTP header, 100 bytes of user data, and a 1,544,000-bits/sec link between two nodes, the estimated rtt is 1.5 ms.

SCTP computes RTO values based on rtt measurements. When packet retransmission occurs, the timeout value is doubled for each retransmission, with an upper limit of *rto-max*. Multihomed nodes have to compromise between allowing a long delay and having responsive switching to an alternate IP address, which is important for multihomed nodes. The maximum RTO value for multihomed nodes should be set equal to or just slightly higher than the minimum RTO value. The number of outstanding bytes allowed decreases with each retransmission timeout. The trade-off of bounding the maximum RTO close to the minimum RTO is the frequency of retransmissions versus increasing transmit delays for packets on the transmit queue. During periods of retransmissions multihomed nodes send duplicate packets until

the alternate address becomes the primary path. The alternate address becomes the primary path when the number of retries exceeds the path-retransmit parameter. The default value for minimum and maximum RTO is 1 second. Propagation delays and latencies vary in networks, so select an RTO value carefully.

Examples

The following example shows how to set the minimum value of the retransmit timeout to 300 milliseconds and the maximum value to 3000 milliseconds:

```
cs7 m3ua 2905
local-ip 4.4.4.4
retransmit-timeout 300 3000
```

Related Commands

Command	Description
cs7 m3ua	Specifies the local port number for M3UA and enters cs7 m3ua submode.

retransmit-timeout (cs7 mated-sg)

To configure the minimum retransmission timeout value for the association, use the **retransmit-timeout** cs7 mated-sg submode command. To disable the timeout value, use the **no** form of this command.

retransmit-timeout *rto-min rto-max*

no retransmit-timeout

Syntax Description

<i>rto-min</i>	Retransmission timeout minimum value in milliseconds. Range is 40 to 60000 milliseconds. The default is the value specified under the local port instance.
<i>rto-max</i>	Retransmission timeout maximum value in milliseconds. Range is 40 to 60000 milliseconds. The default is 1000 milliseconds.

Defaults

The retransmission timeout minimum value default is the value specified under the local port instance. The retransmission timeout maximum value default is 1000 milliseconds.

Command Modes

cs7 mated-sg submode

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The retransmission timeout (RTO) should be adjusted for round-trip delay between nodes. Preferably, the retransmission timeout should be greater than the round-trip delay between nodes. You will have to compromise between allowing a long delay and having responsive discovery of lost frames. You can calculate a general estimate of round-trip times (rtt) for various packet sizes (ignoring propagation delay and latencies in transmission equipment) using the following equation:

$$\text{estimated rtt} = ((\text{packet size} * \text{bits per byte}) / \text{link speed}) * 2$$

For example, if a packet has a 20-byte IP header, a 32-byte SCTP header, 100 bytes of user data, and a 1,544,000-bits/sec link between two nodes, the estimated rtt is 1.5 ms.

SCTP computes RTO values based on rtt measurements. When packet retransmission occurs, the timeout value is doubled for each retransmission, with an upper limit of *rto-max*. Multihomed nodes have to compromise between allowing a long delay and having responsive switching to an alternate IP address, which is important for multihomed nodes. The maximum RTO value for multihomed nodes should be set equal to or just slightly higher than the minimum RTO value. The number of outstanding bytes allowed decreases with each retransmission timeout. The trade-off of bounding the maximum RTO close to the minimum RTO is the frequency of retransmissions versus increasing transmit delays for packets on the transmit queue. During periods of retransmissions multihomed nodes send duplicate packets until the alternate address becomes the primary path. The alternate address becomes the primary path when

the number of retries exceeds the path-retransmit parameter. The default value for minimum and maximum RTO is 1 second. Propagation delays and latencies vary in networks, so select an RTO value carefully.

Examples

The following example shows how to set the minimum value of the retransmit timeout to 300 milliseconds and the maximum value to 3000 milliseconds:

```
cs7 mated-sg BLUE 2905
  remote-ip 5.5.5.5
  retransmit-timeout 300 3000
```

Related Commands

Command	Description
cs7 mated-sg	Configures a connection to a mated SG.

retransmit-timeout (cs7)

To configure the minimum retransmission timeout value used when a new SCTP association is started, use the **retransmit-timeout** *cs7* submode command. To disable the timeout value, use the **no** form of this command.

retransmit-timeout *rto-min rto-max*

no retransmit-timeout

Syntax Description

<i>rto-min</i>	Retransmission timeout minimum value in milliseconds. Range is 40 to 60000 milliseconds. The default is 1000 milliseconds.
<i>rto-max</i>	Retransmission timeout maximum value in milliseconds. Range is 40 to 60000 milliseconds. The default is 1000 milliseconds.

Defaults

The default *rto-min* value is 1000 milliseconds.

The default *rto-max* value is 1000 milliseconds.

Command Modes

cs7 submode

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The retransmission timeout (RTO) should be adjusted for round-trip delay between nodes. Preferably, the retransmission timeout should be greater than the round-trip delay between nodes. You will have to compromise between allowing a long delay and having responsive discovery of lost frames. You can calculate a general estimate of round-trip times (rtt) for various packet sizes (ignoring propagation delay and latencies in transmission equipment) using the following equation:

$$\text{estimated rtt} = ((\text{packet size} * \text{bits per byte}) / \text{link speed}) * 2$$

For example, if a packet has a 20-byte IP header, a 32-byte SCTP header, 100 bytes of user data, and a 1,544,000-bits/sec link between two nodes, the estimated rtt is 1.5 ms.

SCTP computes RTO values based on rtt measurements. When packet retransmission occurs, the timeout value is doubled for each retransmission, with an upper limit of *rto-max*. Multihomed nodes have to compromise between allowing a long delay and having responsive switching to an alternate IP address, which is important for multihomed nodes. The maximum RTO value for multihomed nodes should be set equal to or just slightly higher than the minimum RTO value. The number of outstanding bytes allowed decreases with each retransmission timeout. The trade-off of bounding the maximum RTO close to the minimum RTO is the frequency of retransmissions versus increasing transmit delays for packets on the transmit queue. During periods of retransmissions multihomed nodes send duplicate packets until

the alternate address becomes the primary path. The alternate address becomes the primary path when the number of retries exceeds the path-retransmit parameter. The default value for minimum and maximum RTO is 1 second. Propagation delays and latencies vary in networks, so select an RTO value carefully.

Examples

The following example shows how to set the minimum value of the retransmit timeout to 300 milliseconds and the maximum value to 3000 milliseconds:

```
cs7 5000
local-ip 4.4.4.4
retransmit-timeout 300 3000
```

Related Commands

Command	Description
cs7 sgmp	Establishes an association to the mated SG.

retransmit-timeout (cs7 sua)

To configure the minimum retransmission timeout value used when a new SCTP association is started, use the **retransmit-timeout** cs7 sua submode command. To disable the timeout value, use the **no** form of this command.

retransmit-timeout *rto-min rto-max*

no retransmit-timeout

Syntax Description

<i>rto-min</i>	Retransmission timeout minimum value in milliseconds. Range is 40 to 60000 milliseconds. The default is 1000 milliseconds.
<i>rto-max</i>	Retransmission timeout maximum value in milliseconds. Range is 40 to 60000 milliseconds. The default is 1000 milliseconds.

Defaults

The default *rto-min* value is 1000 milliseconds.

The default *rto-max* value is 1000 milliseconds.

Command Modes

cs7 sua submode

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The retransmission timeout (RTO) should be adjusted for round-trip delay between nodes. Preferably, the retransmission timeout should be greater than the round-trip delay between nodes. You will have to compromise between allowing a long delay and having responsive discovery of lost frames. You can calculate a general estimate of round-trip times (rtt) for various packet sizes (ignoring propagation delay and latencies in transmission equipment) using the following equation:

$$\text{estimated rtt} = ((\text{packet size} * \text{bits per byte}) / \text{link speed}) * 2$$

For example, if a packet has a 20-byte IP header, a 32-byte SCTP header, 100 bytes of user data, and a 1,544,000-bits/sec link between two nodes, the estimated rtt is 1.5 ms.

SCTP computes RTO values based on rtt measurements. When packet retransmission occurs, the timeout value is doubled for each retransmission, with an upper limit of *rto-max*. Multihomed nodes have to compromise between allowing a long delay and having responsive switching to an alternate IP address, which is important for multihomed nodes. The maximum RTO value for multihomed nodes should be set equal to or just slightly higher than the minimum RTO value. The number of outstanding bytes allowed decreases with each retransmission timeout. The trade-off of bounding the maximum RTO close to the minimum RTO is the frequency of retransmissions versus increasing transmit delays for packets on the transmit queue. During periods of retransmissions multihomed nodes send duplicate packets until

the alternate address becomes the primary path. The alternate address becomes the primary path when the number of retries exceeds the path-retransmit parameter. The default value for minimum and maximum RTO is 1 second. Propagation delays and latencies vary in networks, so select an RTO value carefully.

Examples

The following example shows how to set the minimum value of the retransmit timeout to 300 milliseconds and the maximum value to 3000 milliseconds:

```
cs7 sua 15000
local-ip 4.4.4.4
retransmit-timeout 300 3000
```

Related Commands

Command	Description
cs7 sua	Specifies the local port number for SUA and enters cs7 sua submode.

rotate-sls

To enable SLS rotation, use the **rotate-sls** cs7 linkset submode command. To disable the SLS rotation, use the **no** form of this command.

rotate-sls [*bits*]

no rotate-sls

Syntax Description	<i>bits</i> (Optional) Number of bits to rotate. The range is 1 to 4. The default number is 1.

Defaults	SLS rotation is enabled by default for ANSI linksets.

Command Modes	cs7 linkset submode

Command History	Release	Modification
	12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.
	12.4(15)SW2	The <i>bits</i> argument was introduced.
	 Note	This modification applies only to the 12.4(15)SW release train. It does not currently apply to any ITP software release for the Cisco 7600 router.

Usage Guidelines	In ANSI networks, before transmitting an MSU over an MTP3 link, a node performs SLS rotation—changing the SLS field in the MSU by shifting the lower five bits to the right and moving the first bit to the fifth bit. This feature is described in <i>GR-246, Section T1.115.1 Chapter 7</i> .

An SLS value of X7 X6 X5 X4 X3 X2 X1 X0 changes to X7 X6 X5 X0 X4 X3 X2 X1. Because M3UA and SUA nodes might not perform SLS rotation, or might use different schemes for load sharing between multiple ITPs, this enhancement adds a configurable option for an AS to perform ANSI rotation on incoming MSUs before link and linkset selection.

SLS rotation also includes the option to shift these bits by more than one place. For example, if **rotate-sls 4** is configured, then instead of doing the normal ANSI rotation, the ITP shifts the SLS link this way:

X7 X6 X5 X4 X3 X2 X1 X0 changes to X7 X6 X5 X3 X3 X1 X0 X4

Note that unlike the **shift-sls** option in the ITU variant, this option changes the field in the MSU being transmitted later.

Examples

The following example shows how to disable SLS rotation:

```
no rotate-sls
```

The following example shows how to enable an SLS rotation of 2:

```
rotate-sls 2
```

Related Commands

Command	Description
cs7 linkset	Configures a linkset.

routing-key (cs7 as)

To configure the routing key, use the **routing-key cs7 as** submode command. To remove the configuration, use the **no** form of this command.

M3UA AS Syntax

```
routing-key rcontext {gtt | dpc [opc pc pc-mask] [si {aal2 | bicc | b-isup | h248 | isup| sat-isup |
sccp | tup}] [[cic cic-min [cic-max]] | [ssn ssn]]}]
```

no routing-key

SUA AS Syntax

```
routing-key rcontext {gtt | dpc [opc pc pc-mask] [si sccp] [[cic cic-min [cic-max]] | [ssn ssn]]}]
```

no routing-key

Syntax Description

<i>rcontext</i>	The routing context parameter is an unsigned decimal number that uniquely identifies a routing key. An ASP may include the routing context in the ASP Active Request to register receiving traffic for a specific AS.
gtt	Global title translation. (Configuring GTT implies a sccp service indicator.)
<i>dpc</i>	Destination point code indicating the point code associated with this AS and routing key. This destination point code may be unique or share the SG's local point code, secondary point code, or capability point code. An M3UA AS or an SUA AS can share only one of the router's local point codes. For more information, refer to “Point Code Assignment and Management” in the Usage Guidelines section.
opc	Originating point code, which further limits traffic directed to an AS to traffic from a specific point code.
<i>pc</i>	Originating point code.
<i>pc-mask</i>	Point code mask, which allows you to specify a range of originating point codes by indicating the number of significant bits.
si	Service indicator. You can specify a service indicator of either isup or sccp. (This parameter applies to M3UA ASes only. SUA ASes imply an sccp service indicator.)
aal2	AAL2 service indicator (M3UA only).
bicc	BICC service indicator (M3UA only).
b-isup	B ISUP service indicator (M3UA only).
h248	GCP service indicator (M3UA only).
isup	ISUP service indicator (M3UA only).
sat-isup	Satellite ISUP service indicator (M3UA only).
sccp	SCCP service indicator.
tup	TUP service indicator (M3UA only).
<i>cic-min</i>	CIC number or minimum value in a CIC range.
<i>cic-max</i>	Maximum value in a CIC range.

ssn	Subsystem number. (This parameter applies to SUA ASes only. Configuring SSN implies an sccp service indicator.)
<i>ssn</i>	Subsystem number value.

Defaults

None.

Command Modes

cs7 as submode

Command History

Release	Modification
12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.
12.2(18)IXH 12.4(15)SW3 12.2(33)IRC	Additional service indicators were added.

Usage Guidelines

The routing key describes a set of SS7 parameters and parameter values that uniquely define the range of signaling traffic to be handled by a particular AS. Routing key provisioning ensures that traffic is routed correctly. Routing key combinations vary for M3UA and SUA.

If CS7 multiple instance is configured, duplicate routing keys are allowed for ASes or AS routes in different instances.

The ITP SG uses the routing key table to map incoming SS7 messages to the appropriate AS or AS route table. Relevant fields of the incoming SS7 messages are compared to the existing routing keys. An AS is selected based on the best matching routing key. The routing keys are prioritized by selecting the best matching gtt keys first, followed by the longest matching routing key at the highest layer in the protocol stack.

The following list shows the routing key combinations in order of priority. The dpc must match for a non-GTT AS to be selected.

- gtt
- dpc + sccp + ssn + opc or dpc + isup + cic + opc
- dpc + sccp + ssn or dpc + isup + cic
- dpc + sccp + opc or dpc + isup + opc
- dpc + sccp or dpc + isup
- dpc + opc
- dpc

Valid routing key combinations vary for M3UA and SUA.

Routing Key Definitions for M3UA

For M3UA ASes, the routing key has the following parameters:

```
routing-key rcontext {gtt [gtt-selector-name [gtt-gta]] | dpc [opc pc pc-mask] [si {aal2 | bicc |
b-isup | h248 | isup| sat-isup | sccp | tup}] cic-min [cic-max]}
```

Specify the following parameters to configure a routing key for M3UA GTT traffic. SI SCCP is enabled by default.

```
routing-key rcontext {gtt [gtt-selector-name [gtt-gta]]
```

Specify the following parameters to configure a routing key for M3UA ISUP traffic. If **cic** is selected, then **si isup** is enabled by default.

```
routing-key rcontext dpc [opc pc pc-mask] si isup [cic cic-min [cic-max]]
```

Use the following parameters to configure a routing key for M3UA SSN traffic. **si sccp** is enabled by default.

```
routing-key rcontext dpc [opc pc pc-mask] si sccp ssn ssn
```

Routing Key Definitions for SUA

For SUA ASes, the routing key has the following parameters. SUA supports **si sccp** only.

```
routing-key rcontext {gtt [gtt-selector-name [gtt-gta]] | dpc [opc pc pc-mask] si sccp [ssn ssn]}
```

To configure a routing key for SUA TCAP traffic:

```
routing-key rcontext dpc [opc pc pc-mask] si sccp ssn ssn
```

To configure a routing key for SUA GTT traffic:

```
routing-key rcontext {gtt [gtt-selector-name [gtt-gta]]
```

Point Code Assignment and Management

Take special care when planning the assignment of point codes to ASes. The ITP SG feature allows point code assignment to ASes and ASPs as follows:

- An AS may be assigned the primary local point code or secondary local point code owned by the SG. The AS is sharing the point code with the SG.
- An AS may be assigned a capability code or alias point code of the SG. The AS is sharing the point code with the SG's mated pair.
- An AS may be assigned a unique point code not previously assigned to any of the SGs in the mated-pair.
- An ASP can be assigned a unique point code by being the only ASP in an AS that has been assigned a unique point code.
- All ASes or groups of ASes serviced by the SG may share a given point code. Any group of ASes that shares the same point code is referred to as a Signaling Point Management Cluster (SPMC). Note that an M3UA AS and an SUA AS may share only one of the router's point codes (primary local, secondary local, or capability).

Assigning more than one AS the same point code can have significant effect on the ability of the SG to report ASP, AS, user part, or subsystem outages or unavailability to the SS7 network. Consider the following case:

AS1 and AS2 are sharing point code 2.2.2 in the same network appearance. AS1 handles ISUP traffic for CIC 1 to 500. AS2 handles ISUP traffic for CIC 501 to 1000 from the same OPC. AS1 and AS2 have no ASPs in common. If all of the ASPs in AS1 become unavailable, the SG cannot send a TFP to the SS7 network. Sending a TFP would inaccurately indicate that point code 2.2.2 is totally unreachable through the SG when only a subset of the ASPs in point code 2.2.2 are unreachable. If AS1 and AS2 each had its own point code, then the SG would be able send a TFP to the SS7 network.

Unallocated MSU processing

When an MSU is received and does not match any of the configured routing keys, that MSU is referred to as an unallocated MSU. The default treatment for unallocated messages varies. If a trap has been enabled for unallocated messages, the DPC, OPC, and SIO of an unallocated MSU are reported to the designated management entity. If the unallocated MSU trap has not been enabled, the MSU is counted and dropped.

To prevent the MSU from being dropped, you can configure routing keys with minimal parameters to catch traffic that does not match more specific routing keys. For example, in the case of ISUP traffic, the following configuration catches errant ISUP traffic for tracking purposes:

```
cs7 as defaultisup m3ua
  routingkey 222 dpc 2.3.3 si isup
  asp isupbucket
```

All ISUP traffic for DPC 2.3.3 that does not match the CIC range of one of the more specific routing keys is sent to the isupbucket ASP. Note that, if the isupbucket ASP is not active, the MSU is dropped with the appropriate warning.

Examples

The following examples show how to configure routing key provisioning:

```
cs7 as as1 m3ua
  routing-key 01010101 gtt

cs7 as as2 m3ua
  routing-key 02020202 2.2.2

cs7 as as3 m3ua
  routing-key 03030303 3.3.3 opc 5.5.5 255.255.128

cs7 as as4 sua
  routing-key 04040404 4.4.4 si sccp ssn 40
```

Related Commands

Command	Description
cs7 as	Defines an application server (AS) and enters cs7 as submode.

rule (cs7 mlr ruleset)

To specify the rules for a routing trigger within a multilayer ruleset table, use the **rule** command in cs7 mlr ruleset configuration mode. To disable the specific rule, use the **no** form of this command.

```
rule order {{ gsm-map | ansi-41 } operation-name [default] | all-operations | default-rule}
```

```
no rule order {{ gsm-map | ansi-41 } operation-name [default] | all-operations | default-rule}
```

Syntax Description		
<i>order</i>		Specifies the order in which rules are searched. The order must be unique among all rules. The routing table is sequentially searched for a match, with the rules being tested in the order specified. Valid numbers are 1 to 1000.
gsm-map ansi-41		Valid application layer protocols are gsm-map or ansi-41 . If you specify a protocol in the MLR ruleset, you cannot specify the protocol for a rule.
<i>operation-name</i>		Specifies the operation of the message that must be matched. Valid operation names are listed in the tables in the Usage Guidelines section.
default		Specifies the processing of messages that match the specified operation name only. Optional for all the operations supported but will be NVGENed for new operations, because only one rule can be configured for each new operation.
all-operations		Identifies a match of any valid operation code. If you specify a protocol at the MLR ruleset level, specifying all-operations in a rule applies only for that protocol.
default-rule		Matches default rule when no rule matches.

Defaults	None.

Command Modes	cs7 mlr ruleset configuration

Command History	Release	Modification
	12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.
	12.2(33)IRG 12.4(15)SW7	The mobileUSSD operation name was introduced.
	12.2(33)IRI 12.4(15)SW9	The default-rule operation name was introduced.

Usage Guidelines	The rule command specifies the attributes of an application-layer message to be matched, and the resulting behavior for handling the message. At least one rule must be specified for the ruleset to be valid. Enables mlr ruleset rule configuration mode.

The following command enters into the cs7 mlr set rule configuration submode:

```

ITP(cfg-cs7-mlr-set)# rule 1 default-rule ?
<cr>
ITP(cfg-cs7-mlr-set-rule)# ?
  allow-multi-message-dialogue  Allow multi-message-dialogues to match a default rule
  exit                          Exit from CS7 MLR rule configuration submode
  no                             Negate a command or set its defaults
  pam                           Apply a PAM during result processing
  result                         Configure result

```

Table 34 and Table 35 list GSM-MAP and GSM-MAP Version 1 operation names mapped to ITP operations names. Table 36 lists GSM operations that allow you to route and screen based on MAP parameters and MAP-User parameters.

Valid operation names are presented in the CLI depending on the specified protocol.

Table 34 GSM-MAP Operation Name Mapping to ITP CLI Operation Name

Operation Name in GSM-MAP Specification	ITP CLI Operation Name	Opcode Value
activatess	actSS	12
activateTraceMode	actTraceMode	50
alertServiceCentre)	alertSC	64
anyTimeInterrogation	anyTimeInterr	71
authenticationFailureReport	authFailRep	15
anyTimeModification	anyTimeMod	65
anyTimeSubscriptionInterrogation	anyTimeSubInterr	62
cancelLocation	cancelLoc	3
checkIMEI	checkIMEI	43
deactivateSS	deactSS	13
deactivateTraceMode	deactTraceMode	51
deleteSubscriberData	delSubData	8
eraseCC-Entry	eraseCCEntry	77
eraseSS	eraseSS	11
failureReport	failRep	25
forwardAccessSignalling	fwdAccessSig	34
forwardCheckSs-Indication	fwdCheckSsInd	38
forwardGroupCallSignalling	fwdGrpCallSig	42
mt-forwardSM	sms-mt	44
mo-forwardSM	sms-mo	46
getPassword	getPwd	18
informServiceCentre	informSC	63
insertSubscriberData	insSubData	7
interrogateSs	interrSS	14
istAlert	istAlert	87
istCommand	istCmd	88

Table 34 *GSM-MAP Operation Name Mapping to ITP CLI Operation Name (continued)*

Operation Name in GSM-MAP Specification	ITP CLI Operation Name	Opcode Value
unstructuredSS_Request	mobileUSSD	59
processUnstructuredSS-Request		
noteMsPresentForGprs	noteMsPresentForGprs	26
noteSubscriberDataModified	noteSubDataMod	5
prepareGroupCall	prepGrpCall	39
prepareHandover	prepHandover	68
prepareSubsequentHandover	prepSubsHandover	69
processAccessSignalling	processAccessSig	33
processGroupCallSignalling	processGrpCallSig	41
processUnstructuredSS-Request	processUnstructSSReq	59
provideRoamingNumber	provideRoamNumber	4
provideSIWFSNumber	provideSIWFSNumber	31
provideSubscriberLocation	provideSubLoc	83
provideSubscriberInfo	provideSubInfo	70
purgeMS	purgeMS	67
readyForSM	readyForSM	66
registerCC-Entry	regCCEntry	76
registerPassword	regPwd	17
registerSS	regSS	10
remoteUserFree	remoteUserFree	75
reportSmDeliveryStatus	repSmDeliveryStatus	47
reset	reset	37
restoreData	restoreData	57
resumeCallHandling	resumeCallHandling	6
secureTransportClass1	secureTransClass1	78
secureTransportClass2	secureTransClass2	79
secureTransportClass3	secureTransClass3	80
secureTransportClass4	secureTransClass4	81
sendGroupCallEndSignal	sendGrpCallEndSig	40
sendEndSignal	sendEndSig	29
sendAuthenticationInfo	sendAuthInfo	56
sendIdentification	sendId	55
sendIMSI	sendIMSI	58
sendRoutingInfoForSM	sri-sm	45
sendRoutingInfoForGprs	sri-gprs	24
sendRoutingInfoForLCS	sri-lcs	85

Table 34 *GSM-MAP Operation Name Mapping to ITP CLI Operation Name (continued)*

Operation Name in GSM-MAP Specification	ITP CLI Operation Name	Opcode Value
sendRoutingInfo	sri-call (route a call to the MS)	22
setReportingState	setRepState	73
SIWFSSignallingModify	SIWFSSigMod	32
statusReport	statusRep	74
subscriberLocationReport	subLocRep	86
ss-Invocation-Notification	ssInvocNot	72
unstructuredSS-Request	networkUSSD	60, 61
unstructuredSS-Notify		
updateGprsLocation	updGprsLoc	23
updateLocation	updLoc	2
NoteMM-Event	noteMMEvent	89

Table 35 *GSM-MAP Version 1 Operation Code Mapping to ITP CLI Operation Name*

GSM-MAP Version 1 Operation Code	ITP CLI Operation Name	Opcode Value
AlertServiceCenterWithoutResult	alertScWoResult	49
allocateForHandoverNumber	allocHandOverNum	31
attachIMSI	attachIMSI	6
Authenticate	authenticate	39
BeginSubscriberActivity	beginSubActivity	54
CompleteCall	completeCall	23
ConnectToFollowingAddress	connectFollowAddress	24
detachIMSI	detachIMSI	5
forwardNewTMSI	fwdNewTMSI	41
forwardSSNotification	fwdSSNot	16
invokeSS	invokeSS	15
NoteInternalHandover	noteIntHandOver	35
NoteMSPresent	noteMSPresent	48
Page	page	26
PerformHandover	performHandOver	28
PerformSubsequentHandover	performSubHandOver	30
ProcessAccessRequest	processAccessReq	53
processCallWaiting	processCallWait	25
ProcessUnstructuredSS-Data	processUnstructSSData	19
provideIMSI	provideIMSI	40
RegisterChargingInformation	regChargingInfo	36

Table 35 *GSM-MAP Version 1 Operation Code Mapping to ITP CLI Operation Name (continued)*

GSM-MAP Version 1 Operation Code	ITP CLI Operation Name	Opcode Value
searchForMobileSubscriber	searchForMobileSub	27
sendHandOverReport	sendHandOverRep	32
SendInfoForIncomingCall	sendInfoForIncCall	20
SendInfoForOutgoingCall	sendInfoForOutgCall	21
SendParameters	sendParams	9
setCipherringMode	setCipherMode	42
SetMessageWaitingData	setMsgWaitData	47
TraceSubscriberActivity	traceSubAct	52
updateLocationArea	updateLocArea	1

Table 36 *Valid Rule Parameters by Operation*

	alertSc	all	smdpp	sms-mo	sms-mt	smsNot	smsReq	sri-sm
dest-port				X	X			
dest-sme	X		X	X	X	X	X	X
dest-sme-table			X	X				
dest-smsc	X			X				
match-unknown-ton-np	X		X	X	X	X	X	X
multi-message-dialogue		X		X	X			
orig-imsi				X				
orig-imsi-table				X				
orig-sme			X	X	X			
orig-sme-table			X	X				
orig-smsc					X			X
pid				X	X			
teleservice			X			X	X	

Examples

In the following example, any MSU that does not match the two defined DPC triggers will match the default trigger. Ruleset GEN_OPC_GSM is used in the default cases and the MAP operation is matched with the rules in ascending order. If a rule matches, the result of the rule is applied.

```
cs7 instance 0 mlr ruleset MLR_RULES
rule 5 gsm-map sms-mo
  dest-sme 12345678901234567890 min-digits 20 max-digits 20 np 4
  orig-sme 1234567891234567 min-digits 16 max-digits 16 np 4
  dest-smsc 1234567891234567 min-digits 16 max-digits 16 np 4
  orig-imsi 1234567891234567 min-digits 16 max-digits 16
  pid 254
  dest-port 65534
  match-unknown-ton-np
  result gt 123456789123456 tt 0 gti 4 np 4 nai 0
```



```

rule 10 gsm-map sms-mo
  dest-sme 100
  orig-sme 1234 exact ton 5 np 2
  dest-smsc 12345 min-digits 6 max-digits 10
  orig-imsi 123
  pid 35
  dest-port 30
  match-unknown-ton-np
  result continue
rule 20 gsm-map sms-mo
  dest-sme 100
  dest-port 30
  result continue
rule 24 gsm-map sIWFSSigMod default
  result continue
rule 28 gsm-map networkUSSD default
  multi-message-dialogue
  result continue
rule 43 gsm-map connectFollowAddress default
  result gt 123456789012345 tt 255 gti 4 np 15 nai 127
rule 44 gsm-map processUnstructSSData default
  result gt 123456789123456 tt 0 gti 4 np 4 nai 0
rule 45 gsm-map alertSc default
  result continue
rule 50 all-operations
  result continue
!
cs7 instance 0 mlr ruleset MLR_TEST_RUL
  rule 10 all-operations
  result continue
!
cs7 instance 0 mlr ruleset GEN_OPC_GSM protocol gsm-map
  rule 5 alertSc
  dest-smsc *
  result continue
  rule 10 updLoc default
  result continue
  rule 20 sri-sm default
  result continue
  rule 100 all-operations
  multi-message-dialogue
  result continue
!
cs7 instance 0 mlr ruleset DEF
  rule 10 gsm-map sms-mo default
  result continue
!
cs7 instance 0 mlr ruleset TRACE event-trace
  rule 1 gsm-map updLoc default
  rule 2 gsm-map alertSc default
  rule 3 gsm-map invokeSS default
  rule 4 gsm-map authFailRep default
  rule 5 gsm-map sendInfoForOutgCall default
  rule 8 gsm-map sri-sm default
  rule 9 gsm-map sIWFSSigMod default
  rule 10 gsm-map repSmDeliveryStatus default
!
cs7 instance 0 mlr table MLR
  trigger mtp3 dpc 5.4.4 ruleset GEN_OPC_GSM
  trigger mtp3 dpc 4.2.2 ruleset MLR_RULES
  trigger default ruleset GEN_OPC_GSM

```

Related Commands	Command	Description
	dest-port (cs7 mlr ruleset rule)	Specifies the application destination port number.
	dest-sme-table (cs7 mlr ruleset rule)	Specifies MLR table of destination SME addresses (address table).
	dest-smsc (cs7 mlr ruleset rule)	Specifies the address of the destination service center address within an SMS operation.
	match-unknown-ton-np (cs7 mlr ruleset rule)	Specifies that incoming messages containing parameters with unknown ton or np values will match the corresponding rule parameter regardless of the rule's configured ton/np values.
	modify-profile (cs7 mlr ruleset rule)	Specifies SCCP and MAP addresses to modify in messages that are routed using MLR.
	allow-multi-message-dialogue (cs7 mlr ruleset rule)	Specifies that short messages segmented at the MAP layer and SMS MT messages that have the More-Messages-To-Send indicator set match the rule.
	orig-imsi (cs7 mlr ruleset rule)	Configures origin IMSI.
	orig-imsi-table (cs7 mlr ruleset rule)	Configures an MLR table of origin IMSI addresses.
	orig-sme (cs7 mlr ruleset rule)	Specifies the address of the origin SME.
	orig-sme-table (cs7 mlr ruleset rule)	Configures MLR table of origin SME addresses.
	pid (cs7 mlr ruleset rule)	Configures the protocol identifier.
	response-timer (cs7 sms profile parms)	Specifies the processing to be performed on a packet matching the specified trigger and rule.
	result (cs7 mlr ruleset rule)	Specifies the processing that will be performed on a packet matching the specified trigger and rule.
	teleservice	Specifies the service identifier value for an smdpp , sri-sm , or sms-notify operation.
	ussd-string (cs7 mlr ruleset rule)	Specifies the USSD string to be used in filtering and routing mobile initiated GSM-MAP messages.



ITP Command Set: S - Z

All other commands used with this feature are documented in the Cisco IOS Release 12.2 Command Reference publications.

- [sack-frequency \(cs7 asp\), page 1067](#)
- [sack-frequency \(cs7 link\), page 1069](#)
- [sccp-msg, page 1072](#)
- [sctp-rfc-version \(cs7 local peer\), page 1074](#)
- [sctp-rfc-version \(cs7 m3ua\), page 1075](#)
- [sctp-rfc-version \(cs7 sua\), page 1076](#)
- [send-window \(cs7 sms profile parms\), page 1077](#)
- [send-window \(cs7 sms session parms\), page 1078](#)
- [session-init-timer \(cs7 sms profile parms\), page 1079](#)
- [session-init-timer \(cs7 sms session parms\), page 1081](#)
- [set, page 1083](#)
- [show cs7, page 1085](#)
- [show cs7 access-lists, page 1087](#)
- [show cs7 accounting, page 1088](#)
- [show cs7 ansi41, page 1093](#)
- [show cs7 as, page 1095](#)
- [show cs7 asp, page 1098](#)
- [show cs7 audit status, page 1103](#)
- [show cs7 billing configuration, page 1104](#)
- [show cs7 billing statistics, page 1105](#)
- [show cs7 dcs, page 1107](#)
- [show cs7 dcs-group, page 1109](#)
- [show cs7 group, page 1110](#)
- [show cs7 gtt address-conversion, page 1112](#)
- [show cs7 gtt application-group, page 1113](#)
- [show cs7 gtt concern-pclist, page 1115](#)

- [show cs7 gtt config, page 1116](#)
- [show cs7 gtt consistency, page 1118](#)
- [show cs7 gtt gta, page 1120](#)
- [show cs7 gtt map, page 1123](#)
- [show cs7 gtt measurements, page 1125](#)
- [show cs7 gtt selector, page 1129](#)
- [show cs7 gws action-set, page 1130](#)
- [show cs7 gws as, page 1132](#)
- [show cs7 gws config, page 1134](#)
- [show cs7 gws counters, page 1135](#)
- [show cs7 gws linkset, page 1136](#)
- [show cs7 gws table, page 1138](#)
- [show cs7 linkset, page 1141](#)
- [show cs7 log, page 1147](#)
- [show cs7 m2pa, page 1149](#)
- [show cs7 m3ua, page 1157](#)
- [show cs7 mated-sg, page 1159](#)
- [show cs7 mlr address-table, page 1162](#)
- [show cs7 mlr configuration, page 1164](#)
- [show cs7 mlr errors, page 1166](#)
- [show cs7 mlr options, page 1168](#)
- [show cs7 mlr result, page 1169](#)
- [show cs7 mlr ruleset, page 1170](#)
- [show cs7 mlr statistics, page 1176](#)
- [show cs7 mlr table, page 1183](#)
- [show cs7 msu-rates, page 1186](#)
- [show cs7 mtp2, page 1190](#)
- [show cs7 mtp3 counters, page 1198](#)
- [show cs7 mtp3 errors, page 1199](#)
- [show cs7 mtp3 event-history, page 1203](#)
- [show cs7 mtp3 timers, page 1204](#)
- [show cs7 nso, page 1205](#)
- [show cs7 offload, page 1207](#)
- [show cs7 offload mtp3, page 1210](#)
- [show cs7 pc-conversion, page 1212](#)
- [show cs7 ping, page 1213](#)
- [show cs7 pmp, page 1214](#)
- [show cs7 point-codes, page 1216](#)

- [show cs7 qos](#), page 1218
- [show cs7 rate-limit](#), page 1220
- [show cs7 route](#), page 1222
- [show cs7 sample sls](#), page 1227
- [show cs7 sami ip](#), page 1230
- [show cs7 sccp gti-conversion](#), page 1232
- [show cs7 sccp instance-conversion](#), page 1234
- [show cs7 sccp ssn-conversion](#), page 1236
- [show cs7 sgmp](#), page 1237
- [show cs7 sms address-table](#), page 1239
- [show cs7 sms dest-sme-binding](#), page 1241
- [show cs7 sms gsm-map](#), page 1242
- [show cs7 sms group](#), page 1245
- [show cs7 sms route-table](#), page 1246
- [show cs7 sms ruleset](#), page 1249
- [show cs7 sms statistics](#), page 1252
- [show cs7 sua](#), page 1254
- [show cs7 tcap](#), page 1256
- [show cs7 version](#), page 1257
- [show cs7 virtual-linkset](#), page 1259
- [show hosts](#), page 1262
- [show ip sctp](#), page 1264
- [show ip sctp association appl-name dead](#), page 1271
- [show ip sctp association monitor](#), page 1272
- [show monitor event-trace](#), page 1274
- [show redundancy states](#), page 1282
- [show redundancy inter-device](#), page 1284
- [show sscf-nni](#), page 1286
- [show sscop](#), page 1288
- [show tech-support](#), page 1291
- [shutdown \(cs7 asp\)](#), page 1293
- [shutdown \(cs7 dcs\)](#), page 1294
- [shutdown \(cs7 link\)](#), page 1295
- [shutdown \(cs7 linkset\)](#), page 1296
- [shutdown \(cs7 m3ua\)](#), page 1298
- [shutdown \(cs7 mated-sg\)](#), page 1299
- [shutdown \(cs7 sgmp\)](#), page 1300
- [shutdown \(cs7 sua\)](#), page 1301

- [shutdown \(group\)](#), page 1302
- [shutdown \(ipc association\)](#), page 1303
- [si](#), page 1304
- [sls-shift](#), page 1308
- [smsc-map-version \(cs7 sms gsm\)](#), page 1309
- [snmp-server enable traps bits-clock](#), page 1310
- [snmp-server enable traps cs7](#), page 1311
- [snmp-server enable traps sctp](#), page 1314
- [sscf-nni](#), page 1315
- [sscop](#), page 1317
- [teleservice](#), page 1319
- [threshold-rcvd](#), page 1320
- [threshold-send](#), page 1321
- [timeout-count](#), page 1322
- [timer \(cs7 hs-mtp2 profile\)](#), page 1323
- [timer \(cs7 linkset\)](#), page 1325
- [timer \(cs7 profile\)](#), page 1328
- [traffic-mode \(cs7 as\)](#), page 1330
- [traffic-rate-timer](#), page 1333
- [transaction-timer \(cs7 sms route table\)](#), page 1334
- [trigger cdpa \(cs7 mlr table\)](#), page 1335
- [trigger cgpa \(cs7 mlr table\)](#), page 1340
- [trigger default](#), page 1343
- [trigger mtp3](#), page 1346
- [ttl](#), page 1349
- [tmap](#), page 1350
- [tmap \(cs7 as\)](#), page 1351
- [tt-range](#), page 1352
- [tx-queue-depth \(cs7 asp\)](#), page 1354
- [tx-queue-depth \(cs7 hs-mtp2 profile\)](#), page 1355
- [tx-queue-depth \(cs7 link\)](#), page 1357
- [tx-queue-depth \(cs7 m2pa profile\)](#), page 1359
- [tx-queue-depth \(cs7 m3ua\)](#), page 1361
- [tx-queue-depth \(cs7 mated-sg\)](#), page 1362
- [tx-queue-depth \(cs7 mtp2 profile\)](#), page 1363
- [tx-queue-depth \(cs7 sgmp\)](#), page 1364
- [tx-queue-depth \(cs7 sua\)](#), page 1365
- [tx-queue-depth \(group peer\)](#), page 1366

- [ucp \(cs7 sms group\)](#), page 1368
- [udp-checksum](#), page 1369
- [unordered-priority \(cs7 m3ua\)](#), page 1370
- [unordered-priority \(cs7 sgmp\)](#), page 1371
- [unordered-priority \(cs7 sua\)](#), page 1372
- [unrouteable-accounting \(cs7 as\)](#), page 1373
- [unrouteable-accounting \(cs7 linkset\)](#), page 1374
- [update \(cs7 gtt address conversion\)](#), page 1375
- [update \(cs7 sccp gti conversion\)](#), page 1377
- [update route \(route-table\)](#), page 1379
- [ussd-string \(cs7 mlr ruleset rule\)](#), page 1382
- [variant](#), page 1383
- [variant jt1](#), page 1384
- [wait-timeout](#), page 1386

sack-frequency (cs7 asp)

To configure the selective acknowledgment (SACK) for SCTP associations, use the **sack-frequency** command in cs7 asp configuration mode. To disable the configuration, use the **no** form of this command.

sack-frequency *consecutive-packets*

no sack-frequency *consecutive-packets*

Syntax Description

<i>consecutive-packets</i>	The number of consecutive packets to send a sack.

Defaults

The default value is two consecutive packets.

Command Modes

cs7 asp configuration

Command History

Release	Modification
12.4(15)SW5	This command was introduced.
12.2(33)IRE	

Usage Guidelines

SCTP is a reliable protocol. When SCTP does not get a acknowledgment for a sent packet, it triggers a retransmission of the same packet. SCTP can use the SACK mechanism to selectively acknowledge packets. This decreases the retransmission burden relative to an open acknowledgement of packets.

The frequency of SACKs can affect the SCTP overhead. The **sack-frequency** command allows you to tune the frequency of SACKs for your network.

Examples

The following example shows a SACK frequency of three set for the ASP alpha:

```
cs7 multi-instance
cs7 instance 0 variant ANSI
cs7 instance 0 network-name ANSI
cs7 instance 0 point-code 6.0.1
cs7 instance 0 secondary-pc 6.0.2
cs7 instance 0 capability-pc 6.0.3
cs7 instance 0 description ANSI:6.0.1

cs7 instance 2 variant ITU
cs7 instance 2 network-name ITU
cs7 instance 2 point-code 6.2.1
cs7 instance 2 secondary-pc 6.2.2
cs7 instance 2 capability-pc 6.2.3
cs7 instance 2 description ITU:6.2.1
!
cs7 instance 0 linkset to72_rsp 15256
link 0 sctp 192.168.127.102 1377 1377
  sack-frequency 3
!
cs7 asp alpha 7779 7779 sua
```

sack-frequency (cs7 asp)

```
remote-ip 10.74.50.146
sack frequency 3
```

Related Commands!

Command	Description
assoc-retransmit (cs7 asp)	Configures association retransmissions.
cs7 asp	Defines an application server process and enables cs7 asp submode.
show cs7 asp	Displays ASP information.

sack-frequency (cs7 link)

To configure the selective acknowledgment (SACK) frequency for SCTP associations, use the **sack-frequency** command in link configuration mode. To disable the configuration, use the **no** form of this command.

sack-frequency *consecutive-packets*

no sack-frequency *consecutive-packets*

Syntax Description

<i>consecutive-packets</i>	The number of consecutive packets to send a sack.

Defaults

The default value is two consecutive packets.

Command Modes

cs7 link configuration

Command History

Release	Modification
12.4(15)SW5	This command was introduced.
12.2(33)IRE	

Usage Guidelines

SCTP is a reliable protocol. When SCTP does not get a acknowledgment for a sent packet, it triggers a retransmission of the same packet. SCTP can use the SACK mechanism to selectively acknowledge packets. This decreases the retransmission burden relative to an open acknowledgement of packets.

The frequency of SACKs can affect the SCTP overhead. The **sack-frequency** command allows you to tune the frequency of SACKs for your network.

Examples

The following example shows a sack frequency of three set for the linkset to72_rsp 15256:

```
cs7 multi-instance
cs7 instance 0 variant ANSI
cs7 instance 0 network-name ANSI
cs7 instance 0 point-code 6.0.1
cs7 instance 0 secondary-pc 6.0.2
cs7 instance 0 capability-pc 6.0.3
cs7 instance 0 description ANSI:6.0.1

cs7 instance 2 variant ITU
cs7 instance 2 network-name ITU
cs7 instance 2 point-code 6.2.1
cs7 instance 2 secondary-pc 6.2.2
cs7 instance 2 capability-pc 6.2.3
cs7 instance 2 description ITU:6.2.1
!
cs7 instance 0 linkset to72_rsp 15256
link 0 sctp 192.168.127.102 1377 1377
sack-frequency 3
```

sack-frequency (cs7 link)

```
!  
cs7 asp alph 7779 7779 sua  
  remote-ip 10.74.50.146  
  sack frequency 3  
!
```

Related Commands

Command	Description
assoc-retransmit (cs7 link)	Configures association retransmissions.
cs7 linkset	Specifies a linkset and enters cs7 linkset submode.
show cs7 linkset	Displays linkset information.

sccp-class1-loadbalance (cs7 gtt app grp)

To evenly distribute Class 1 traffic within an application group per the multiplicity configuration, use the **sccp-class1-loadbalance** command in cs7 gtt app grp configuration mode. To deactivate this feature, use the **no** form of this command.

sccp-class1-loadbalance

no sccp-class1-loadbalance

Syntax Description	This command has no arguments or keywords.

Command Default	None.

Command Modes	cs7 gtt app grp configuration

Command History	Release	Modification
	12.4(15)SW8	This command was introduced.
	12.2(33)IRH	

Usage Guidelines	Use this command to evenly distribute Class 1 traffic in a way similar to Class 0 within the GTT application group.

Examples	The following example shows this feature configured:

```
cs7 instance 3 gtt application-group appl
multiplicity share
pc 300 1 gt
pc 400 1 gt
sccp-class1-loadbalance
```

Related Commands	Command	Description
	—	—

sccp-msg

To specify a SCCP message header table entry, use the **sccp-msg** command in `cs7 gws sccp` header configuration mode. To remove the specification, use the **no** form of this command.

sccp-msg *sccp-msg-type* **result** {**action** *action-set-name* | **table** *table-name*}

no sccp-msg *sccp-msg-type*

Syntax Description

<i>sccp-msg-type</i>	SCCP message types that are valid in this configuration are listed in Table 37 .
result	Specifies the next step.
action	Screens the result by action set.
<i>action-set-name</i>	Action set name. Valid names may not exceed 12 alphanumeric characters.
table	Screens the result by table.
<i>table-name</i>	Table name. Valid names may not exceed 12 alphanumeric characters.

Command Default

None.

Command Modes

`cs7 gws sccp` header configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

[Table 37](#) lists valid SCCP message types.

Table 37 **SCCP Message Types**

CR	CC	CREF	RLSD	RLC
DT1	DT2	AK	UDT	XUDT
UDTS	XUDTS	LUDT	LUDTS	ED
EA	RSR	RSC	ERR	IT

Examples

The following example shows how to specify SCCP message type entries:

```
cs7 instance 0 gws table SCCP0 type sccp-msg-hdr
  default result action ALLOW
  sccp-msg udta result action ALLOW
  sccp-msg xudta result action ALLOW
```

Related Commands

Command	Description
cs7 gws table	Configures a gateway screening table.

sctp-rfc-version (cs7 local peer)

To set the RFC compliance to either SCTP RFC 2960 or SCTP RFC 4960, use the **sctp-rfc-version** command in cs7 local-peer configuration submode.

sctp-rfc-version {2960 | 4960}

Syntax Description

2960	SCTP RFC 2960 is the earlier version of the standard.
4960	SCTP RFC 4960 is the later version of the standard. It obsoletes SCTP RFC 2960.

Defaults

The default is SCTP RFC 2960.

Command Modes

cs7 local-peer submode configuration

Command History

Release	Modification
12.2(33)IRD	This command was introduced.

Usage Guidelines

Prior to the ITP releases 12.2(33)IRD and 12.4(15)SW4, ITP was compliant with SCTP RFC 2960 but not compliant with SCTP RFC 4960. Releases 12.2(33)IRD, 12.4(15)SW4 and later bring ITP into compliance with SCTP RFC 4960.

Examples

The following example shows how to set the compliance to SCTP RFC 4960:

```
sctp-rfc-version 4960
```

Related Commands

Command	Description
cs7 local-peer	Specifies the local peer.

sctp-rfc-version (cs7 m3ua)

To set the RFC compliance to either SCTP RFC 2960 or SCTP RFC 4960, use the **sctp-rfc-version** command in cs7 m3ua configuration submode.

sctp-rfc-version {2960 | 4960}

Syntax Description	2960	SCTP RFC 2960 is the earlier version of the standard.
	4960	SCTP RFC 4960 is the later version of the standard. It replaces and makes obsolete SCTP RFC 2960.
Defaults	The default is SCTP RFC 2960.	
Command Modes	cs7 m3ua submode configuration	
Command History	Release	Modification
	12.2(33)IRD	This command was introduced.
Usage Guidelines	Prior to the ITP releases 12.2(33)IRD and 12.4(15)SW4, ITP was compliant with SCTP RFC 2960 but not compliant with SCTP RFC 4960. Releases 12.2(33)IRD, 12.4(15)SW4 and later bring ITP into compliance with SCTP RFC 4960.	
Examples	The following example shows how to set the compliance to SCTP RFC 4960: sctp-rfc-version 4960	
Related Commands	Command	Description
	cs7 m3ua	Specifies the local port number for M3UA and enters m3ua submode.

sctp-rfc-version (cs7 sua)

To set the RFC compliance to either SCTP RFC 2960 or SCTP RFC 4960, use the **sctp-rfc-version** command in cs7 sua configuration submode.

sctp-rfc-version {2960 | 4960}

Syntax Description

2960	SCTP RFC 2960 is the earlier version of the standard.
4960	SCTP RFC 4960 is the later version of the standard. It replaces and makes obsolete SCTP RFC 2960.

Defaults

The default is SCTP RFC 2960.

Command Modes

cs7 sua submode configuration

Command History

Release	Modification
12.2(33)IRD	This command was introduced.

Usage Guidelines

Prior to the ITP releases 12.2(33)IRD and 12.4(15)SW4, ITP was compliant with SCTP RFC 2960 but not compliant with SCTP RFC 4960. Releases 12.2(33)IRD, 12.4(15)SW4 and later bring ITP into compliance with SCTP RFC 4960.

Examples

The following example shows how to set the compliance to SCTP RFC 4960:

```
sctp-rfc-version 4960
```

Related Commands

Command	Description
cs7 sua	Specifies the local port number for SUA and enters sua submode.

send-window (cs7 sms profile parms)

To specify the number of outstanding UCP operations between an SMSC and a SMS application, use the **send-window** command in cs7 sms profile parameters configuration mode. To remove the specification, use the **no** form of this command.

send-window *operations*

no send-window *operations*

Syntax Description	<i>operations</i> Number of outstanding UCP operations between an SMSC and a SMS application. Valid range is 1 to 100. The default is 10.													
Defaults	10 outstanding UCP operations													
Command Modes	cs7 sms profile parameters configuration													
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>12.2(18)IXA</td><td rowspan="3">This command was introduced.</td></tr><tr><td>12.4(11)SW</td></tr><tr><td>12.2(33)IRA</td></tr></table>		Release	Modification	12.2(18)IXA	This command was introduced.	12.4(11)SW	12.2(33)IRA						
Release	Modification													
12.2(18)IXA	This command was introduced.													
12.4(11)SW														
12.2(33)IRA														
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>bind-type (cs7 sms profile parameters)</td><td>Specifies SMPP bind type.</td></tr><tr><td>inactivity-timer (cs7 sms profile parameters)</td><td>Specifies session inactivity timer.</td></tr><tr><td>keepalive-timer (cs7 sms profile parameters)</td><td>Specifies session keepalive timer.</td></tr><tr><td>response-timer (cs7 sms profile parms)</td><td>Specifies session response timer.</td></tr><tr><td>session-init-timer (cs7 sms profile parms)</td><td>Specifies session initiation time.</td></tr></table>		Command	Description	bind-type (cs7 sms profile parameters)	Specifies SMPP bind type.	inactivity-timer (cs7 sms profile parameters)	Specifies session inactivity timer.	keepalive-timer (cs7 sms profile parameters)	Specifies session keepalive timer.	response-timer (cs7 sms profile parms)	Specifies session response timer.	session-init-timer (cs7 sms profile parms)	Specifies session initiation time.
Command	Description													
bind-type (cs7 sms profile parameters)	Specifies SMPP bind type.													
inactivity-timer (cs7 sms profile parameters)	Specifies session inactivity timer.													
keepalive-timer (cs7 sms profile parameters)	Specifies session keepalive timer.													
response-timer (cs7 sms profile parms)	Specifies session response timer.													
session-init-timer (cs7 sms profile parms)	Specifies session initiation time.													

send-window (cs7 sms session parms)

To specify the number of outstanding UCP operations between an SMSC and an SMS application, use the **send-window** command in cs7 sms session parameters configuration mode. To remove the specification, use the **no** form of this command.

send-window *operations*

no send-window *operations*

Syntax Description

<i>operations</i>	Number of outstanding UCP operations between an SMSC and an SMS application. Valid range is 1 to 100. The default is 10.

Defaults

10 outstanding UCP operations

Command Modes

cs7 sms session parameters configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Examples

The following example shows how to create an SMPP connection and configure a destination and several parameters:

```
cs7 sms smpp 5000 local-ip 10.10.10.200 dynamic
destination offisland 10.10.20.2 6000
bind-type any
inactivity-timer 5000
keepalive-timer 1000
response-timer 2000
send-window 50
session-init-timer 5000
```

Related Commands

Command	Description
inactivity-timer (cs7 sms session parameters)	Specifies session inactivity timer.
keepalive-timer (cs7 sms session parameters)	Specifies session keepalive timer.
response-timer (cs7 sms session parms)	Specifies session response timer.
session-init-timer (cs7 sms session parms)	Specifies session initiation timer.

session-init-timer (cs7 sms profile parms)

To specify the time lapse allowed between a network connection being established and the establishment of the UCP connection, use the **sessions-init** command in cs7 sms profile parameters configuration mode. To remove the specification, use the **no** form of this command.

session-init-timer *msec*

no session-init-timer *msec*

Syntax Description	<i>msec</i>	Time lapse allowed between a network connection being established and the establishment of the UCP connection. Range is 500 ms to 120000 ms. The default is 10000 ms.

Defaults	10000 ms

Command Modes	cs7 sms profile parameters configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples	The following example shows how to create an SMPP profile named mmprofile and configure several parameters:

```
cs7 sms smpp profile mmprofile
bind-type any
inactivity-timer 5000
keepalive-timer 1000
response-timer 2000
send-window 50
session-init-timer 5000
```

Related Commands	Command	Description
	bind-type (cs7 sms session parameters)	Specifies SMPP bind type.
	inactivity-timer (cs7 sms profile parameters)	Specifies session inactivity timer.
	keepalive-timer (cs7 sms profile parameters)	Specifies session keepalive timer.

Command	Description
response-timer (cs7 sms profile parms)	Specifies session response timer.
send-window (cs7 sms profile parms)	Specifies send window size.

session-init-timer (cs7 sms session parms)

To specify the time lapse allowed between a network connection being established and the establishment of the UCP connection, use the **sessions-init** command in cs7 sms session parameters configuration mode. To remove the specification, use the **no** form of this command.

session-init-timer *msec*

no session-init-timer *msec*

Syntax Description	<i>msec</i>	Time lapse allowed between a network connection being established and the establishment of the UCP connection. Range is 500 ms to 120000 ms. The default is 10000 ms.

Defaults	10000 ms

Command Modes	cs7 sms session parameters configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples	The following example shows how to create an SMPP connection and configure a destination and several parameters:

```
cs7 sms smpp 5000 local-ip 10.10.10.200 dynamic
destination offisland 10.10.20.2 6000
bind-type any
inactivity-timer 5000
keepalive-timer 1000
response-timer 2000
send-window 50
session-init-timer 5000
```

Related Commands	Command	Description
	bind-type (cs7 sms session parameters)	Specifies SMPP bind type.
	inactivity-timer (cs7 sms session parameters)	Specifies session inactivity timer.
	keepalive-timer (cs7 sms session parameters)	Specifies session keepalive timer.

Command	Description
response-timer (cs7 sms session parms)	Specifies session response timer.
send-window (cs7 sms session parms)	Specifies send window size.

set

To specify GTI conversion, subsystem mapping, and address-conversion tables to be assigned from one instance to another, use the **set** command in **cs7 sccp** instance conversion configuration mode. To remove the configuration, use the **no** form of this command.

set { **address-conversion** *table-name* | **gti-conversion** *table-name* | **message-handling** *option* | **national-indicator** *natl-ind* | **ssn-conversion** *table-name* }

no set { **address-conversion** *table-name* | **gti-conversion** *table-name* | **message-handling** *option* | **national-indicator** *natl-ind* | **ssn-conversion** *table-name* }

Syntax Description

address-conversion <i>table-name</i>	Specifies an address-conversion table.										
gti-conversion <i>table-name</i>	Specifies a GTI conversion table.										
message-handling <i>option</i>	Specifies the SCCP message handling option. The following values determine message handling: <table> <tr> <td>0</td><td>no special options</td></tr> <tr> <td>1-7</td><td>spare values (for example, unassigned)</td></tr> <tr> <td>9-15</td><td>additional spare values (for example, unassigned)</td></tr> <tr> <td>no change</td><td>leave field unchanged</td></tr> <tr> <td>return-on-error</td><td>return [x]udts on error</td></tr> </table>	0	no special options	1-7	spare values (for example, unassigned)	9-15	additional spare values (for example, unassigned)	no change	leave field unchanged	return-on-error	return [x]udts on error
0	no special options										
1-7	spare values (for example, unassigned)										
9-15	additional spare values (for example, unassigned)										
no change	leave field unchanged										
return-on-error	return [x]udts on error										
national-indicator <i>natl-ind</i>	Specifies the national indicator. The following options are valid: <table> <tr> <td>0</td><td>international</td></tr> <tr> <td>1</td><td>national</td></tr> <tr> <td>no change</td><td>leave field unchanged</td></tr> </table>	0	international	1	national	no change	leave field unchanged				
0	international										
1	national										
no change	leave field unchanged										
ssn-conversion <i>table-name</i>	Specifies an SSN conversion table.										

Defaults

None.

Command Modes

cs7 sccp instance conversion configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

All three conversion methods can be used, or just one or two. This command is optional, so if no conversion methods are assigned, the GTT in the MSUs do not change.

Examples

The following examples show how to use the **set** command with its various keywords:

```
cs7 sccp instance-conversion in-instance 1 out-instance 0
set gti-conversion gti-conv0
```

```
cs7 sccp instance-conversion in-instance 1 out-instance 0
set ssn-conversion ssntable
```

```
cs7 sccp instance-conversion in-instance 1 out-instance 0
set address-conversion addr-conv
```

```
cs7 sccp instance-conversion in-instance 1 out-instance 0
set message-handling 0
```

```
cs7 sccp instance-conversion in-instance 1 out-instance 0
set national-indicator 1
```

Related Commands

Command	Description
cs7 sccp instance-conversion	Configures or updates an SCCP instance conversion entry.

show cs7

To display ITP basic configuration status, use the **show cs7** EXEC command.

show cs7

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Command Modes	EXEC

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples	The following example includes output from the show cs7 command:

```
ITP#show cs7
Default Instance
Point Code          2.2.3:0
SS7 Variant         ITU
Network Indicator   international
Network Name        'INST0'
Capability PC(s)
  MTP3 Restart status    Completed
Total Linksets       4
Available Linksets   2
Total Links          10

Instance Number 1
Point Code          2.2.1:1
SS7 Variant         ANSI
Network Indicator   international
Network Name        'INST1'
Capability PC(s)
  MTP3 Restart status    In Progress
Total Linksets       2
Available Linksets   0
Total Links          1

Instance Number 7
Point Code          2.2.4:7
SS7 Variant         ANSI
Network Indicator   international
Network Name        'INST7'
Capability PC(s)
  MTP3 Restart status    In Progress
Total Linksets       1
```

■ **show cs7**

```

Available Linksets      0
Total Links             2

MTP3 offload           Enabled

Non Disruptive Upgrade  In Progress
                        CS7 config locked out

```

[Table 38](#) describes the fields in the display.

Table 38 *show cs7 Field Descriptions*

Field	Description
Point Code	Unique address of the node
SS7 Variant	SS7 variation (ANSI or ITU)
Network Indicator	Network indicator (international, national, reserved, or spare)
Network Name	Network name
Capability Point Code	Capability point code
MTP3 Restart status	Restart status
MTP3 Restart occurred	Elapsed time since restart
Total Linksets	Total number of configured linksets
Available Linksets	Available linksets
Total Links	Total number of configured links

Related Commands

Command	Description
show tech-support	Collects and displays a large amount of ITP configuration information.

show cs7 access-lists

To display ITP access lists, use the **show cs7 access-lists** EXEC command.

show cs7 [*instance-number*] **access lists** [*access-list-number*] [*access-list-name*]

Syntax Description	<i>instance-number</i>	Specifies the instance. The valid range is 0 to 7. The default instance is 0.
	<i>access-list-number</i>	Access list number. Valid number is from 2700 to 2999.
	<i>access-list-name</i>	Access list name.

Defaults	The default instance is 0.

Command Modes	EXEC

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples	The following example includes output from the show access-lists command:

```
ITP# show cs7 access-lists
Cisco SS7 access list 2700
  permit dpc 4.100.0 0.0.255
```

[Table 39](#) describes the fields in the display.

Table 39 *show cs7 access-lists* Field Descriptions

Field	Description
Cisco SS7 access list 2700	Information about Cisco access list number 2700.
permit	Permits access if the conditions match.
dpc	Applies destination point code 4.100.0 with wildcard mask 0.0.255 to this access list.

Related Commands	Command	Description
	access-list	Defines a Cisco SS7 access list.
	access-group	Issued from cs7 linkset submode, assigns an access list to a linkset to screen either inbound or outbound packets.
	cs7 linkset	Specifies a linkset and enters cs7 linkset submode.

show cs7 accounting

To display ITP accounting details, use the **show cs7 accounting** EXEC command.

```
show cs7 [instance-number] accounting [point-code] [linkset] [[as [as-name]] | [gtt [checkpoint]]
| [checkpoint] | [unrouteable [checkpoint]] | [access-violations [checkpoint]]]
```

Syntax Description

<i>instance-number</i>	Specifies the instance. The valid range is 0 to 7. The default instance is 0.
<i>point-code</i>	Point code filter.
<i>linkset</i>	Linkset name.
<i>as-name</i>	Specifies which AS is displayed. If this value is not provided, the accounting information for all ASes is displayed by default.
as	Displays xUA accounting information for all ASes or for a dedicated AS.
gtt	Displays the CS7 GTT accounting database(s).
checkpoint	Displays the CS7 checkpointed data.
unrouteable	Displays the CS7 unroutable MSU database.
access-violations	Displays the CS7 access-violations database.

Defaults

The default instance is 0.

If a value for *as-name* is not specified, ITP displays accounting information for all ASes.

Command Modes

EXEC

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Examples

The following example includes output from the **show cs7 accounting** command:

```
ITP# show cs7 accounting
```

```
Checkpoint Interval = 5 min
```

```
Linkset = 'linkset1'
```

DPC	OPC	SI	In Pkts	In Bytes	Out Pkts	Out Bytes
3-4-2	3-4-4	0	0	0	10	120
3-4-4	3-4-2	2	29	348	0	0
3-4-2	3-4-4	2	0	0	29	348

The following example includes output for an accounting report for instance 0:

```
ITP# show cs7 0 accounting
```

Instance Number:0 Checkpoint Interval = 5 min

Linkset = 'linkset1'

DPC	OPC	SI	In Pkts	In Bytes	Out Pkts	Out Bytes
1.15.1:0	1.11.1:0	1	1	9	0	0
1.11.1:0	1.15.1:0	1	0	0	1	9

The following example includes output from the **show cs7 accounting** command with the **access-violations** keyword. The sample output shows that access violations occurred for packets destined for 3.3.3 from origin point code 4.4.4. Packets are received on the input, but no packets are being routed to the destination point code.

ITP# **show cs7 accounting access-violations**

Checkpoint Interval = 5 min

Linkset = 'linkset1'

DPC	OPC	SI	In Pkts	In Bytes	Out Pkts	Out Bytes
3-7-2	3-4-6	3	84	11088	0	0

This data is stored in a two-stage database. The first database is a quick-access table that shows the data accumulated since the last checkpoint event. Checkpointing is the process of moving data records from the quick-access table to the large backend database that stores long-term accounting records. The checkpointed database contains accumulated accounting data since the last clearing or from the time accounting was originally enabled.

The following example includes output from the **show cs7 accounting** command with the **access-violations** and **checkpoint** keywords:

ITP# **show cs7 accounting access-violations checkpoint**

Checkpoint Interval = 5 min

Linkset = 'linkset1'

DPC	OPC	SI	In Pkts	In Bytes	Out Pkts	Out Bytes
3-7-2	3-4-6	3	2	264	0	0

The following example includes output from the **show cs7 accounting** command with the **checkpoint** keyword, displaying the accumulated checkpointed data:

ITP# **show cs7 accounting checkpoint**

Checkpoint Interval = 5 min

Linkset = 'linkset1'

DPC	OPC	SI	In Pkts	In Bytes	Out Pkts	Out Bytes
3-4-4	3-4-6	0	8	84	0	0
3-4-4	3-4-6	2	7893	94716	0	0
3-4-6	3-4-4	0	0	0	6	57
3-4-6	3-4-4	2	0	0	7893	94716

GTT accounting is a flow-based accounting method that is performed on a per-linkset basis. This accounting generates records based on traffic entering a given linkset that is processed by the GTT function of the ITP's SCCP layer. Individual records containing output packet and byte counts are kept for traffic that matches a given GTA entry and is translated to a specific point code.

The following example includes output from the **show cs7 accounting** command with the **gtt** keyword:

ITP# **show cs7 accounting gtt**

show cs7 accounting

Checkpoint Interval = 5 min

Inbound Linkset = 'linkset1'

Matched Selector	Matched Global Title	Translated Point Code	Input Packets	Bytes
my_sel	919341	3-7-1	38	5016
my_sel	919341	3-7-2	688	90816

In the following example the Instance Translation feature has been configured, so the SCCP Accounting tables show an instance number with the translated point code:

ITP# **show cs7 account gtt**

Instance Number:4 Checkpoint Interval = 5 min

Inbound Linkset = 'scp-4'

Matched Selector	Matched Global Title	Translated Point Code	Input Packets	Bytes
sel-4	919	5.1.1:3	2	86

The following example includes output from the **show cs7 accounting** command with MTP3 accounting configured:

Router# **show cs7 0 accounting VirtualLS0_1**

Instance Number:0 Checkpoint Interval = 5 min Count:2

Linkset = 'VirtualLS0_1'

DPC	OPC	SI	In Pkts	In Bytes	Out Pkts	Out Bytes
1.26.1:0	1.1.1:0	0	0	0	1	8
1.1.1:0	1.26.1:0	1	906	8154	0	0

The following example includes output from the **show cs7 accounting** command with virtual linkset GTT accounting configured:

Router# **show cs7 0 accounting VirtualLS0_1 gtt**

Checkpoint Interval = 5 min

Inbound Linkset = 'VirtualLS0_1'

Matched Selector	Matched Global Title	Translated Point Code	Input Packets	Bytes
test 123		6.0.3	1741	23418

The following example includes output from the **show cs7 accounting as** command for an M3UA AS and no optional keywords:

Router# **show cs7 0 accounting as m3ua_as_1**

Instance Number:0 Checkpoint Interval = 5 min Count:2

M3UA AS Name = 'm3ua_as_1'

DPC	OPC	SI	In Pkts	In Bytes	Out Pkts	Out Bytes
2.8.1:0	6.0.3	1	10	90	0	0
2.8.1:0	6.0.3	3	146574	3810924	0	0

The following example includes output from the **show cs7 accounting as** command for an M3UA AS and the **unrouteable** keyword:


```
Router# show cs7 0 accounting as m3ua_as_1 unroutable
```

```
Instance Number:0 Checkpoint Interval = 5 min Count:2
```

```
M3UA AS Name = 'm3ua_as_1'
```

DPC	OPC	SI	In Pkts	In Bytes	Out Pkts	Out Bytes
2.8.1:0	6.0.3	1	10	90	0	0
2.8.1:0	6.0.3	3	146574	3810924	0	0

The following example includes output from the **show cs7 accounting as** command for an M3UA AS and the **gtt** keyword:

```
Router# show cs7 0 accounting as m3ua_as_1 gtt
```

```
Checkpoint Interval = 5 min
```

```
Inbound M3UA AS = 'm3ua_as_1'
```

Matched Selector	Matched Global Title	Translated Point Code	Input Packets	Input Bytes
test	123456	6.0.3	1741	234183

The following example includes output from the **show cs7 accounting as** command for an SUA AS and no optional keywords:

```
Router# show cs7 accounting as sua_as_1
```

```
Checkpoint Interval = 5 min
```

```
SUA AS = 'sua_as_1'
```

DPC	OPC	SI	In Pkts	In Bytes	Out Pkts	Out Bytes
2.8.1:0	6.0.3	3	146574	3810924	0	0

The following example includes output from the **show cs7 accounting as** command for an SUA AS and the optional keyword **unrouteable**:

```
Router# show cs7 accounting as sua_as_1 unroutable
```

```
Checkpoint Interval = 5 min
```

```
SUA AS = 'sua_as_1'
```

DPC	OPC	SI	In Pkts	In Bytes	Out Pkts	Out Bytes
2.8.1:0	6.0.3	3	146574	3810924	0	0

The following example includes output from the **show cs7 accounting as** command for an SUA AS and the optional keyword **gtt**:

```
Router# show cs7 0 accounting as sua_as_1 gtt
```

```
Checkpoint Interval = 5 min
```

```
Inbound SUA AS = 'sua_as_1'
```

Matched Selector	Matched Global Title	Translated Point Code	Input Packets	Input Bytes
test	123456	6.0.3	1741	234183

Table 40 describes the fields in the display.

Table 40 *show cs7 accounting Field Descriptions*

Field	Description
Destination Point Code	Destination point code
Originating Point Code	Originating point code
Input Packet	Input packets
Input Bytes	Input bytes
Output Packets	Output packets
Output Bytes	Output bytes

Related Commands

Command	Description
gtt-accounting (linkset)	Enables GTT accounting on a linkset.
clear cs7 accounting	Clears the ITP accounting databases.
show tech-support	Collects and displays a large amount of ITP configuration information that can be used for troubleshooting.

show cs7 ansi41

To display CS7 ANSI41 MAP information, use the **show cs7 ansi41** privileged EXEC command.

show cs7 ansi41 [detail | statistics]

Syntax Description	detail	Displays information in detailed format.
	statistics	Displays ANSI41 MAP statistics.

Defaults None.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples The following example includes output from the **show cs7 ansi41** command with the **detail** keyword:

```
ITP# show cs7 ansi41 detail
ANSI41 MAP PROVIDER STATISTICS
Open Dialogues: 0/184/37000 (current/high/max)

MAP Provider Global Aborts Generated
Unrecognized Opcode:          0
Support Dlg Released:         0
Internal Error:               0

MAP App Internal Req/Resp Errors
Send Request Error:           0
Send Response Error:          0
Send Abort Error:             0

ANSI41 MAP APPLICATION STATISTICS: SMS ANSI41 DSMR
Operation      Req      Conf      Ind      Resp      Err
-----
SMSNotification 28200    14100    4700    4700        0

Error Comp      -         0        -         0         0
Reject Comp     -         0        -         0         0
Error Summary   0         0        0         0         0

Aborts Sent                Aborts Received
-----
User Requested: 0      User Requested: 0
Resource Unavailable 0
Unsupported Op: 0
Resource Limitation: 0
```

```

Procedure Error:          0
Error Received:           0
Reject Received:         0
Cancel Received:         9400

```

Cancels/Notices

```

-----
Local Cancel:           9400  Notice:           4700

```

```

MAP App: SMS ANSI41 DSMR  No. of Operations: 1
      Operation          SSN   loc   rem
SMSNotification          (54)  11    Y    Y

```

The following example includes output from the **show cs7 ansi41** command with the **statistics** keyword:

ITP# **show cs7 ansi41 statistics**

ANSI41 MAP PROVIDER STATISTICS

Open Dialogues: 0/184/37000 (current/high/max)

MAP Provider Global Aborts Generated

```

Unrecognized Opcode:      0
Support Dlg Released:     0
Internal Error:           0

```

MAP App Internal Req/Resp Errors

```

Send Request Error:       0
Send Response Error:      0
Send Abort Error:         0

```

ANSI41 MAP APPLICATION STATISTICS: SMS ANSI41 DSMR

Operation	Req	Conf	Ind	Resp	Err
SMSNotification	28200	14100	4700	4700	0
Error Comp	-	0	-	0	0
Reject Comp	-	0	-	0	0
Error Summary	0	0	0	0	0

Aborts Sent

Aborts Received

```

-----
User Requested:          0  User Requested:          0
Resource Unavailable      0
Unsupported Op:           0
Resource Limitation:      0
Procedure Error:          0
Error Received:           0
Reject Received:          0
Cancel Received:         9400

```

Cancels/Notices

```

-----
Local Cancel:           9400  Notice:           4700

```

show cs7 as

To display AS and routing key information, use the **show cs7 as** privileged EXEC command.

```
show cs7 [instance-number] as [binding-table | [m3ua [include-gtt | exclude-gtt | only-gtt]] | [sua
[include-gtt | exclude-gtt | only-gtt]] | [all [include-gtt | exclude-gtt | only-gtt]] | [name
as-name]] [operational | active | all] [statistics | detail | brief | event-history]
```

Syntax Description	
<i>instance-number</i>	Specifies the instance. The valid range is 0 to 7. The default instance is 0.
binding-table	Displays binding table.
m3ua	Filters on M3UA.
include-gtt	Includes ASes with GTT routing keys (the default).
exclude-gtt	Excludes ASes with GTT routing keys.
only-gtt	Displays only those ASes with GTT routing keys.
sua	Filters on SUA.
all	Displays all ASes (the default).
name	Filters on AS name.
<i>as-name</i>	AS name.
operational	Displays operational ASes (non-shut state).
active	Displays active ASes.
statistics	Displays AS statistics
detail	Displays information in detailed format.
brief	Displays information in brief format (the default).
event-history	Displays AS history.

Defaults The default display includes ASes with GTT routing keys.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.
	12.4(15)SW3 12.2(33)IRC	PMP status and assigned inbound and/or outbound DCS groups were added to the information displayed with the detail keyword.
	12.2(18)IXH 12.4(15)SW3 12.2(33)IRC	Enhanced the command output to display the binding table for an AS.
	12.4(15)SW9 12.2(33)IRI	Enhanced the command output to display SCCP class 2 binding feature.

Usage Guidelines

The ASes and routing keys are displayed in order of priority (with the first entry having the highest priority).

ASes with GTT routing keys are displayed first.

The GTT ASes are ordered alphabetically based on the AS name.

ASes with non-GTT routing keys are grouped by DPC (highest to lowest).

ASes with the same DPC display the AS with the longest matching routing key at the highest layer in the protocol stack first.

Examples**Syntax examples**

The following command shows how to display all M3UA ASes in detailed format:

```
show cs7 as m3ua detail
```

The following command shows how to display the AS named BLUE:

```
show cs7 as name blue
```

The following command shows how to display all non-GTT ASes (the default):

```
show cs7 as
```

The following command shows how to display the binding table for the AS:

```
show cs7 as binding-table
```

Output examples

If multi-instances have been enabled, the instance number is displayed after the colon in the displayed point code.

The following example includes output from the **show cs7 as** command with the **all** keyword. The display is in the default brief format.

```
ITP# show cs7 as all
```

AS Name	State	Context	Routing Selector	GTT Routing Key GTT Address
asname000012	down	44		
green	down	101	800TABLE	1123456789001

AS Name	State	Context	Routing Dpc	Routing Key Si	Opc	Ssn	Cic Min	Cic Max
kure2as	active	1	0.0.2:0	isup			0	1000
kure2as2	inactv	2	0.0.2:4	isup			1001	2000

The following example includes output from the **show cs7 as** command with the **binding-table** keyword:

```
ITP# show cs7 as binding-table
```

```
AS: mas2 (Total ASP Weight: 8)
```

ASP	State	Mate State	Weight	CIC
dasp2	down	active	1	0, 4
dasp3	active	inactive	0	
dasp4	down	inactive	0	
dasp5	active	inactive	3	1, 2, 3, 5, 6, 7d
aspl	down	inactive	4	

The following example includes output from the **show cs7 as** command with the **detail** keyword:

ITP# **show cs7 as detail**

```

AS name: as_to_bal_1      State: down                Type: M3UA
RoutContxt: 1
SCCP class 2 binding: disabled
Traf mode: loadshare bindings
SLS Option: opc-sls
Mate AS state: unknown  Rerouting queue depth: 0
Recovery tmout: 2000 ms  Recovery queue depth: 0
QOS Class: 0             Burst recovery tmout: 4000 ms
PMP Status: Y            Inbound/outbound DCS group: group_pmp_04 / group_pmp_14
Routing Key:
  Dest PC: 1.1.1:1        Origin PC: n/a            Origin PC mask: n/a
  SI: n/a                 CIC min: n/a            CIC max: n/a
  SSN: n/a                 GTT: n/a              Network Appearance: n/a
ASP Name      AS Name      State      Type  Rmt Port Remote IP Addr  Sctp
asp_to_bal12  as_to_bal_1  down      M3UA  10002   10.0.50.231
asp_to_bal_1  as_to_bal_1  down      M3UA  10000   10.0.50.231

```

The following example includes output from the **show cs7 as** command with the **statistics** keyword:

ITP# **show cs7 as statistics**

```

AS name: myas              Type: M3UA              State: down
Active Time:                Not Active
Failover Attempts:          0          Successful Failovers: 0
Takeovers:                  0          Max Recovery Que Depth: 0
Longest Recovery Time:      0          Average Recovery Time: 0
Packets Retrieved:          0          Packets Rerouted: 0
Recovery Pkts Dropped:      0          Pkts Dropped AS State: 0
Pkts Dropped Mate State: 0
Outbound Packets Rcvd:      0          Outbound Octets Rcvd: 0
Outbound Packets Sent:      0          Outbound Octets Sent: 0

```

Related Commands

Command	Description
clear cs7 as	Clears CS7 AS measurements.
cs7 as	Defines an application server (AS).
dcs-group	Identifies a name to be associated with a DCS group.
show tech-support	Collects and displays a large amount of ITP configuration information that can be used for troubleshooting.
traffic-mode (cs7 as)	To identify the traffic mode of operation of the ASP within an AS.

show cs7 asp

To display ASP information, use the **show cs7 asp** privileged EXEC command.

show cs7 [*instance-number*] **asp** [**m3ua** | **sua** | **all** | **name** *asp-name* | **asname** *as-name*] [**statistics** | **detail**] | **bindings** | **detail** | **event-history**]

Syntax Description

<i>instance-number</i>	Specifies the instance. The valid range is 0 to 7. The default instance is 0.
all	Displays all ASPs (the default).
asname	Filters on AS name.
<i>as-name</i>	AS name.
bindings	Displays ASP bindings.
detail	Displays detail format including the ASP.
event-history	Displays ASP history.
m3ua	Filters on M3UA.
name	Filters on ASP name.
<i>asp-name</i>	ASP name.
statistics	Displays ASP statistics.
sua	Filters on SUA.

Defaults

If no keyword is included, the **all** keyword takes effect.

Unless the **detail** keyword is included, the output defaults to brief format.

The default instance is 0.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.
12.2(18)IXH 12.4(15)SW3 12.2(33)IRC	Output was enhanced with the remote ASP state field.
12.4(15)SW4 12.2(33)IRD	Output was enhanced with the mate state field.
12.4(15)SW8 12.2(33)IRH	Output was enhanced with the XUA error messages fields.

Usage Guidelines

In the brief format, an entry is displayed for each ASP/AS pair. The ASP name might appear multiple times if the ASP is in multiple ASes.

The AS name filter checks all ASes (regardless of GTT). You can check the remote ASP state by using the **detail** keyword.

Examples

Output of the detail format

The following example includes output from the **show cs7 asp** command in the **detail** format and filtering on the ASP name **asp1**. This ASP (type SUA) is down and the association state is closed. It is offloaded to the line card in slot 6.

AspVipId is an internal number used to identify the ASP.

Options for ASP state include: down/inactive/active/standby

The Mate state is the status of the remote ASP. Options include: inactive/active

If the ASP is down or shut down, the remote port and remote IP address display the configured values instead of the actual values.



Note Local receive window configured at SCTP or Port number level will take precedence and is effective for the system. All other levels have lower precedence.

```
ITP# show cs7 asp name asp1 detail
ASP name: asp1                               Type: SUA
Availability: enabled                         ASP id: n/a
SCTP association state: closed                Association id: n/a
AS name: asl                                ASP state: down    Mate state: inactive
Traffic mode: ldshr rr                       Active Time: Not Active
Configured remote port: 6000                 Actual remote port: 6000
Configured remote ip addresses: 10.10.20.2
Actual remote ip addresses: n/a
Local port: 6000
Offload to FlexWAN: Yes Slot: 6 AspVipId: 101
ASP protocol class capability: class 0, class 1
ASP interworking with SS7 networks capability: ASP
Local receive window 64000                   Cumulative sack timeout: 200 ms
Assoc retrans: 10                             Path retrans: 4
Max init retrans: 8                           Max init RTO: 1000 ms
Minimum RTO: 1000 ms                         Maximum RTO: 1000 ms
Bundle status: on                             Bundle timeout: 5 ms
Keep alive status: true                       Keep alive timeout: 30000 ms
Unordered priority: equal                     Cleanup timeout: 0 ms
Link status T1 timeout: 0 ms                  Remote congest T6 timeout: 0 ms
SCTP congestion level: 0                     SCON congestion level: 0
Transmit queue depth: 1000
Thresholds for congestion on transmit queue
  Level 1 onset: 500                          Level 1 abate: 300
  Level 2 onset: 700                          Level 2 abate: 500
  Level 3 onset: 900                          Level 3 abate: 700
  Level 4 onset: 1000                         Level 4 abate: 900
QOS Class: 4 (instance:4) IP TOS: 0x60
Match Type: Any                               Class:4 (instance:4)
```

The following example shows ASP22, type M3UA, as active for 4 days and 20 hours. The association ID is 0x0301000B. This hexadecimal value can be used in the **show ip sctp association** command. ASP22 is not offloaded to a line card. ASP22 serves the AS as2 with traffic mode **loadshare roundrobin**.

```
ITP# show cs7 asp name asp22 detail
ASP name: asp22                               Type: M3UA
Availability: enabled                         ASP id: n/a
```

show cs7 asp

```

SCTP association state: established           Association id: x0301000B
AS name: as2      ASP state: active          Mate state: inactive
Traffic mode: ldshr rr                      Active Time: 4d20h
Configured remote port: 6600                Actual remote port: 6600
Configured remote ip addresses: 172.18.48.67
Actual remote ip addresses: 172.18.48.67    State: active (effective prim)
Local port: 6600
Offload to FlexWAN: No      Slot: -1      AspVipId: 0
ASP protocol class capability: n/a
ASP interworking with SS7 networks capability: n/a
Local receive window: 64000      Cumulative sack timeout: 200 ms
Assoc retrans: 10      Path retrans: 4
Max init retrans: 8      Max init RTO: 1000 ms
Minimum RTO: 1000 ms      Maximum RTO: 1000 ms
Bundle status: on      Bundle timeout: 5 ms
Keep alive status: true      Keep alive timeout: 30000 ms
Unordered priority: equal      Cleanup timeout: 0 ms
Link status T1 timeout: 0 ms      Remote congest T6 timeout: 0 ms
SCTP congestion level: 0      SCON congestion level: 0
Initial cwnd: 768000      Idle cwnd rate: 80
Retrans cwnd rate: 40      Retrans cwnd mode: FastRetrans
Transmit queue depth: 1000
Thresholds for congestion on transmit queue
  Level 1 onset: 500      Level 1 abate: 300
  Level 2 onset: 700      Level 2 abate: 500
  Level 3 onset: 900      Level 3 abate: 700
  Level 4 onset: 1000     Level 4 abate: 900
QOS Class: 0      IP TOS: 0x0
Match Type: None

```

Output of the statistics format

The following example includes output from the **show cs7 asp** command with the **statistics** keyword:

```

ITP# show cs7 asp statistics
ASP name: aspl                               Type: SUA
  Active Time: Not Active
    Data Packets/MSU Stats
      Inbound Packets Rcvd: 0      Inbound Octets Rcvd: 0
      Inbound Packets Sent: 0      Inbound Octets Sent: 0
      Outbound Packets Rcvd: 0     Outbound Octets Rcvd: 0
      Outbound Packets Sent: 0     Outbound Octets Sent: 0
      Inbound CLDTs Rcvd: 0        Inbound CLDTs Sent: 0
      Outbound CLDTs Rcvd: 0       Outbound CLDTs Sent: 0
      Inbound CLDRs Rcvd: 0        Inbound CLDRs Sent: 0
      Outbound CLDRs Rcvd: 0       Outbound CLDRs Sent: 0

```

Options for ASP state include: Down/Inactive/Active/Standby

Options for ASP availability include: Shutdown/Enabled

Output of detailed statistics

The following shows output from the **show cs7 asp** command with the **statistics detail** keywords:

```

ITP# show cs7 asp statistics detail
ASP name: aspl Type: M3UA
Data Packets/MSU Stats
Inbound Packets Rcvd: 0 Inbound Octets Rcvd: 0
Inbound Packets Sent: 0 Inbound Octets Sent: 0
Outbound Packets Rcvd: 0 Outbound Octets Rcvd: 0
Outbound Packets Sent: 0 Outbound Octets Sent: 0
Outbound LC Packets Rcvd:0 Outbound LC Octets Rcvd:0
Outbound LC Packets Sent:0 Outbound LC Octets Sent:0

```

```

Largest Packet Rcvd: 0 Largest Packet Sent: 0
ASP State Maintenance (ASPSM) Stats
ASPUP Rcvd: 0 ASPUP ACK Sent: 0
ASPDN Rcvd: 0 ASPDN ACK Sent: 0
BEAT Rcvd: 0 BEAT ACK Sent: 0
ASP Traffic Maintenance (ASPTM) Stats
ASPAC Rcvd: 0 ASPAC ACK Sent: 0
ASPIA Rcvd: 0 ASPIA ACK Sent: 0
ASPAC NRC Rcvd: 0 ASPIA NRC Rcvd: 0
ASPAC Over-ride: 0 ASPAC Load-share: 0
ASPAC Broadcast: 0 Active Routing Keys: 0
MTP3 Stats
MSUs Sent To MTP3: 0 MSUs Dropped (Cong): 0
MSUs Buffered: 0 MSUs Dropped (Err): 0
Buffer Allocation Stats
Buffer Alloc Failures: 0 Buffer Growth Failures: 0
MSUs Sent To MTP3: 0 MSUs Dropped By MTP3: 0
XUA Error Messages Sent Stats
ERR Invalid Version: 0 ERR Unsupported Class: 0
ERR Unsupported Type: 0 ERR Traffic Mode: 0
ERR Unexpected Msg: 0 ERR Protocol Error: 0
ERR Invalid Stream ID: 0 ERR Refused, Mgmt Block:0
ERR ASP ID Required: 0 ERR Invalid ASP ID: 0
ERR Invalid Parm Value: 0 ERR Parm Field Error: 0
ERR Unexpected Parm: 0 ERR Dest Status Unknown:0
ERR Inv Network App: 0 ERR Missing Parm: 0
ERR Inv Routing Context: 0 ERR No Cfg As For Asp 0
ERR Subsystem Status: 0 ERR Inv Loadshare Label 0
XUA Error Messages Received Stats
ERR Invalid Version: 0 ERR Unsupported Class: 0
ERR Unsupported Type: 0 ERR Traffic Mode: 0
ERR Unexpected Msg: 0 ERR Protocol Error: 0
ERR Invalid Stream ID: 0 ERR Refused, Mgmt Block:0
ERR ASP ID Required: 0 ERR Invalid ASP ID: 0
ERR Invalid Parm Value: 0 ERR Parm Field Error: 0
ERR Unexpected Parm: 0 ERR Dest Status Unknown:0
ERR Inv Network App: 0 ERR Missing Parm: 0
ERR Inv Routing Context: 0 ERR No Cfg As For Asp 0
ERR Subsystem Status: 0 ERR Inv Loadshare Label 0
ERR Rcieved Counter : 0 ERR Timer Value 0
XUA Notify Messages Sent Stats
NOTIFY-AS Inactive: 0 NOTIFY-AS Active: 0
NOTIFY-AS Pending: 0 NOTIFY-Insuf ASP: 0
NOTIFY-Alt ASP Active: 0 NOTIFY-ASP Failure: 0
Outbound SSNM From SS7 Stats
TFAs Rcvd: 0 TFPs Rcvd: 0
TFRs Rcvd: 0 UPUs Rcvd: 0
Cong 0 TFCs Rcvd: 0 Cong 1 TFCs Rcvd: 0
Cong 2 TFCs Rcvd: 0 Cong 3 TFCs Rcvd: 0
Outbound SSNM to ASP Stats
DUNAs Sent: 0 DAVAs Sent: 0
DRSTs Sent: 0 DUPUs Sent: 0
Cong 0 SCONs Sent: 0 Cong 1 SCONs Sent: 0
Cong 2 SCONs Sent: 0 Cong 3 SCONs Sent: 0
Inbound SSNM to SS7 Stats
TFAs Sent: 0 TFPs Sent: 0
TFRs Sent: 0 UPUs Sent: 0
Cong 0 TFCs Sent: 0 Cong 1 TFCs Sent: 0
Cong 2 TFCs Sent: 0 Cong 3 TFCs Sent: 0
Inbound SSNM from ASP Stats
SCON No Level Rcvd: 0 DAUDs Rcvd: 0
DUNAs Rcvd: 0 DAVAs Rcvd: 0
DUPUs Rcvd: 0
Cong 0 SCONs Rcvd: 0 Cong 1 SCONs Rcvd: 0

```

```

Cong 2 SCONs Rcvd: 0 Cong 3 SCONs Rcvd: 0
Congestion Stats
Pkts Dropped At Pri 0: 0 Pkts Dropped At Pri 1: 0
Pkts Dropped At Pri 2: 0 Pkts Dropped At Pri 3: 0
ERR Pkts Dropped: 0 DUNA Pkts Dropped: 0
DAVA Pkts Dropped: 0 SCON Pkts Dropped: 0
DUPU Pkts Dropped: 0 DRST Pkts Dropped: 0
Pkts Dropped by VIP: 0
Level 1 Congestion Cnt: 0 Level 2 Congestion Cnt: 0
Level 3 Congestion Cnt: 0 Level 4 Congestion Cnt: 0
Offload Stats
Bundles Received: 0 Packets in bundles: 0
Bundles Sent: 0 Packets in bundles: 0

```

Output of the event-history format

The **event-history** keyword displays events related to an XUA ASP. The following example includes output from the **show cs7 asp** command with the **event-history** keyword. The output details failed association attempts.

ITP# **show cs7 asp event-history**

Log of failed association attempts:

AssocID	RemotePort	LocalPort	RemoteIpAddr	TimeStamp	ErrorReason
15010016	1028	1024	10.2.2.155	07/05/06 16:15:54	ASP not in AS
15010017	1028	1024	10.2.2.155	07/05/06 16:15:54	ASP not in AS
15010018	1028	1024	10.2.2.155	07/05/06 16:15:54	ASP not in AS

The log size is capped at 5000 in a circular list formation. When 5000 is reached, the earliest entry is deleted and the new entry is added.

If XUA offload is running only on a Cisco 7600 router, the log is sent from the FlexWAN to the line card at a maximum of 100 every 10 seconds.

To clear the log, use the **clear cs7 asp event-history all** or **clear cs7 all** command.

If XUA offload is running only on a Cisco 7600 router, the timestamp refers to the time the log is received on the SUP, not to the time it occurs on the FlexWAN. The log is sorted by the most recent time on the SUP.

The ErrorReason field may list any of the following messages:

"invalid association id"	/* 05 ASPM_INVALID_ASSOCID */
"AVL insert failed"	/* 14 ASPM_AVLINSERT_FAILED */
"ASP not found"	/* 16 ASPM_ASP_NOT_FOUND */
"ASP not in AS"	/* 25 ASPM_ASP_NOT_IN_AS */
"invalid ASP state"	/* 29 ASPM_INVALID_ASP_STATE */
"ASP is shutdown"	/* 32 ASPM_ASP_IS_SHUT */
"protocol is shutdown"	/* 33 ASPM_PROTOCOL_IS_SHUT */

Related Commands

Command	Description
cs7 asp	Specifies an application server process (ASP) and enables cs7 asp submode.
cs7 sua	Specifies the local port number for SUA and enters cs7 sua submode
cs7 m3ua	Specifies the local port number for M3UA and enters m3ua submode.
show tech-support	Collects and displays a large amount of ITP configuration information that can be used for troubleshooting.

show cs7 audit status

To display the latest audit begin time, end time, and audit status, use the **show cs7 audit status** command in Privileged EXEC mode. The display provides a sampling of information based on the current period.

show cs7 audit status

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Command Modes	Privileged EXEC

Command History

Examples	The following example includes output from the show cs7 audit status command:

```
ITP# show cs7 audit status
Component slot/cpu Status Begin-time End-time Success Fail Abort
GWS 1/0 SUCCESS 15:45:44 15:45:46 10 0 0
GWS 1/1 SUCCESS 15:45:44 15:45:45 10 0 0
MLR 1/0 ABORT 15:45:44 15:45:46 9 1 0
MLR 1/1 ABORT 15:45:45 15:45:45 9 0 1
```

ABORT means configuration changes occurred during the audit. SUCCESS means the configuration is consistent between the LC and RP. FAIL means the configuration is not consistent between the LC and RP.

Related Commands	Command	Description
	cs7 audit	Validates and audits the consistency of the content of the LC and SUP files.

show cs7 billing configuration

To display the cs7 billing configuration, use the **show cs7 billing configuration** command in Privileged EXEC mode.

show cs7 billing configuration [**account** *account-name* | **pc-table** | **options** | **load**]

Syntax Description

<i>account-name</i>	Displays a configuration for a specific cs7 billing account.
pc-table	Displays billing pc-table configuration.
options	Displays billing options configuration.
load	Displays billing configuration loading information.

Defaults

The default **show cs7 billing config** with no optional keywords shows the entire billing configuration.

Command Modes

Privileged EXEC

Command History

Examples

The following command displays the cs7 billing configuration loading information:

```
ITP# show cs billing config
cs7 instance 0 billing pc-table mymtp3table mtp3
  point-code 1.1.1 si 2
  point-code 1.1.1 si 4

cs7 instance 1 billing pc-table mysccp sccp
  point-code 1.1.1 gta 222 tt 2 gti 2
cs7 billing options
  backstore 0 ftp://10.74.57.210
```

Related Commands

Command	Description
cs7 billing pc-table	Configures a pc-table for the billing account.
cs7 billing options	Configures options for billing.
cs7 billing load	Specifies the billing configuration file to load.

show cs7 billing statistics

To display the latest collected billing statistics , use the **show cs7 billing statistics** command in Privileged EXEC mode.

show cs7 billing statistics [**account** *acctnt-name*] [**type** { **mtp3** | **sccp** | **sms_sccp** }]

Syntax Description	<i>acctnt-name</i>	Displays a specific cs7 billing account.
	mtp3	Specifies the PC table type as MTP3.
	sccp	Specifies the PC table type as SCCP.
	sms_sccp	Specifies the PC table type as SMS.

Defaults None.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.4(15)SW4 12.2(33)IRD	This command was introduced.
	12.4(15)SW6 12.2(33)IRF	The keyword sms_sccp was added.

Examples The following examples displays cs7 billing statistics information:

```
#show cs7 billing statistics

Start Timestamp : 2009/09/22/09:15:03.191
End Timestamp   : 2009/09/22/09:16:33.183
SDR Version ID: Ver-1.0
Total Records   : 10
-----
Instance : 0
Instance          : 0
Account           : sms-acc
Linkset           : m2pa_194_0_0
SCCP OPC IN      : 1.1.2
SSN               : others
SMS MSU/SMS OCTETS : 10/1380
-----
Instance          : 0
Account           : sms-acc
Linkset           : m2pa_194_0_0
SCCP OPC IN      : 1.1.1
SSN               : others
SMS MSU/SMS OCTETS : 4/36
```

Related Commands	Command	Description
	cs7 billing pc-table	Configures a PC table for the billing account.
	cs7 billing options	Configures options for billing.
	cs7 billing load	Specifies the billing configuration file to load.

show cs7 dcs

To display information about the DCS node, use the **show cs7 dcs** privileged EXEC command.

show cs7 dcs [*name*] [*detail*]

Syntax Description	<i>name</i>	DCS node name.
	<i>detail</i>	Displays detailed information about the DCS.

Defaults None.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.4(15)SW3	This command was introduced.
	12.2(33)IRC	

Examples The following example includes output from the **show cs7 dcs** command:

ITP# **show cs7 dcs**

```
Effect Primary
DCS Name      DCS Group      State      Rmt Port  Remote IP Addr  Cost
-----
polystar      polystar      active     33500     213.238.208.200  0
to_itp_test   to_itp_test   down       33500     10.74.57.197    0
```

The following example includes output from the **show cs7 dcs detail** command:

ITP# **show cs7 dcs detail**

```
DCS Name: polystar                DCS Group Name: polystar
DCS State: active                 Active Time: 2d04h
Local address:                    64.104.170.9
Remote addresses:                 213.238.208.200
Effective remote address:         213.238.208.200
Remote Port:                      33500    Local Port:      33500
Encapsulation MSU Data Type:      2         UDP Checksum:    Off
Keep Alive Interval:              5         Timeout Count:   3
Available Remote Addresses:        1         Reference Count: 1

DCS Name: to_itp_test             DCS Group Name: to_itp_test
DCS State: down                   Active Time: Not Active
Local address:                    10.74.57.125
Remote addresses:                 10.74.57.197
Effective remote address:         n/a
Remote Port:                      33500    Local Port:      33500
Encapsulation MSU Data Type:      2         UDP Checksum:    On
```

■ show cs7 dcs

```

Keep Alive Interval:      5      Timeout Count:   3
Available Remote Addresses: 0      Reference Count:  1

```

Related Commands

Command	Description
cs7 pmp	Turns probeless monitoring on for all linksets and ASes.
cs7 pmp hold-queue	Sets the integer range of PMP hold queue thresholds.
cs7 dcs-group	Identifies a name to be associated with a DCS group and enters cs7 dcs-group configuration mode.
cs 7 dcs	Identifies a name to be associated with a DCS node and enters cs7 dcs configuration mode.
show cs7 pmp	Displays errors and information about the PMP.
show cs7 dcs-group	Displays information about the DCS group.

show cs7 dcs-group

To display information about the DCS group, use the **show cs7 dcs-group** privileged EXEC command.

show cs7 dcs-group *name*

Syntax Description	<i>name</i> DCS group name.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.4(15)SW3	This command was introduced.
	12.2(33)IRC	

Examples The following example includes output from the **show cs7 dcs-group** command:

ITP# **show cs7 dcs-group**

DCS Group	DCS Name	State	Cost
-----	-----	-----	----
polystar	polystar	active	0
to_itp_test	to_itp_test	down	0

Related Commands	Command	Description
	cs7 pmp	Turns probeless monitoring on for all linksets and ASes.
	cs7 pmp hold-queue	Sets the integer range of PMP hold queue thresholds.
	cs7 dcs-group	Identifies a name to be associated with a DCS group.
	cs 7 dcs	Identifies a name to be associated with a DCS node.
	show cs7 pmp	Displays errors and information about the PMP.
	show cs7 dcs	Displays information about the DCS node.

show cs7 group

To display ITP group operational information, use the **show cs7 group** privileged EXEC command.

show cs7 group { counters [detailed] | state | transport }

Syntax Description	counters	Displays ITP group counters.
	detailed	Displays detailed counter information.
	state	Displays ITP group state information.
	transport	Displays ITP group transport information.

Defaults None.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples The following example shows how to display ITP group state information:

```
ITP# show cs7 group state
ITP Group state information:
  Redundancy Facility state:
    RF State           = 13 (ACTIVE)
    RF Peer State      = 8 (STANDBY HOT)
  Group role information:
    Current State:     Manager
    Previous State:    Negotiating
    Latest event:      NEGO_MANAGER
    Peer name:         group_member2
    Active timer:      none
  Checkpointing state:
    Last seq  sent:      549
    Last seq  rcvd:      0
    Congested:          FALSE
    Current send queue depth: 0
```

[Table 41](#) describes the significant fields shown in the display.

Table 41 *show cs7 group state Field Descriptions*

Field	Description
RF State	Current Redundancy Facility state of this device
RF Peer State	Current Redundancy Facility state of the group peer
Current State	Current Group Finite State Machine (FSM) state
Previous State	Group FSM state before latest FSM event
Latest event	Last FSM event processed
Peer name	Name of group peer
Active timer	Name of FSM timer running, or none
Last seq # sent	Sequence number of last Group Checkpointing message sent to group peer
Last seq # rcvd	Sequence number of last Group Checkpointing message received from group peer
Congested	TRUE if congestion is present on communication transport to group peer
Current send queue depth	Number of messages waiting to be sent to group peer

The following example shows how to display ITP group counters information:

```
ITP# show cs7 group counters detail
Checkpointing counters:
  Messages sent:                10
  Messages received:            0
  Max depth reached by send queue: 5
  Requeues to send queue:      0
  Flow control ON indications:  0
  Flow control OFF indications: 0
  Message buffer alloc failures: 0
  Message transmission failures: 0
  Message acknowledgement failures: 0
  Send element alloc failures:  0
  Receive element alloc failures: 0
  Unrecognized messages received: 0
Messages counters:
  Bulk_Sync_Complete : sent=2
  TPRC_Sync          : sent=2
  Linkset_Sync       : sent=2
  SCCP_Global_Meas   : sent=2
  MIB_seq            : sent=2

Group association drops : 0
RF association drops   : 0
CF association drops    : 0
```

Related Commands

Command	Description
cs7 group	Configures the ITP group feature.
show tech-support	Collects and displays a large amount of ITP configuration information that can be used for troubleshooting.

show cs7 gtt address-conversion

To display CS7 GTT address-conversion entries, use the **show cs7 gtt address-conversion** privileged EXEC command.

show [*instance-number*] **cs7 gtt address-conversion** [*name*]

Syntax Description

<i>instance-number</i>	Specifies the instance. The valid range is 0 to 7. The default instance is 0.
<i>name</i>	Displays output for a specified address-conversion table.

Defaults

The default instance is 0.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Examples

The following example includes output from the **show cs7 gtt address-conversion** command:

ITP# **show cs7 gtt address-conversion**

Conversion Table Name: e212e214

New NP:

New NAI:

Ref Count: 1

in-address	out-address	np	nai	es
-----	-----	---	---	---
65507	1456			1

Related Commands

Command	Description
cs7 gtt address-conversion	Configures a GTT address-conversion table.

show cs7 gtt application-group

To display CS7 GTT application group entries, use the **show cs7 gtt application-group** privileged EXEC command.

show cs7 [*instance-number*] **gtt application-group** [**brief**] [**name** *app-grp-name*] [**rate-limit**]

Syntax Description

<i>instance-number</i>	Specifies the instance. The valid range is 0 to 7. The default instance is 0.
brief	Displays a brief form of the output.
name	Displays a specific application group by name.
<i>app-grp-name</i>	Application group name.
rate-limit	Displays the rate-limit of DPC/AS in GTT application group wide.

Defaults

The default instance is 0.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.
12.4(15)SW4 12.2(33)IRD	The rate-limit keyword was introduced.
12.4(15)SW8 12.2(33)IRH	Output enhanced with the SCCP Class 1 load balance field.
12.4(15)SW9 12.2(33)IRI	Output enhanced with sccp-allow-pak-conv conversion option.

Examples

The following example includes output from the **show cs7 gtt application-group** command:

```
ITP# show cs7 gtt application-group name abc
Application Group Name      : abc
Distribute-sccp-sequenced: Instance-level
sccp-class1-loadbalance   : Disabled
Multiplicity               : share
Ref Count                 : 0
Instance                  : 0
Application Identifier      RI    Cost  PCST   SST    CONGESTED  AS ST  SCCP-PAK-CONV-OPT
-----
PC=2222:1      SSN=2      pcssn  1    UNAVL  UNAVL  -----      1
PC=6880:0      SSN=2      gt     2    avail  -----
PC=3333:2      SSN=2      pcssn  2    UNAVL  UNAVL  -----      3
PC=6076:0      SSN=2      pcssn  3    avail  avail  -----
```

■ show cs7 gtt application-group

The following example includes output from the **show cs7 gtt application-group** command with the keyword **name**, the namen argument bbb and the keyword **rate-limit**:

```
ITP# show cs7 7 gtt application-group name bbb rate-limit
# of limited point: 2
      node id: 1504
      rate limit: 1000
configuration type: SCCP App Group Wide
      instance: 7
      xUA AS: ENUM-TITAN
Application Group: bbb

SLOT    QUOTA    IN_PKTS
1/0      1000      500
1/1       66       0
2/0       66       0
2/1       66       0
```

Related Commands

Command	Description
cs7 gtt application-group	Specifies a GTT application group.
show cs7 gtt consistency	Displays GTT point codes that do not have routes provisioned for them.
cs7 rate-limit	Limits traffic rate to a specified DPC/AS in an MTP over-flow load-share that uses a GTT application group. Adds or changes a point code and optional subsystem number in the application group
pc (cs7 gtt application group)	Adds or changes a point code and optional subsystem number in the application group.
asname (cs7 gtt application group)	Assigns an M3UA or SUA AS directly to a global title.

show cs7 gtt concern-pclist

To display a CS7 GTT concerned point code list, use the **show cs7 gtt concern-pclist** privileged EXEC command.

show cs7 [*instance-number*] **gtt concern-pclist** [*name pc*]

Syntax Description

<i>instance-number</i>	Specifies the instance. The valid range is 0 to 7. The default instance is 0.
<i>name</i>	GTT concerned PC list name.
<i>pc</i>	Point code.

Defaults

The default instance is 0.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Examples

The following example includes output from the **show cs7 gtt concern-pclist** command:

```
ITP# show cs7 gtt concern-pclist
List Name: mylist  Ref Count = 0
Concerned Point Codes
-----
5.100.5
```

Related Commands

Command	Description
cs7 gtt concern-pclist	Specifies a GTT concerned point code list.

show cs7 gtt config

To display the complete configuration for GTT, use the **show cs7 gtt config** privileged EXEC command.

show cs7 [*instance-number*] **gtt config**

Syntax Description	<i>instance-number</i>	Specifies the instance. The valid value range is 0 to 7.

Defaults	The default instance is 0.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.
	12.4(15)SW5 12.2(33)IRE	Command output was extended to include next table information.
	12.4(15)SW9 12.2(33)IRI	Output enhanced with sccp-allow-pak-conv conversion option.

Usage Guidelines	Since the GTT data is not stored in NVRAM, commands such as show running config will not display the GTT data. To display the current running configuration regarding GTT use the show cs7 gtt config command.

Examples	The following example includes output from the show cs7 gtt config command including next table information:

```
ITP# show cs7 gtt config
cs7 instance 0 gtt map 1234      sol
!
cs7 instance 0 gtt application-group appl
multiplicity share
pc 1234 ssn 2 1 gt sccp-allow-pak-conv 1
!
cs7 instance 0 gtt selector sel1 tt 0 gti 2
gta 11100 pcssn 1234 gt sccp-allow-pak-conv 1
```

Related Commands	Command	Description
	cs7 gtt application-group	Configures a GTT application group.
	cs7 gtt concern-pelist	Specifies a GTT concerned point code list.

Command	Description
cs7 gtt map	Specifies a GTT mated-application entry.
cs7 gtt selector	Creates a GTT selector.
next-table	Creates a next table for the GTT default table.
gta app-grp	Creates or modifies a GTA application group.

show cs7 gtt consistency

To display GTT point codes that do not have routes provisioned for them, use the **show cs7 gtt consistency** privileged EXEC command.

show cs7 gtt consistency

Syntax Description This command has no arguments or keywords.

Defaults None.

Command Modes Privileged EXEC

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Examples

The following example includes output from the **show cs7 gtt consistency** command:

ITP# **show cs7 gtt consistency**

Report: GTT MAP PCs which do not have associated MTP3 Full, Cluster, or Summary Route configured:

PC	Ref Count
1.1.1:0	1
1.1.2:0	1
1.1.3:0	1
1.10.1:0	1
1.10.2:0	1
2.2.2:0	0
6.5.6:0	1

Report: GTT AppGroups which contain PCs that do not have associated MTP3 Full, Cluster, or Summary Route configured:

Application Group	PC
test	2.2.2:0
steve	1.1.1:0

Report: GTT Selectors which contain PCs that do not have associated MTP3 Full, Cluster, or Summary Route configured:

Selector	GTA	PC
test	123456789012345	1.1.1:0
test	1	1.1.3:0
test	default	1.1.2:0

Related Commands

Command	Description
cs7 gtt application-group	Configures a GTT application group.
cs7 gtt map	Configures a global title mated-application (MAP) entry.
show cs7 gtt application-group	Displays CS7 GTT application group entries.
show cs7 gtt gta	Displays CS7 GTT GTA entries.
show cs7 gtt map	Displays CS7 GTT MAP entries.

show cs7 gtt gta

To display CS7 GTT GTA entries, use the **show cs7 gtt gta** privileged EXEC command.

show cs7 [*instance-number*] **gtt gta** *selector-name* [[**sgta** *sgta* **egta** *egta*] | [**match** *gta*]]

Syntax Description

<i>instance-number</i>	Specifies the instance. The valid range is 0 to 7. The default instance is 0.
<i>selector-name</i>	Selector name.
sgta	Specifies a start global title address.
<i>sgta</i>	Starting global title address.
egta	Specifies an end global title address.
<i>egta</i>	Ending global title address.
match	Specifies a matching global title address.
<i>gta</i>	Global title address.

Defaults

The default instance is 0.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.
12.4(15)SW9 12.2(33)IRI	Output enhanced with sccp-allow-pak-conv conversion option.

Usage Guidelines

GTA-MATCH counters apply only for LC. Hence, the counters do not increment on SUP. If the command is executed on SUP, the output is zero for GTA_MATCH counters.

Examples

The following example includes output from the **show cs7 gtt gta** command for all GTAs on the selector named sell:

```
ITP# show cs7 gtt gta sell
Selector Name  TT   GTI  NP   NAI   QOS  PreGttConv  PostGttConv  #GTAs  Next-Table Name  NTT
-----
sell          0    2                1

GTA           PC           RI      SSN  TT   App-Grp      QOS  ASname      PAM  GTA_MATCH
11100         1234:0        gt
SCCP-PAK-CONV-OPT PakConvCounter  PakDropCounter
```

1

0

0

Table 42 describes the fields in the display.

Table 42 *show cs7 gtt gta Field Descriptions*

Field	Description
Selector Name	Selector
TT	Translation type
GTI	Global title indicator
NP	Numbering plan for the selector
NAI	Nature of address indicator for the selector
QOS	QoS characteristics for the selector
PreGttConv	Global title address conversion table to apply prior to performing local global title translation
PostGttConv	Global title address conversion table to apply after performing local global title translation
#GTAs	Number of GTAs for the selector
Next-Table Name	Default GTT selector points to this next table
NTT	New translation type
GTA	Global title address
PC	Point code
RI	Routing indicator
SSN	Subsystem number
TT	Translation type
App-Grp	Application group
QOS	QoS characteristics for the GTA
ASname	M3UA or SUA application server name
PAM	PAM table name
GTA_MATCH	Global title address match count
SCCP-PAK-CONV-OPT	Shows which option is selected for pak conversion, i.e. XUDT-to-UDT, UDT-to-XUDT, or no conversion
PakConvCounter	Shows how many packets are converted from XUDT-to-UDT or UDT-to-XUDT
PakDropCounter	Shows how many packets ITP was not able to convert

Related Commands

Command	Description
gta app-grp	Creates or modifies a GTA entry that translates a GTA to a GTT application group.

Command	Description
gta pcssn	Creates or modifies a GTA entry that translates a GTA to a point code and optional subsystem number.
show cs7 gtt consistency	Displays GTT point codes that do not have routes provisioned for them.

show cs7 gtt map

To display CS7 GTT MAP entries, use the **show cs7 gtt map** privileged EXEC command.

show cs7 [*instance-number*] **gtt map** [**pc** *ppc* [**SSN** *ssn*]] [**status**]

Syntax Description		
<i>instance-number</i>		Specifies the instance. The valid range is 0 to 7. The default instance is 0.
pc		Specifies a primary point code.
<i>ppc</i>		Primary SS7 point code, in the form zone.region.sp.
SSN		Specifies a subsystem number.
<i>ssn</i>		Subsystem number ranging from 2 to 255.
status		Displays the status of the subsystems.

Defaults The default instance is 0.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples The following example includes output from the **show cs7 gtt map** command with no keywords:

```
ITP# show cs7 gtt map
  PPC      PSSN  MULT  BPC      BSSN  ConPCLst      RRC ADJ  Ref
2.2.2      10    sol   -----   ---              off no   1
2.2.3      10    sol   -----   ---              off no   1
2.2.4      10    sol   -----   ---              off no   1
```

The following example includes output from the **show cs7 gtt map** command with the **statistics** keyword. The output displays the real-time status of each entry in the GTT MAP table.

```
ITP# show cs7 gtt map statistics
 PC      SSN  PCST  SST  CONGESTED
 668      250  UNAVL  avail -----
1003      250  avail  avail -----
1008      250  avail  UNAVL -----
2020      250  avail  avail  level 2
```

[Table 43](#) describes the fields in the display.

Table 43 *show cs7 gtt map Field Descriptions*

Field	Description
PCST	Point code status
SST	Subsystem status
CONGESTED	MTP3 congestion level for the point code

Related Commands

Command	Description
cs7 gtt map	Creates a GTT mated-application entry.
show cs7 gtt consistency	Displays GTT point codes that do not have routes provisioned for them.

show cs7 gtt measurements

To display a summary of CS7 GTT/SCCP measurements, use the **show cs7 gtt measurements** privileged EXEC command.

```
show cs7 [instance-number] gtt measurements [[app-grp app-grp-name] | [counters] | [map] |
[selector [selector]] | [systot] | [line-card [line-card-num]]]
```

Syntax Description		
app-group		Displays measurements kept on a GTT application group basis.
<i>app-grp-name</i>		GTT application group name.
counters		Displays Q.752 counters for GTT.
<i>instance-number</i>		Specifies the instance. The valid range is 0 to 7. The default instance is 0.
line-card		Displays measurements kept on a line card basis.
<i>line-card-num</i>		Line card number. If <i>line-card-num</i> is not specified, all measurements for all line cards are displayed.
map		Displays measurements kept on a GTT MAP basis.
selector		Displays statistics kept on a GTT selector basis.
<i>selector</i>		Displays statistics for a specified selector.
systot		Displays measurements kept on a system-wide basis.

Defaults

If no keyword is specified, the system totals (systot) are displayed.
The default instance is 0.

Command Modes

Privileged EXEC

Command History	Release	Modification
	12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.
	12.4(15)SW9 12.2(33)IRI	Output enhanced with sccp-allow-pak-conv conversion option.

Examples

The following example shows output from the **show cs7 gtt measurements map** command:

```
ITP# show cs7 gtt measurements map
GTT/SCCP Mated Application Measurements Report

Point Code  SSN  USED      CONG_RR  PC_UNAV  SS_UNAV  PC_CONG  SS_CONG  MTP3_FAIL
2.2.2       10   0         0         0         0         0         0         0
2.2.3       10   0         0         0         0         0         0         0
2.2.4       10   0         0         0         0         0         0         0
```

show cs7 gtt measurements

The following example shows output from the **show cs7 gtt measurements selector** command with no selector specified:

```
ITP# sh cs7 gtt measurements selector
GTT/SCCP Selector Measurements Report

Selector Name  GTT_PERF      GTA_NF      sccpPakConvCounter  sccpPakDropCounter
si_ch          0              0              0                    0
sell           0              0              0                    0
selsample      0              0              0                    0
```

The following example shows output from the **show cs7 gtt measurements selector** command for the selector named sell:

```
ITP# sh cs7 gtt measurements selector sell
GTT/SCCP Selector Measurements Report

Selector Name  GTT_PERF      GTA_NF      sccpPakConvCounter  sccpPakDropCounter
sell           0              0              0                    0
```

The following example shows output from the **show cs7 gtt measurements systot** command:

```
ITP# show cs7 gtt measurements systot
GTT/SCCP System Wide Measurements Report

GTT_PERF      GTTSEL_NF      BAD_GT_FMT      GTA_NF      CONGEST_RR
0              0              0              0              0

GTT_HOP_ERR    GTT_MAP_NF      UNEQUIP_SS      SCCP_UNAV      DPC_UNAV
0              0              0              0              0

SS_UNAV        DPC_CONG      SS_CONG      MTP3_FAIL
0              0              0              0
```

The following example shows output from the **show cs7 gtt measurements app-grp app1** command which includes the total number of packets converted and packets dropped at the app-grp level:

```
ITP# show cs7 gtt measurements app-grp app1
Application Group Name: app1
Multiplicity          : share
Ref Count              : 0
Instance               : 0

Application Identifier RI    Cost  Used Class0    Class1    PakConvCounter  PakDropCounter
-----
PC=6871:0    SSN=2    pcssn 1    0    0              0              410              0
```

The following example shows output from the **show cs7 gtt measurements counters** command:

```
ITP_254# sh cs7 gtt measurements counters

Q.752 counters for instance 0

Total Messages      0          Local Messages      0
Total GTT Messages  0
UDT Sent:           0          UDT Rcvd:           0
UDTS Sent           0          UDTS Rcvd:          0
XUDT Sent:          0          XUDT Rcvd:          0
XUDTS Sent:         0          XUDTS Rcvd:         0
LUDT Sent:          0          LUDT Rcvd:          0
LUDTS Sent:         0          LUDTS Rcvd:         0
CR to MTP3:         0          CR from MTP3:       0
CREF to MTP3:       0          CREF from MTP3:     0
RSR to MTP3:        0          RSR from MTP3:      0
ERR to MTP3:        0          ERR from MTP3:      0
```

```

XUDT-UDTconv:      0          XUDTS-UDTSConv:      0
UDT-XUDTconv:      0          UDTs-XUDTSConv:      0
SEG UNSUP:         0          REASS UNSUP:         0

Q.752 counters for instance 1
Total Messages      0          Local Messages      0
Total GTT Messages  0
UDT Sent:           0          UDT Rcvd:           0
UDTS Sent           0          UDTs Rcvd:          0
XUDT Sent:          0          XUDT Rcvd:          0
XUDTS Sent:         0          XUDTS Rcvd:         0
LUDT Sent:          0          LUDT Rcvd:          0
LUDTS Sent:         0          LUDTS Rcvd:         0
CR to MTP3:         0          CR from MTP3:        0
CREF to MTP3:       0          CREF from MTP3:      0
RSR to MTP3:        0          RSR from MTP3:       0
ERR to MTP3:        0          ERR from MTP3:       0
XUDT-UDTconv:      0          XUDTS-UDTSConv:      0
UDT-XUDTconv:      0          UDTs-XUDTSConv:      0
SEG UNSUP:         0          REASS UNSUP:         0

```

Table 44 describes the fields in the display.

Table 44 *show cs7 gtt measurements Field Descriptions*

Field	Description
GTT_PERF	Total number of successful translations performed
GTTSEL_NF	Total number of times a message requiring GTT was received with a TT, GTI, [NP, NAI] that did not exist in the GTT selector table
BAD_GT_FMT	Total number of times a message requiring GTT was received with an invalid or unsupported format
GTA_NF	Total number of times a message requiring GTT was received with a global title address that did not exist in the GTT table for the matching selector
CONGEST_RR	Total number of times a message requiring GTT was routed to an alternate backup route because of congestion
GTT_HOP_ERR	Total number of times a message requiring GTT was received with a hop count that violated the rules concerning XUDT messages
GTT_MAP_NF	Total number of times a message requiring GTT was received and final GTT was performed to a PC and SSN that were not provisioned in the GTT MAP table
UNEQUIP_SS	Total number of times SCCP failed to route due to a subsystem being unequipped in the MAP table
SCCP_UNQUAL	The total number of times SCCP failed due to an error that is unqualified by any of the other errors listed.
SCCP_UNAV	Total number of times SCCP failed to route due to the SCCP subsystem being unavailable on a remote node
DPC_UNAV	Total number of times SCCP failed to route due to the destination point code being unavailable
SS_UNAV	Total number of times SCCP failed to route due to the subsystem on a remote node being unavailable

Table 44 *show cs7 gtt measurements Field Descriptions (continued)*

DPC_CONG	Total number of times SCCP failed to route due to the destination point code being congested
SS_CONG	Total number of times SCCP failed to route due to the subsystem on a remote node being congested
MTP3_FAIL	Total number of times SCCP failed to route due to an MTP3 failure (a point code used in the GTT table has no configured route in the MTP3 routing tables)

Related Commands

Command	Description
show cs7 gtt map	Displays a GTT mated-application entry.
show cs7 gtt selector	Displays GTT selectors.
show tech-support	Collects and displays a large amount of ITP configuration information that can be used for troubleshooting.

show cs7 gtt selector

To display CS7 GTT selectors, use the **show cs7 gtt selector** privileged EXEC command.

show cs7 [*instance-number*] **gtt selector** [**gti** *gti*] [**nai** *nai*] [**name** *selector-name*] [**np** *np*] [**tt** *tt*]

Syntax Description		
<i>instance-number</i>		Specifies the instance. The valid range is 0 to 7. The default instance is 0.
gti		Specifies a global title indicator.
<i>gti</i>		Global title indicator. Valid range is 0 to 4.
nai		Specifies a nature of address indicator.
<i>nai</i>		Nature of address indicator.
name		CS7 GTT selector name.
<i>selector-name</i>		Selector name.
np		Specifies a numbering plan.
<i>np</i>		Numbering plan.
tt		Specifies a translation type.
<i>tt</i>		Translation type.

Defaults The default instance is 0.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples The following example includes output from the **show cs7 gtt selector** command with no keywords:

```
ITP# show cs7 gtt selector
  Selector Name   TT   GTI   NP   NAI   DFLTQOS   #GTAs
  -----
c7gsp             0     4     1     3             3
itp_gtt           0     4     0     4             1
```

Related Commands	Command	Description
	cs7 gtt selector	Creates and configures a GTT selector.

show cs7 gws action-set

To display ITP gateway screening action-set information, use the **show cs7 gws action-set EXEC** command.

show cs7 gws action-set [*name action-set-name*]

Syntax Description

name	Specifies the action set.
<i>action-set-name</i>	Name of the action set. Valid names can contain up to 12 alphanumeric characters.

Defaults

None.

Command Modes

EXEC

Command History

Examples

The following example includes output from the **show cs7 gws action-set** command with no keywords:

```
ITP# show cs7 gws action-set
Action-set Name: ALLOW Action: allow Logging:
  Refcount:          42  NumUsed:          0

Action-set Name: BLOCK Action: block Logging:
  RefCount:           4  NumUsed:          0

Action-set Name: DONTALLOW Action: block Logging:
  RefCount:           0  NumUsed:          0

Action-set Name: ALWAYSALLOW Action: allow Logging:
  RefCount:           0  NumUsed:          0

Action-set Name: allowed-ver Action: allow Logging:
  RefCount:           0  NumUsed:          0

Action-set Name: blocked-ver Action: block Logging:
  RefCount:           1  NumUsed:          0
```

[Table 45](#) describes the fields in the display.

Table 45 *show cs7 gws action-set Field Descriptions*

Field	Description
Action-set Name:	Action set name
Action:	Action either to allow or to block
RefCount:	Number of times the action set was used by entries in other tables
NumUsed:	Number of times the action set was used in screening activity to allow or block an MSU

Related Commands

Command	Description
cs7 gws action-set	Specifies gateway screening action sets.

show cs7 gws as

To display Cisco ITP gateway screening AS information, use the **show cs7 gws as** EXEC command.

show cs7 [*instance-number*] **gws as** [*name as-name* | **default**]

Syntax Description		
	<i>instance-number</i>	Specifies the instance. The valid range is 0 to 7. The default instance is 0.
	name	Specifies the AS.
	<i>as-name</i>	Name of the AS.
	default	Displays information about the default entry for the AS.

Defaults The default instance is 0.

Command Modes EXEC

Command History	Release	Modification
	12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.
	12.4(15)SW6 12.2(33)IRF	Enhanced to show the number of MSUs discarded silently or with an error due to the rate limit feature.

Examples The following example includes output from the **show cs7 gws as** command with no keywords:

```
ITP# show cs7 gws as
AS name: 'default' Instance: 0 Screening: Enabled
  Inbound screening - not defined
  Outbound screening - not defined
AS name: dallas-as Instance: 0 Screening: Enabled
  Inbound Screening ---- Result: Table OPCALLOW
    Inbound Logging : type both file verbose
      MSUs Screened:      0, Allowed:      0, Blocked:      0
      MSUs Suspended:    0, Resumed:      0
  Outbound Screening ---- Result: Action-set ALLOW
    Outbound Logging : type both file verbose
      MSUs Screened:      0, Allowed:      0, Blocked:      0

AS name: dallas-sua Instance: 0 Screening: Enabled
  Inbound Screening ---- Result: Table OPCALLOW
    Inbound Logging : type both file verbose
      MSUs Screened:      0, Allowed:      0, Blocked:      0
      MSUs Suspended:    0, Resumed:      0
  Outbound Screening ---- Result: Action-set ALLOW
    Outbound Logging : type both file verbose
      MSUs Screened:      0, Allowed:      0, Blocked:      0
```

[Table 46](#) describes the fields in the display.

Table 46 *show cs7 gws as Field Descriptions*

Field	Description
AS name	AS name
Instance	Instance number
Screening	Indicates whether screening is enabled or disabled (if corresponding CS7 AS is defined, field indicates enabled)
Inbound Screening	Indicates whether inbound screening is defined and, if defined, indicates the result
Result	Result action set or table name
Inbound Logging	Logging parameters that have been configured
MSUs Screened	Number of MSUs screened
Allowed:	Number of MSUs allowed
Blocked:	Number of MSUs blocked
MSUs Suspended	Indicates that, for CDPA screening, MSU screening is suspended for GTT
Resumed:	Indicates that, after GTT, screening is resumed
Outbound Screening	Indicates whether outbound screening is defined and, if defined, indicates the result
Outbound Logging	Logging parameters that have been configured
MSUs Screened	Number of MSUs screened
Allowed:	Number of MSUs allowed
Blocked:	Number of MSUs blocked
Rate Limit	The GWS rate limit traffic rate feature.
MSUs Discarded silently	Number of MSUs silently discarded when the rate limit of the GWS rate limit feature is exceeded.
MSUs Discarded with error	Number of MSUs discarded with an error message sent when the sending of a return on error option is configured on the GWS rate limit feature.

Related Commands

Command	Description
cs7 gws as	Specifies an AS table for gateway screening.

show cs7 gws config

To display the whole configuration of GWS, including global action sets, linksets, global table entries, tables, and table entries, use the **show cs7 gws config** command in EXEC mode.

show cs7 [*instance-number*] **gws config**

Syntax Description	<i>instance-number</i>	Specifies the instance. The valid range is 0 to 7. The default instance is 0.

Defaults	The default instance is 0.

Command Modes	EXEC

Command History

Examples The following example includes output from the **show cs7 gws config** command:

```
Router# show cs7 gws config
cs7 instance 0 gws action-set action-set1 mlr group test pam pam1
cs7 instance 0 gws action-set action-set2 mlr ruleset test pam pam2
cs7 instance 0 gws action-set action-set2 allow pam pam3
```

Related Commands	Command	Description
	show cs7 gws table	Specifies a linkset table for gateway screening.
	cs7 gws-table replace	Replaces a single GWS table with the table configuration file specified by the URL.
	cs7 gws load	Loads GWS configuration, including GWS tables, from a specified remote or local file during a Cisco ITP restart or reload.
	cs7 gws replace	Replaces the running GWS configuration file or existing GWS tables with ones from a local or remote file.

show cs7 gws counters

To display the counters in GWS packet processing, use the **show cs7 gws counters** command in EXEC mode.

show cs7 gws counters

Syntax Description	None.

Defaults	None.

Command Modes	EXEC

Command History	

Examples	The following example includes output from the show cs7 gws counters command:

```
Router# show cs7 gws counters
ITP-251#sh cs7 gws counters
GWS Counters instance:
SCCP unable to parse the packet:
Number of UDTs missed:
PC entry not found:
No valid entry for pcssn in table with scmg=0:
SI entry not found in table:
Entry corresponding to MTP3 message not found:
Entry corresponding to ISUP message not found:
Entry for message type is not found:
GTT selector not found in the table:
GTA entry not found in the table:
Invalid routing indicator:
Invalid number of concerned pc's:
Unsupported SCCP message type:
Screening count exceeds the maximum limit:
Action-set or table is not available in the result:
MLR routing info in gws action set is NULL:
Invalid global entry or inbound Screening not defined:
Outbound Screening not defined:
Entry for GWS Ls is invalid:
Default Entry for GWS Ls is invalid:
Ingress rate limit is crossed for LS:
Egress rate limit is crossed for LS:
Entry for GWS as is invalid:
Ingress rate limit is crossed for AS:
Egress rate limit is crossed for AS:
```

show cs7 gws linkset

To display ITP gateway screening information for a linkset, use the **show cs7 gws linkset EXEC** command.

show cs7 [*instance-number*] **gws linkset** [**name** *ls-name* | **default**]

Syntax Description

<i>instance-number</i>	Specifies the instance. The valid range is 0 to 7. The default instance is 0.
name	Specifies the linkset.
<i>ls-name</i>	Name of the linkset.
default	Shows the default linkset information.

Defaults

The default instance is 0.

Command Modes

EXEC

Command History

Release	Modification
12.4(15)SW1	This command was introduced.
12.2(18)IXE	This command was introduced.
12.4(15)SW6 12.2(33)IRF	This command was modified to show the number of MSUs discarded silently or with an error due to the rate limit feature on inbound screening.
12.4(15)SW7 12.2(33)IRG	This command was modified to show the number of MSUs discarded silently or with an error due to the rate limit feature on outbound screening.

Examples

The following example includes output from the **show cs7 gws linkset** command with no keywords:

```
ITP# show cs7 gws linkset name hsl_tg3_0
Linkset name: hsl_tg3_0 Instance: 0 Screening: Enabled
  Inbound Screening ---- Result: Action-set ac1
    Rate Limit timer : 60 Rate Limit Threshold---onset: 90 abate: 80 MSUs Screened :
1200, Allowed: 1200, Blocked: 0
    MSUs MLR routed : 0
    MSUs Suspended: 0, Resumed: 0
  Rate Limit
    MSUs Discarded silently: 20
  Outbound Screening ---- Result: Action-set ac1
    Egress Rate Limit timer : 5 Egress Rate Limit Threshold---onset: 80 abate: 60 MSUs
Screened : 2000, Allowed: 2000, Blocked: 0
    MSUs MLR routed : 0
    MSUs Suspended: 0, Resumed: 0
  Egress Rate Limit
    MSUs Discarded silently: 150
    MSUs Discarded with error: 0
```

[Table 47](#) describes the fields in the display.

Table 47 *show cs7 gws linkset Field Descriptions*

Field	Description
Linkset name	Linkset name.
Instance	Instance number.
Screening	Indicates whether screening is enabled or disabled (if corresponding CS7 linkset is defined, indicates enabled)
Inbound Screening	Indicates whether inbound screening is defined and, if defined, indicates the result
Result	Result action set or table name
Inbound Logging	Logging parameters that have been configured
MSUs Screened	Number of MSUs screened
Allowed:	Number of MSUs allowed
Blocked:	Number of MSUs blocked
MSUs Suspended	Indicates that, for CDPA screening, MSU screening is suspended for GTT
Resumed:	Indicates that, after GTT, screening is resumed
Outbound Screening	Indicates whether outbound screening is defined and, if defined, indicates the result
Outbound Logging	Outbound logging parameters that have been configured
MSUs Screened	Number of MSUs screened
MSUs Suspended	Indicates that, for CDPA screening, MSU screening is suspended for GTT
Rate Limit	The GWS rate limit traffic rate feature.
MSUs Discarded silently	Number of MSUs silently discarded when the rate limit of the GWS rate limit feature is exceeded.

Related Commands

Command	Description
cs7 gws linkset	Specifies a linkset table for gateway screening.

show cs7 gws table

To display gateway screening table details, use the **show cs7 gws table** EXEC command.

show cs7 [**instance** *instance-number*] **gws table** [[**name** *table-name*] | [**type** *table-type*]] [**detail** | **entry-summary** | **result-summary**]

Syntax Description

instance <i>instance-number</i>	Specifies the instance. The valid range is 0 to 7. The default instance is 0.
name <i>table-name</i>	Specifies the table name.
type <i>table-type</i>	Displays information about tables of a specified type. Specifies the table type. Valid types are:
	aff-dest Affected Dest Table
	aff-pc-ssn SCCP Aff. PC-SSN Table
	cdpa-pc-prefix CdPA GTA Prefix Table
	cdpa-pc-range CdPA GTA Range Table
	cdpa-pc-ssn CdPA PC-SSN Table
	cdpa-selector CdPA Selector Table
	cdpa-pc-prefix CdPA GTA Prefix Table
	cdpa-pc-range CdPA GTA Range Table
	cgpa-pc-ssn CgPA PC-SSN Table
	cgpa-selector CgPA Selector Table
	dpc DPC Table
	isup-msg-type ISUP Msg Type Table
	mtp-msg-type MTP Msg Type Table
	opc OPC Table
	sccp-msg-hdr SCCP Msg Hdr Table
	sio SIO Table
detail	Displays detailed statistics of the table.
result-summary	Displays a summary of the table results.
entry-summary	Displays a summary of the table entries.

Defaults

The default instance is 0.

Command Modes

EXEC

Command History

Release	Modification
12.2(33)IRA	This command was introduced.

Examples

The following example includes output from the **show cs7 gws table** command:

```
ITP# show cs7 gws table name OPCALLOW
```

```
Table Name:OPCALLOW Type:opc Action Type:allowed Instance:0
```

```

Start-PC      End-PC      Result
-----
default
3.3.3         3.3.4         Table al-cg-pcssn
3.3.5         Table al-cg-pcssn

```

The following example includes output from the **show cs7 gws table** command specified with the **detail** keyword:

```
ITP# show cs7 gws table name OPCALLOW detail
```

```
Table Name:OPCALLOW Type:opc Action Type:allowed Instance:0
```

```
Table Statistics:
```

```

-----
MSUs Screened :      0
MSUs Allowed  :      0
MSUs Blocked  :      0
Num Entries   :      2
Ref Count     :      2

```

```
Parameters:
```

```

-----
Default Result: Action-set ALLOW
Start PC: 3.3.3 End PC: 3.3.4
Result: Table al-cg-pcssn
MSUs Screened:  80
MSUs Allowed   :  60
MSUs Blocked   :  20
Start PC: 3.3.5
Result: Table al-cg-pcssn
MSUs Screened:  70
MSUs Allowed   :  30
MSUs Blocked   :  40

```

[Table 48](#) describes the fields in the display.

Table 48 *show cs7 gws table Field Descriptions*

Field	Description
Table Name	Table name
Type	Table type
Action Type	Type of screening action performed (allowed or blocked)
Start-PC	Starting pc in the range
End-PC	Ending pc in the range
Result	Action set or table
Table Statistics:	
MSUs Screened	Number of MSUs screened
MSUs Allowed	Number of MSUs allowed

Table 48 *show cs7 gws table Field Descriptions (continued)*

Field	Description
MSUs Blocked	Number of MSUs blocked
Num Entries	Number of entries defined in this table
Ref Count	Number of times this table is referenced by others
Parameters:	
Default Result	Default result action set or table
Start PC End PC	Start and End point codes
Result	Result action set or table
MSUs Screened	Number of MSUs screened
MSUs Allowed	Number of MSUs allowed
MSUs Blocked	Number of MSUs blocked

Related Commands

Command	Description
cs7 gws table	Defines a gateway screening table.

show cs7 linkset

To display ITP linkset information, use the **show cs7 linkset** EXEC command.

show cs7 [*instance-number*] **linkset** [*ls-name* | **cell** | **combined** | **routes** | **sls** | **state** | **statistics** | **timers** | **tmap** | **utilization**] [**brief** | **detailed**]

Syntax Description		
<i>instance-number</i>		Specifies the instance. The valid range is 0 to 7. The default instance is 0.
brief		Does not display individual links.
combined		Displays all combined linksets.
cell		Displays HSL cell counts for the linkset.
detailed		Displays detailed linkset information.
<i>ls-name</i>		Displays information for the specified linkset.
routes		Displays all routes using a linkset.
sls		Displays SLC to SLS relationship.
state		Displays MTP3 states for link.
statistics		Displays link usage statistics.
timers		Displays timer values.
tmap		Displays TT mappings for linkset.
utilization		Displays link utilization statistics.

Defaults The default instance is 0.

Command Modes EXEC

Command History	Release	Modification
	12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.
	12.4(15)SW3 12.2(33)IRC	PMP status and assigned inbound and/or outbound DCS groups were added to the information displayed with the detailed keyword.

Usage Guidelines The **cs7 util-plan-capacity** command must be configured globally or the **plan-capacity-rcvd** and **plan-capacity-send** commands must be configured in the cs7 link submode for a complete output of the **show cs7 linkset ls-name utilization** command.

Examples

Linkset States

- **UNAVAIL** Indicates the linkset does not have any “available” links and cannot transport traffic.
- **shutdown** Indicates the linkset has been shut down in the configuration.

- **avail** Indicates the linkset has at least one available link and can carry traffic.

Link States

- **UNAVAIL**

Indicates the link is not available to carry traffic. This unavailability can occur if the link is remotely or locally inhibited by a user. It can also be unavailable if MTP2 or M2PA has not been able to successfully activate the link connection, or the link test messages sent by MTP3 are not being acknowledged.

- **shutdown**

Indicates the link has been shut down in the configuration. A link is in this state when it is shut down at the MTP3 layer.

- **avail**

Indicates the link is active and able to transport traffic.

- **FAILED**

Indicates the link is not shut down but is unavailable at Layer 2 for some reason, or it is unavailable because it has been inhibited or blocked.

- **sys-shutdown**

Indicates the link has been shut down by the system. A link may be in this state when:

- MTP3 offload is configured and the system is performing error recovery on the line card.
- MTP3 offload has been permanently disabled on a line card by the system due to excessive errors. When MTP3 offload has been permanently disabled on a line card (by the system), all links on that line card are in the sys-shutdown state.

The following example includes output from the **show cs7 linkset** command with no keyword options:

```
ITP# show cs7 linkset
lsn=to_sandy      apc=1.4.2      state=avail      available/links=1/1
  SLC  Interface          Service  PeerState      Inhib
    00  172.18.44.151 4096 4096      avail    InService      -----

lsn=to_doc        apc=1.4.3      state=avail      available/links=1/1
  SLC  Interface          Service  PeerState      Inhib
    00  Serial2/0/0:0      avail    -----        -----
```

The following example includes output from the **show cs7 linkset** command with the **cell** keyword:

```
ITP# show cs7 linkset cell
lsn=7570c_to_757  apc=3.10.4      state=avail      available/links=1/1
  SLC  Cells In   Cells Out
    0   12285197  10902248
```

The following example includes output from the **show cs7 linkset** command with the **detailed** keyword:

```
MSTP# show cs7 linkset STP1 detailed
lsn=STP1          apc=2.76.0      state=avail      avail/links=1/1
  Local Point Code =2.24.0      Adjacent Restart Enabled = Y
  Broadcast TFP     =Y           Broadcast TFA         = Y
  Access Group IN   = NONE       Access Group OUT      = NONE
  MTP3 Accounting   = Y          GTT Accounting        = N
  Rotate SLS        = Y          Remote Processor Outage = N
  SLS Shift         = 0
  Input QOS Match   = NONE

  SLC QoS Interface          Service  PeerState      Inhib
    00  0 172.18.44.181 4100 4100      avail    InService      -----
```

```

Address List  Pri  Eff  State      SRTT
172.18.44.181  P    E   active    47 ms

```

The following example includes output from the **show cs7 linkset** command with the **routes** keyword:

```

ITP# show cs7 linkset routes
lsn=to_sandy      apc=1.4.2      state=avail      available/links=1/1
Destination      Cong Prio QoS Route  Route Table
-----
1.4.3/14         acces          9      avail  system
1.5.3/14         INACC          9      UNAVAIL system
1.3.3/14         acces          9      avail  system
1.2.3/14         acces          9      avail  system
1.4.2/14         acces          1      avail  system

lsn=to_doc        apc=1.4.3      state=avail      available/links=1/1
Destination      Cong Prio QoS Route  Route Table
-----
1.4.3/14         acces          1      avail  system

```

The following example includes partial output for an ITU variant ITP configured for QoS. The output is from the **show cs7 linkset** command with the **sls** keyword. QoS class 0 (the default class) shows peer link member slc 0 and QoS class 1 shows peer link member slc 1. QoS class 2 does not have any peer link members available.

```

ITP# show cs7 linkset michael sls
lsn=michael      apc=3.3.3      state=avail      available/links=2/3

QOS Level 0
sls->slc    sls->slc    sls->slc    sls->slc
00->00      04->00      08->00      12->00
01->00      05->00      09->00      13->00
02->00      06->00      10->00      14->00
03->00      07->00      11->00      15->00

QOS Level 1
sls->slc    sls->slc    sls->slc    sls->slc
00->01      04->01      08->01      12->01
01->01      05->01      09->01      13->01
02->01      06->01      10->01      14->01
03->01      07->01      11->01      15->01

No available links for QOS Level 2...

```

The following example includes output from the **show cs7 linkset** command with the **state** keyword:

```

ITP# show cs7 linkset STP1 state
lsn=STP1 apc=2.76.0 state=avail avail/links=1/1
Broadcast TFP = Y Broadcast TFA = Y
TCBC Q depth (cur/high) = 0/0
SLC Interface Service PeerState Inhib
00 172.18.44.181 4100 4100 avail InService -----
Link Congestion Level = 0
LSAC state = LSAC_active , emergency = F
LSAC link_loaded = T, stm_ready_rcvd = F
Link shutdown by system = NO
TSRC state =idle
TSRC link_available = T, link_inhibited = F
TSRC changeover_complete = F TSRC adjacent SP restart = F
TLAC state =available, management_request = F
TLAC locally_inhibited = F
TLAC remotely_inhibited = F, inhibit_retry = F
TLAC emergency_changeover_order = F, changeback_in_progress = F
TLAC changeover_in_progress = F, failed = F
TLAC remote_blocked = F, adjacent_SP_restarting = F

```

```

TLAC SP_restarting = F
TLAC fsn = 0
TCOC state = idle, buffering = F
TCOC retrieveQ depth (cur/high) = 0/0
TCOC bufferedQ depth (cur/high) = 0/0
TCOC link_unavailable = F
TCOC sequence controlled = 0, time controlled = 0
TCOC msu initiated = 0, not required = 0
TCOC not retrievable = 0, retrieve timeout = 0
TCBC state = idle, buffering = F
TCBC sequence controlled = 0 time controlled = 1
TCBC no traffic to divert = 0 not required = 0

```

The following example includes output from the **show cs7 linkset** command with the **statistics** keyword:

```

ITP# show cs7 linkset statistics
lsn=to_sandy      apc=1.4.2      state=avail      available/links=1/1
  SLC      MSU In      MSU Out      Drops      LSSU In      LSSU Out      ByteCnt In      ByteCnt Out
  00      31978      32773      0      4      6      570321      583852

lsn=to_doc        apc=1.4.3      state=avail      available/links=1/1
  SLC      MSU In      MSU Out      Drops      LSSU In      LSSU Out      ByteCnt In      ByteCnt Out
  00      26369      26681      0      501      620      316140      320398

```

The following example includes output from the **show cs7 linkset** command with the **timers** keyword:



Note

The Scope field indicates where the linkset timer value was configured. For example, if the linkset timer value was configured from the global configuration level, the scope field displays “global.” If the linkset timer value was configured from the linkset submode configuration level, the scope field displays “ls.”

```

ITP# show cs7 linkset to_doc timers
lsn=to_doc        apc=1.4.3      state=avail      available/links=1/1
Timer  Value(ms)  Description                                     Scope
-----
t19      68000  (supervision timer during MTP restart)           ls
t21      64000  (MTP restart timer at adjacent signaling point)   ls

link slc = 0
Timer  Value(ms)  Description                                     Scope
-----
t01      800    (delay to avoid msg mis-seq. on changeover)       link
t02     1400  (waiting for changeover acknowledgement)         link
t03      800    (time controlled delay to avoid mis-seq.)         link
t04      800    (waiting for change back ack.(first attempt))     link
t05      800    (waiting for change back ack.(second attempt))    link
t12     1150  (waiting for uninhibit acknowledgement)           link
t13     1150  (waiting for force uninhibit)                     link
t14     2500  (waiting for inhibition acknowledgement)           link
t17     1150  (delay to avoid oscillation of initial alignment)  link
t22    300000  (local inhibit test timer)                        link
t23    300000  (remote inhibit test timer)                       link
t24      500    (stabilizing timer after local processor outage)   link
slt-t01   8000  (signaling link test acknowledgement timer)       link
slt-t02  60000  (interval timer for sending test msgs.)           link
retry    60000  (link activation retry timer)                     link

```

The following example includes output from the **show cs7 linkset** command with the **ttmap** keyword:

```

ITP# show cs7 linkset ttmap
lsn=ernesto      apc=1.13.1      state=avail      available/links=1/1
  ETT  MTTin  MTTout
  254  10      ---

```

```
lsn=mgts2          apc=1.12.1          state=avail          available/links=1/1
  ETT  MTTin  MTTout
  10   254   254

lsn=mgts1          apc=1.11.1          state=avail          available/links=1/1
  ETT  MTTin  MTTout
   6   254   ---
 254   11    11
```

The following example includes output from the **show cs7 linkset** command with the **utilization** keyword:

```
Router #show cs7 linkset to-75b-fast utilization
Sample Interval(seconds):120  Thresholds onset/abate:40/30
lsn=to-75b-fast  apc=4.1.2          state=avail          available/links=4/5
  Link Utilization Thresholds Plan-capacity(bps) Kbps
    SLC      Rec  Sent  Rec  Sent  Rec  Sent      Rec  Sent
    0         0    0    50  50   128  128         0    0
    1         0    0    40  40   256  256         0    0
    7         0    0    40  40     0    0         0    0
    8         0    0    40  40     0    0         0    0
   13         0    0    40  40     0    0         0    0
```

Where

```
SLC Signaling link code
Link Utilization Rec => link receive utilization 0-999
Link Utilization Sent => link receive utilization 0-999
Link Thresholds Rec => receive threshold to generate traps
Link Thresholds Sent => Sent threshold to generate traps
Link Plan-capacity Rec => estimate of link receive capacity
Link Plan-capacity Sent => estimate of link send capacity
Kbps Rec => average Kilobits received per second on link
Kbps Sent => average Kilobits sent per second on link
```

After the addition of the probeless monitoring feature to ITP, the output contains two new fields: Inbound DCS Group and Outbound DCS Group. The following example includes output from the **show cs7 linkset** command with the **detailed** keyword.

```
lsn=to_halley_6          apc=6.3.3:6          state=avail          avail/links=4/4
  Local Point Code = 6.2.2:6          Adjacent Restart Enabled = Y
  Broadcast TFP = Y          Broadcast TFA = Y
  Preventive TFP = Y          Emergency = N
  MTP3 Accounting = Y          GTT Accounting = Y
  Rotate SLS = Y          SLS Shift = 0
  Access Group IN = NONE          Access Group OUT = NONE
  Input QOS Match = NONE
  C-link ls = N          C-link ls secondary = N
  CRD state = 0          PMP Status = Y
  Inbound DCS Group = group_pmp_02          Outbound DCS Group = group_pmp_01

  SLC  Interface          Service  PeerState          Inhib
  00   Serial4/1/0:0      avail   -----          -----
  01   Serial4/1/0:1      avail   -----          -----
  02   Serial4/1/0:2      avail   -----          -----
  03   Serial4/1/0:3      avail   -----          -----
```

Related Commands	Command	Description
	cs7 prompt enhanced	Configures the command line interface (CLI) prompt to display the current linkset.
	cs7 util-abate	Specifies the integer range utilization threshold.
	cs7 util-sample-interval	Specifies the sample interval for link utilization.
	cs7 util-threshold	Specifies the global threshold for link utilization.
	link-timer	Configures MTP3 timers that control the link.
	plan-capacity-rcvd	Specifies the link receive planning capacity.
	plan-capacity-send	Specifies the link send planning capacity.
	show cs7 mtp3 timers	Displays all global timers, and all linkset and link timers that have been defined at the global level.
	show tech-support	Collects and displays a large amount of ITP configuration information that can be used for troubleshooting.
	threshold-rcvd	Specifies the receive threshold for a link.
	threshold-send	Specifies the send threshold for a link.
	timer (cs7 linkset)	Configures MTP3 timers that control the linkset (and, optionally, timers for links on the linkset).
	tmap	Assigns a translation type mapping rule to the linkset.
	dcs-group	Identifies a name to be associated with a DCS group.

show cs7 log

To display the current log, use the **show cs7 log** command in global configuration mode.

show cs7 log *type*

Syntax Description	<i>type</i>	Specifies the type of log. Valid log types are:
	• gtt	Information related to global title translation.
	• gws-nontest	Information related to GWS logging in nontest mode.
	• gws-test	Information related to GWS logging in test mode.

Defaults	None.

Command Modes	Global configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced for <i>type</i> gtt.
	12.4(11)SW	
	12.2(33)IRA	

Examples The following example includes output from the **show cs7 log gtt** command:

```
itp# show cs7 log gtt
```

```
Error Log: 779 of 10000 errors in log.
```

```
11:56:40 : No translation configured.
```

```
MsgType udt    LS: mgts2
```

```
OPC: 1-12-1      CgPA: tt 9 gta 1065433330 pc 1-12-1
```

```
DPC: 1-2-2      CdPA: tt 10 gta 712148002887 ssn 7
```

```
11:56:40 : No translation configured.
```

```
MsgType udt    LS: mgts1
```

```
OPC: 1-11-1      CgPA: tt 9 gta 1065433330 pc 1-11-1
```

```
DPC: 1-2-2      CdPA: tt 10 gta 712148002887 ssn 7
```

```
11:56:40 : No translation configured.
```

```
MsgType udt    LS: mgts2
```

```
OPC: 1-12-1      CgPA: tt 9 gta 1065433330 pc 1-12-1
```

```
DPC: 1-2-2      CdPA: tt 10 gta 712148002887 ssn 7
```

 show cs7 log

Related Commands	Command	Description
	cs7 log	Enables the ITP to log events, errors, and traces.
	cs7 log checkpoint	Enables automatic archiving of a log to a remote or local destination at a specified interval of every <i>secs</i> seconds.
	cs7 save log	Saves a log to a file.

show cs7 m2pa

To display ITP M2PA statistics, use the **show cs7 m2pa** EXEC command.

show cs7 m2pa [**congestion** *ls-name* | **local-peer** *port-num* | **peer** *ls-name* [*slc*] | **sctp** {**parameters** | **statistics**} *ls-name* [*slc*] | **state** *ls-name* [*slc*] | **statistics** *ls-name* [*slc*] | **timers** *ls-name* [*slc*]]

Syntax Description		
congestion		Displays M2PA congestion status.
local-peer		Displays information about an M2PA local peer.
<i>port-num</i>		Port number of the local peer. Valid range is 4096 to 32767.
peer		Displays information about an M2PA remote peer.
sctp parameters		Displays SCTP peer parameters.
sctp statistics		Displays SCTP peer statistics.
state		Displays the M2PA state machine status.
statistics		Displays the M2PA peer statistics.
timers		Displays M2PA timers for RFC.
<i>ls-name</i>		Linkset name.
<i>slc</i>		Signaling link code. Valid range is 0 to 15.

Defaults None.

Command Modes EXEC

Command History	Release	Modification
	12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.
	12.2(18)IXH 12.4(15)SW3 12.2(33)IRC	The show cs7 m2pa peer command was added to verify that the large MSU feature is turned on or off.

Examples

The following example includes output from the **show cs7 m2pa** command using the **congestion** keyword with the linkset name (*ls-name* argument) **to_nagshead**:

```
ITP#show cs7 m2pa congestion to_nagshead
```

```
CS7 M2PA Congestion Status for (50.0.0.5 : 4000)
```

```
RxCongestion status      : Abated          RxCongestionCount drops: 0
RxCongestionCount onset: 0          RxCongestionCount abate: 0
```

```
TxCongestion status      : Abated (Level0)
TxCongestionCount Level 1: 0          TxCongestionCount Level 2: 0
TxCongestionCount Level 3: 0          TxCongestionCount Level 4: 0
```

```

Tx Queue (max)      : 1000
Tx Queue (size)     : 0

Tx Level 1 onset    : 500 ( 50% of Tx Queue Depth)
Tx Level 2 onset    : 700 ( 70% of Tx Queue Depth)
Tx Level 3 onset    : 900 ( 90% of Tx Queue Depth)
Tx Level 4 onset    : 1000 (100% of Tx Queue Depth)

```

The following example includes output from the **show cs7 m2pa** command using the **local-peer** keyword with the port number (*port-num* argument) **9000**:

```

ITP#show cs7 m2pa local-peer 9000
CS7 M2PA Local Peer Info for local port = 9000

Local Port          = 9000
Local IP            = 172.18.44.163
SCTP Instance Handle: 8           Offload: No
Instance Local Recv Window: 64000 Instance maxInitRetrans: 8
Instance maxInitTimeout: 1000 ms  Instance Unordered Priority: EQUAL
Instance IP Precedence: 0

```

The following example includes output from the **show cs7 m2pa** command using the **peer** keyword with the linkset name (*ls-name* argument) **alpha**. The **show cs7 m2pa** command with the **peer** keyword displays the status of the large MSU feature with the field *Large MSU Supported*.

```

ITP#show cs7 m2pa peer alpha
CS7 M2PA internal Peer Control Block Info for (172.18.40.46 : 10001)

Peer Protocol      : sctp
Peer Port          : 10001
Peer Version       : RFC
Peer Address       : 172.18.40.46
Primary Address    : 172.18.40.46
Effective Address  : 172.18.40.46

Transport Handle    : 0x1C010001      Passive Peer      : FALSE
Transport Handle History: 0x00000000 0x00000000 0x00000000 0x00000000
Hold Transport      : TRUE            Assoc Retransmission: 10
Init Retransmission : 8               Init RTO Max       : 1000    ms
Path Retransmission : 4               Cumulative Sack    : 200     ms
Bundling            : Enabled          Bundle Timeout     : 5        ms
Minimum RTO         : 1000            Maximum RTO        : 1000    ms
IP Precedence       : 0               QoS class         : 0
Keep Alive          : Enabled          Keep Alive Timeout : 30000 ms
Initial cwnd        : 3000            Idle cwnd rate     : 50
Retrans cwnd rate   : 50              Retrans cwnd mode  : RFC
FastRetransmit cwnd rate: 50          m2paCfgMode       : RFC
n1                  : 1000            Debug mask        : 0x00000004
Large MSU Supported : TRUE

```

The following example includes output from the **show cs7 m2pa** command using the **sctp parameters** keywords with the linkset name (*ls-name* argument) **to_nagshead** and the signaling link code value (*slc* argument) **0**:

```

ITP#show cs7 m2pa sctp parameters to_nagshead 0

** SCTP Association Parameters AssocID:0x00010001

AssocID: 0x00010001 Instance ID: 0 Offload: No
Assoc state: ESTABLISHED Context: 2187768704 Uptime: 1d01h
Local port: 4000

```

```

Local addresses: 50.0.0.3 172.18.44.163

Remote port: 4000
Primary dest addr: 50.0.0.5
Effective primary dest addr: 50.0.0.5
Destination addresses:

50.0.0.5   State: ACTIVE
  Heartbeats: Enabled   Timeout: 30000 ms
  RTO/RTT/SRTT: 1000/16/9 ms   TOS: 0   MTU: 1500
  cwnd: 3072   ssthresh: 64000   outstand: 0
  Retrans cwnd rate: 50   Retrans cwnd mode: RFC
  FastRetrans cwnd rate: 50   Idle dest cwnd rate: 50
  Num retrans: 3   Max retrans: 4   Num times failed: 0
  50.0.0.3 retrans: 0   172.18.44.163 retrans: 0

172.18.44.162   State: ACTIVE
  Heartbeats: Enabled   Timeout: 30000 ms
  RTO/RTT/SRTT: 1000/4/0 ms   TOS: 0   MTU: 1500
  cwnd: 3000   ssthresh: 64000   outstand: 0
  Retrans cwnd rate: 50   Retrans cwnd mode: RFC
  FastRetrans cwnd rate: 50   Idle dest cwnd rate: 50
  Num retrans: 2   Max retrans: 4   Num times failed: 0
  50.0.0.3 retrans: 0   172.18.44.163 retrans: 0

Local vertag: 4B6AECE0   Remote vertag: ADB2E766
Num inbound streams: 2   outbound streams: 2
Max assoc retrans: 10   Max init retrans: 8
CumSack timeout: 200 ms   Bundle timeout: 5 ms enabled
Min RTO: 1000 ms   Max RTO: 1000 ms
LocalRwnd: 64000   Low: 63927   RemoteRwnd: 64000   Low: 63972
Congest levels: 4   current level: 0   high mark: 5   chkSum: crc32

```

The following example includes output from the **show cs7 m2pa** command using the **sctp statistics** keywords with the linkset name (*ls-name* argument) **to_nagshead** and the signaling link code value (*slc* argument) **0**:

```

ITP#show cs7 m2pa sctp statistics to_nagshead 0

** SCTP Association Statistics AssocId:0x00010001 **

AssocID: 0x00010001   InstanceID: 0 Offload No
Current State: ESTABLISHED
Control Chunks
  Sent: 14572   Rcvd: 14576
Data Chunks Sent
  Total: 6140   Retransmitted: 0
  Ordered: 6140   Unordered: 0
  Avg bundled: 0   Total Bytes: 190673
Data Chunks Rcvd
  Total: 6149   Discarded: 0
  Ordered: 6149   Unordered: 0
  Avg bundled: 1   Total Bytes: 190758
  Out of Seq TSN: 0
ULP Dgrams
  Sent: 6140   Ready: 6149   Rcvd: 6149
DataGrams Sent: 16119   DataGrams Rcvd: 6128
RexmitTO: 0   RexmitFAST: 0

```

The following example includes output from the **show cs7 m2pa** command using the **state** keyword with the linkset name (*ls-name* argument) **to_nagshead**:

ITP#**show cs7 m2pa state to_nagshead**

CS7 M2PA states for Peer (50.0.0.5 : 4000)

```

Link State Control (LSC)           : InService
SCTP State                        : sctpEstablished
Initial Alignment Control (IAC)    : Idle
Transmission Control (TXC)        : InService
Reception Control (RC)             : InService
Processor Outage Control (POC)     : Idle

Peer Version      : RFC
Cfgd Version      : RFC
Emergency         : FALSE
Hold Transport    : TRUE
Msu Inhibited     : FALSE
Msu Accepted      : TRUE
Tx Queue          : 0
Local ProcOutage  : FALSE
Remote ProcOutage : FALSE

bsnr: 4586      bsnt: 4583      fsnc: 0      fsnt: 4586
fsnf: 4587      fsnl: 4586      fsnr: 4583     fsnx: 4584

```

The following example includes output from the **show cs7 m2pa** command using the **statistics** keyword with the linkset name (*ls-name* argument) **to_nagshead**:

ITP#**show cs7 m2pa statistics to_nagshead**

CS7 M2PA Peer Statistics for (50.0.0.5 : 4000)

```

BytesTransmitted:      166189      BytesReceived:      190962
MSU_XMIT:              4591        MSU_RCV:            4588
MSU_XMIT_Drop:         0           MSU_RCV_Drop:       0
MSU_XMIT_Fail:         0           MSU_RCV_Fail:       0
MSU_XMIT_DataAck:      1543        MSU_RCV_DataAck:    1563
MSU_XMIT_Ack_Drop_Count: 0         MSU_RCV_Ack_Drop_Count: 0

LSSU_XMIT:             15          LSSU_RCV:           7
LSSU_XMIT_Fail:        0           LSSU_RCV_Invalid:   0
LSSU_XMIT_SIIS:        0           LSSU_RCV_SIIS:      0
LSSU_XMIT_SIALIGN:     1           LSSU_RCV_SIALIGN:   1
LSSU_XMIT_SIE:         5           LSSU_RCV_SIE:       0
LSSU_XMIT_SIN:         0           LSSU_RCV_SIN:       5
LSSU_XMIT_SIREADY:     1           LSSU_RCV_SIREADY:   1
LSSU_XMIT_SIOS:        0           LSSU_RCV_SIOS:      0
LSSU_XMIT_SIPOCount:   1           LSSU_RCV_SIPOCount: 0
LSSU_XMIT_SIPOECount:  2           LSSU_RCV_SIPOECount: 0
LSSU_XMIT_SIBCount:   3           LSSU_RCV_SIBCount:  0
LSSU_XMIT_SIBECCount:  2           LSSU_RCV_SIBECCount: 0
AbnormalBSN_rcvd:     0           UnreasonableBSN_rcvd: 0
UnexpectedFSN_rcvd:   0           AbnormalFSN_rcvd:   0
Remote_PO_Count:      0           Remote_Congestion_Count: 0
CongestionCount:      0           RxCongestionCount_drops: 0
Level 1 TxCongestCount: 0          Level 2 TxCongestCount: 0
Level 3 TxCongestCount: 0          Level 4 TxCongestCount: 0
T1_TMO_Count:         0           T2_TMO_Count:       0
T3_TMO_Count:         0           T4_TMO_Count:       0
T6_TMO_Count:         0           T7_TMO_Count:       0

```

The following example includes output from the **show cs7 m2pa** command using the **timers** keyword with the linkset name (*ls-name* argument) **to_nagshead**:

```
ITP#show cs7 m2pa timers to_nagshead

CS7 M2PA Timers for RFC      (50.0.0.5 : 4000)

T1   (alignment ready)      : 45000    ms
T2   (not aligned)          : 60000    ms
T3   (aligned)              : 2000     ms
T4   (emergency proving)    : 500      ms
T4   (normal proving)       : 8000     ms
T6   (remote congestion)    : 4000     ms
T7   (excess ack delay)    : 0        ms
Lssu (lssu interval)       : 4000     ms
```

Table 49 describes the fields in the **show cs7 m2pa statistics** display.

Table 49 *show cs7 m2pa statistics Field Descriptions*

Field	Description
M2PA Peer State	State of the M2PA peer link
SCTP Peer State	State of the associated SCTP peer link
MSU_XMIT_Count	Number of message signal units transmitted
MSU_RCV_Count	Number of message signal units received
LSSU_XMIT_Count	Total number of Link Status Signal Units transmitted
LSSU_XMIT_SIISCount	Number of Link Status In Service Signal Units transmitted
LSSU_XMIT_SIPOCount	Number of Link Status Processor Outage Signal Units transmitted
LSSU_XMIT_SIPOECount	Number of Link Status Processor Outage Ended Signal Units transmitted
LSSU_XMIT_SIBCount	Number of Link Status Busy Signal Units transmitted
LSSU_XMIT_SIBECount	Number of Link Status Busy Ended Signal Units transmitted
LSSU_RCV_Count	Total number of Link Status Signal Units received
LSSU_RCV_SIISCount	Number of Link Status In Service Signal Units received
LSSU_RCV_SIPOCount	Number of Link Status Processor Outage Signal Units received
LSSU_RCV_SIPOECount	Number of Link Status Processor Outage Ended Signal Units received
LSSU_RCV_SIBCount	Number of Link Status Busy Signal Units received
LSSU_RCV_SIBECount	Number of Link Status Busy Ended Signal Units received
LSSU_RCV_InvalidCount	Total number of invalid Link Status Signal Units received
BytesTransmitted	Total number of bytes transmitted (MSUs only)
BytesReceived	Total number of bytes received (MSUs only)
Remote_PO_Count	Number of times Remote Processor Outage occurred
Remote_Congestion_Count	Number of times remote congestion occurred
CongestionCount	Number of times peer link went into congestion

Table 49 *show cs7 m2pa statistics Field Descriptions (continued)*

Field	Description
T1_TMO_Count	Number of times link alignment timer expired
T6_TMO_Count	Number of times remote congestion timer expired

Table 50 describes the fields in the **show cs7 m2pa state** display.

Table 50 *show cs7 m2pa state Field Descriptions*

Field	Description
M2PA Peer State	State of the M2PA peer link
SCTP Peer State	State of the associated SCTP peer link
T1 aligned/ready	Current value of the T1 link alignment timer
T6 remote cong	Current value of the T6 remote congestion timer
Local Processor Outage	Current condition of Local Processor Outage
Remote Processor Outage	Current condition of Remote Processor Outage
InService LSSU Recv'd	Indicates whether a Link Status In Service Signal Unit has been received
Transport Handle	Identifier assigned by transport for this peer

Table 51 describes the fields in the **show cs7 m2pa peer** display.

Table 51 *show cs7 m2pa peer Field Descriptions*

Field	Description
Peer Protocol	Transport protocol used by M2PA
Peer Port	Remote peer port number
Peer Address	IP address of remote peer
RTO	Retransmission timeout value for this remote IP address
SRTT	Smoothed Round-Trip-Time for this remote IP address
Primary Peer Address	Primary remote IP address
Effective Peer Address	Effective remote IP address=50.50.50.2
Transport Handle	Identifier assigned by transport layer to identify this peer link
Passive Peer	Indicates whether the remote peer should initiate the connection
M2PA Peer State	State of the M2PA peer link
SCTP Peer State	State of the SCTP peer link
Local Processor Outage	Indicates whether local processor outage condition is present
Remote Processor Outage	Indicates whether remote processor outage condition is present
T1 aligned/ready	T1 link alignment timer timeout
T6 remote cong	T6 remote congestion timer timeout

Table 51 *show cs7 m2pa peer Field Descriptions (continued)*

Field	Description
Local Recv Window	Local receive window size
Remote Recv Window	Remote receive window size
InService LSSU Recv'd	Indicates whether a Link Status In Service Signal Unit has been received
Assoc Retransmission	Maximum number of retransmissions allowed for the association
Peer Init Retransmission	Maximum number of retries allowed for peer initialization packets
Peer Init RTO Max	Maximum retransmission timeout for peer initialization packets
Peer Path Retransmission	Maximum number of retries before the corresponding address is marked inactive
Cumulative Sack Timeout	Cumulative Acknowledgement timer
Bundle Status	Indicates whether bundling is enabled
Bundle Timeout	Maximum amount of time SCTP waits for messages from M2PA for bundling
Minimum RTO	Minimum retransmission timeout
Maximum RTO	Maximum retransmission timeout
IP Precedence	IP precedence bits setting in IP header for this peer
QoS	QoS class
Keep Alive	Indicates whether keepalives are enabled
Keep Alive Timeout	Keepalive timeout value
Initial cwnd	Size in bytes of the SCTP initial congestion <i>window-size</i>
Idle cwnd rate	Rate at which the size of the SCTP congestion window is decreased due to the association being idle
Retrans cwnd rate	Rate at which the size of the SCTP congestion window is decreased due to retransmission timer expiration
Retrans cwnd mode	Congestion window is set for a fast retransmission
FastRetransmit cwnd rate	Rate at which the size of the SCTP congestion window is decreased due to a fast retransmission
Tx Queue Depth	Maximum allowed depth of transmitQ: (used by M2PA to determine txCongestion thresholds)
TxCongestionOnset Level1	M2PA transmit congestion level threshold (value results from configuration of the tx-queue-depth command)
TxCongestionOnset Level2	M2PA transmit congestion level threshold (value results from configuration of the tx-queue-depth command)
TxCongestionOnset Level3	M2PA transmit congestion level threshold (value results from configuration of the tx-queue-depth command)
TxCongestionOnset Level4	M2PA transmit congestion level threshold (value results from configuration of the tx-queue-depth command)

Table 51 *show cs7 m2pa peer Field Descriptions (continued)*

Field	Description
Debug Mask	Mask indicating which levels of M2PA debug are active
Large MSU Supported	Status of large MSU support

[Table 52](#) describes the fields in the **show cs7 m2pa local-peer** display.

Table 52 *show cs7 m2pa local peer Field Descriptions*

Field	Description
Local Port	Value of local port number
Local IP	IP addresses assigned to this local peer
SCTP Instance Handle	Identifier assigned by transport to identify this local peer
Instance Local Recv Window	Current value of local receive window
Instance maxInitRetrans	Default number of retries of initialization packets for peers assigned to this local peer
Instance maxInitTimeout	Default maximum transmission timeout for peer initialization packets for peers assigned to this local peer
Instance Unordered Priority	Indicates the priority by which unordered packets are delivered to MTP3
Instance IP Precedence	IP ToS setting used for peer link initialization packets

show cs7 m3ua

To display M3UA node information, use the **show cs7 m3ua** privileged EXEC command.

show cs7 [*instance-number*] **m3ua** [*local-port* | **bundling-stats** | **queues** | **statistics**]

Syntax Description	<i>instance-number</i>	Specifies the instance. The valid range is 0 to 7. The default instance is 0.
	<i>local-port</i>	M3UA local port number. Range is 1024 to 65535.
	bundling-stats	CS7 M3UA bundling statistics.
	queues	CS7 M3UA queues.
	statistics	CS7 M3UA global statistics.

Defaults The default instance is 0.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples The following example includes output from the **show cs7 m3ua** command.

This M3UA version uses SIGTRAN RFC 3332.

This M3UA instance (local port 7100) is **shutdown**. The instance handle is **inactive**.

This M3UA instance is *not* offloaded to any line card.

```
ITP# show cs7 m3ua 7100
```

```
Sigtran M3UA RFC number: 3332
```

```

M3UA Local port: 7100      State: shutdown      SCTP instance handle: inactive
Local ip address:          172.18.48.123
Number of active M3UA peers:      0
Max number of inbound streams allowed: 17
Local receive window:          64000
Max init retransmissions:      8
Max init timeout:            1000 ms
Unordered priority:          equal
Extended UPU support:        disabled
Offload to FlexWAN:          No      Slot: -1
SCTP defaults for new associations
Transmit queue depth: 1000      Cumulative sack timeout: 200 ms
Assoc retransmissions: 10      Path retransmissions: 4
Minimum RTO: 1000 ms          Maximum RTO: 1000 ms

```

```

Bundle status:          on          Bundle timeout:          5 ms
Keep alive status:      true         Keep alive timeout:      30000 ms
Initial cwnd:           1234567      Idle cwnd rate:          10
Retrans cwnd rate:      60           Retrans cwnd mode:       FastRetrans
FastRetrans cwnd rate:  20

```

Related Commands

Command	Description
cs7 m3ua	Specifies the local port number for M3UA and enters cs7 m3ua submode.
show tech-support	Collects and displays a large amount of ITP configuration information that can be used for troubleshooting.

New counters added to the command output include:

Current transaction error code counter increments with map error codes that correspond to the current transaction with CAR. For example, the error can be due to incorrect MAPUA configuration or inactive linkset/AS.

Unsuccessful decode of access request counter increments when the incoming packet cannot be decoded by ITP. This can happen due to the following reasons:

- Failed sanity check.
- Failed decryption of vendor attributes.
- Mismatch of secret configured at ITP.
- MAPUA Vendor Specific Attribute not present.
- MAPUA message authenticator attribute not present.

Invalid radius packet length counter increments when a RADIUS packet is dropped due to invalid length.

Jaguar# **show cs7 mapua statistics**

```

mapua EAP-SIM-Auth ip 10.78.170.198 port 1645 inQ 0 maxQ 0 rtt 0/0/0 ms
  Client      Port  Request In  Duplicate In  Accept Out  Reject Out
  10.78.164.40 00000      0           0             0           0

```

Current transaction error code : 0

Input requests dropped

Unsuccessful decode of access request: 0

Invalid length of radius packet : 0

show cs7 mated-sg

To display mated-sg information, use the **show cs7 mated-sg** privileged EXEC command.

show cs7 [*instance-number*] **mated-sg** [**all** | **name** *name*] [**detail** | **event-history** | **fsm-history** | **statistics**]

Syntax Description

<i>instance-number</i>	Specifies the instance. The valid range is 0 to 7. The default instance is 0.
detail	Displays the information in detailed format.
statistics	Displays mated-sg statistics.
all	Displays all mated-sgs (the default).
detail	Displays detailed information on mated-sgs.
event-history	Displays mated-sg history.
fsm-history	(Optional) Displays mated-sgs fsm history.
statistics	Displays mated-sgs statistics.

Defaults

The default instance is 0.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.
12.2(18)IXH 12.4(15)SW3 12.2(33)IRC	Enhanced the command output to include the running SGMP version with the detail keyword.
12.2(33)IRD	Added the fsm-history keyword.

Examples

The following example includes output from the **show cs7 mated-sg** command in the default **brief** format:

Options for the SG Mate state include: Inactive/Active/Shutdown

If the Mate is shut down, then the remote port and remote IP address display the configured values instead of the actual values.

ITP# **show cs7 mated-sg**

MATED-SG Name	AS Name	State	Type	Effect Primary	Rmt Port	Remote IP Addr	SCTP
provencl1	provence	active	SGMP	9000	10.74.57.218	0xA0010028	

The following example includes output from the **show cs7 mated-sg** command with the **fsm-history** keyword. The **fsm-history** keyword can display the status change of the status machine:

ITP# **show cs7 mated-sg fsm-history**

```

2008/12/25/10:14:12.239 Mated-sg: matedsg Event: SGMP_as_cfg_done
    FSM STATE: SGMP_idle -> SGMP_ready_to_go
2008/12/25/10:14:22.203 Mated-sg: matedsg Event: SGMP_T1_timer
    FSM STATE: SGMP_ready_to_go -> SGMP_sctp_connecting

```

The following example includes output from the **show cs7 mated-sg** command in **detail** format:

Options for SG Mate state include: Inactive/Active/Shutdown

ITP# **show cs7 mated-sg name provence11 detail**

```

Mated-sg name: provence11                                Type: SGMP
Availability: enabled                                    Mated-sg id: n/a
SCTP association state: established                       Association id: 0xA0010028
Mated-sg FSM state: SGMP_asp_active
AS name: provence                                        Mated-sg state: active
Traffic mode: undefined                                  Active Time: 16:00:35
Configured remote port: 9000                             Actual remote port: 9000
Configured remote ip addresses: 10.74.57.218
Actual remote ip addresses: 10.74.57.218                 State: active (effective prim)
Local port: 9000
Offload to linecard: Yes Slot: 10 0 AspVipId: 301
Mated-sg protocol class capability: n/a
Mated-sg interworking with SS7 networks capability: n/a
Local receive window: 64000                               Cumulative sack timeout: 200 ms
Assoc retrans: 10                                         Path retrans: 4
Max init retrans: 8                                       Max init RTO: 1000 ms
Minimum RTO: 1000 ms                                     Maximum RTO: 1000 ms
Bundle status: on                                         Bundle timeout: 5 ms
Keep alive status: true                                   Keep alive timeout: 500 ms
SCTP congestion level: 0                                  SCON congestion level: 0
Unordered priority: equal                                Transmit queue depth: 1000
Initial cwnd: 3000                                       Idle cwnd rate: 50
Retrans cwnd rate: 50                                    Retrans cwnd mode: RFC
FastRetrans cwnd rate: 50
Thresholds for congestion on transmit queue
  Level 1 onset: 500                                     Level 1 abate: 300
  Level 2 onset: 700                                     Level 2 abate: 500
  Level 3 onset: 900                                     Level 3 abate: 700
  Level 4 onset: 1000                                    Level 4 abate: 900
QOS Class:0 (instance:0)                                IP TOS: 0x0
Match Type: None

```

The following example includes output from the **show cs7 mated-sg** command with the **statistics** keyword:

ITP# **show cs7 mated-sg statistics**

```

Mated-Sg name: bermuda                                    Type: SGMP
Active Time: 2d12h
  Data Packets/MSU Stats
    Inbound Packets Rcvd: 0                               Inbound Octets Rcvd: 0
    Inbound Packets Sent: 0                               Inbound Octets Sent: 0
    Outbound Packets Sent: 0                              Outbound Octets Sent: 0
  Buffer Allocation Stats
    Buffer Alloc Failures: 0                               Buffer Growth Failures: 0
    Buffer Reused: 0
  XUA Error Messages Sent Stats
    ERR Invalid Version: 0                                ERR Inv Network App: 0
    ERR Unsupported Class: 0                              ERR Unsupported Type: 0
    ERR Traffic Mode: 0                                   ERR Unexpected Msg: 0
    ERR Protocol Error: 0                                 ERR Invalid Stream ID: 0
    ERR Refused, Mgmt Block: 0                            ERR Inv Routing Contxt: 0
    ERR Invalid ASP ID: 0

```

```

ERR Invalid Parm Value: 0          ERR Ukwn Routing Contxt:0
      XUA Error Messages Received Stats
ERR Invalid Version: 0          ERR Inv Network App: 0
ERR Unsupported Class: 0        ERR Unsupported Type: 0
ERR Traffic Mode: 0            ERR Unexpected Msg: 0
ERR Protocol Error: 0          ERR Invalid Stream ID: 0
ERR Refused, Mgmt Block: 0
ERR Invalid ASP ID: 0          ERR Inv Routing Contxt: 0
ERR Invalid Parm Value: 0        ERR Ukwn Routing Contxt:0
      Congestion Stats
Pkts Dropped At Lvl 1: 0        Pkts Dropped At Lvl 2: 0
Pkts Dropped At Lvl 3: 0
Level 1 Congestion Cnt: 0      Level 2 Congestion Cnt: 0
Level 3 Congestion Cnt: 0      Level 4 Congestion Cnt: 0
T1 Timeouts: 0                T6 Timeouts: 0

```

Related Commands

Command	Description
cs7 mated-sg	Configures a connection to a mated SG.
show cs7 sgmp	Displays SGMP information.

show cs7 mlr address-table

To display the addresses matched within the MLR address table, use the **show cs7 mlr address-table** privileged EXEC command.

show cs7 [*instance-number*] **mlr address-table** [*name table-name*] | [**prefix** *digits*] | [**addr** *address*]

Syntax Description

<i>instance-number</i>	Specifies the instance. The valid range is 0 to 7. The default instance is 0.
name	Filters on address table name.
<i>table-name</i>	The name associated with the multilayer result table.
prefix	Filters on addresses prefixed with a specified digit string.
<i>digits</i>	Digit string.
addr	Filters on matching addresses.
<i>address</i>	Digit string.

Defaults

The default instance is 0.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Examples

The following example includes output from the **show cs7 mlr address-table** command:

ITP# **show cs7 1 mlr address-table B-ADDRS**

```

-----
Name: B-ADDRS      Instance: 1
Table Lookups: 0
Address            Result Type-Address      Match
-----
09200800           PC   1-1-3                0
09200800*          AS   smsc1                 0
38012650007149     grp  SMSC-GROUP1            0
ABCD*              PC   1-2-3                0
1800*              PC   1-2-3                0
4082                PC   1-2-3                0
1900*              PC   1-2-3                0

```


Related Commands

Command	Description
addr (cs7 mlr address-table)	Specifies an MLR address within the MLR address table.
cs7 mlr address-table	Defines addresses for a CS7 MLR address table.

show cs7 mlr configuration

To display MLR configuration details, use the **show cs7 mlr configuration** privileged EXEC command.

show cs7 mlr configuration [detail]

Syntax Description	detail	Displays address table entries.
Defaults	None.	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples

The following example includes output from the **show cs7 mlr configuration** command:

```
ITP# show cs7 mlr configuration
itpA#sh cs mlr config
Load for five secs: 7%/4%; one minute: 12%; five minutes: 13%
Time source is NTP, 09:48:25.502 EDT Thu Aug 7 2008

cs7 mlr options
preserve-opc
!
cs7 mlr result isup-0 mode wrp
pc 3.3.0 weight 1
!
cs7 mlr address-table srism-dest
timestamp 1218035331
!
cs7 mlr address-table mlrtbl-0
timestamp 1218035331
!
cs7 mlr ruleset gsm protocol gsm-map
rule 10 anyTimeInterr default
result pc 3.4.0
rule 20 sendAuthInfo default
result pc 3.4.0
rule 30 checkIMEI default
result pc 3.4.0
rule 40 restoreData default
result pc 3.4.0
rule 50 sms-mo
dest-smsc 123
result pc 3.4.0
rule 60 sms-mt
dest-sme *
```

```

    result pc 3.4.0
rule 70 sri-sm
    dest-sme-table srism-dest
    result pc 3.4.0
rule 80 sri-call default
    result pc 3.4.0
rule 90 sendParams default
    result pc 3.4.0
rule 100 updLocation default
    result pc 3.4.0
rule 1000 all-operations
    result pc 3.40.0
rule 1500 default-rule
    result pc 3.40.0
!
```

Related Commands

Command	Description
addr (cs7 mlr address-table)	Specifies an MLR address within the MLR address table.
cs7 mlr options	Enables CS7 MLR options configuration mode.
cs7 mlr address-table	Defines addresses for a CS7 MLR address table.
cs7 mlr result	Specifies a multilayer routing ruleset.
cs7 mlr options	Enables CS7 MLR options configuration mode.
insert-dpc-in-cdpa	Inserts a DPC into the CdPA PC for packets routed with MLR.
preserve-opc (cs7 mlr options)	Preserves the original originating point code (OPC) when an MLR is selected.

show cs7 mlr errors

To display information about the errors encountered in MLR packet parsing, use the **show cs7 mlr errors** command in EXEC mode.

show cs7 mlr errors

Syntax Description	None.

Defaults	None.

Command Modes	EXEC

Command History	Release	Modification
	12.4(15)SW8	This command was introduced.
	12.2(33)IRH	

Examples The following example includes output from the **show cs7 mlr errors** command:

```
ITP# show cs7 mlr errors
Instance 0
Unparsed SCCP Message Received: 0
Segmented SCCP message received not supported by MLR: 0
Resume routing due to invalid trigger action: 0
Result group did not have an available server no member available: 0
Result group in dest-sme-binding mode is only valid for sccp msg: 0
Unrecognized TCAP tag: 0
Failed to get mandatory Invoke ID: 0
Failed to get mandatory Linked ID or operation code: 0
OpCode length is not between 1 and 4: 0
Could not get Component Type Tag: 0
Couldn't get SRI SM MSISDN Tag: 0
Couldn't get SRI SM-RP-PRI Tag: 0
Couldn't get SRI SC Addr Tag: 0
Ignore UDH UDHL indicates too few Octets: 0
Len error in SMS-DELIVER: 0
Invalid sm-RP-DA LMSI length: 0
Couldn't get sm-RP-DA LMSI Tag: 0
Invalid sm-RP-OA length: 0
Couldn't get sm-RP-OA Tag: 0
Couldn't get sm-RP-UI Tag: 0
Internal error : unknown mlrType: 0
Couldn't get Dlg/Component Tag: 0
Failed to get mandatory Invoke ID: 0
Couldn't retrieve DTID: 0
ITU_TCAP_ParseDialoguePortion failed with error: 0
Invalid MIN Length: 0
Invalid MDN length: 0
Couldn't get updLoc IMSI Tag: 0
Invalid updLoc IMSI length: 0
```

```
Invalid SMS_DestinationAddress length: 0
Invalid SMS_OriginalDestinationAddress length: 0
Invalid SMS_OriginalDestinationAddress length: 0
Invalid SMS_OriginatingDestinationAddress length: 0
Invalid SMS_OriginalOriginatingAddress length: 0
Invalid SMS_TeleserviceIdentifier length: 0
Couldn't get ssUnstructuredSS_Request: 0
```

Related Commands

Command	Description
—	—

show cs7 mlr options

To display MLR global options information, use the **show cs7 mlr options** privileged EXEC command.

show cs7 mlr options

Syntax Description This command has no arguments or keywords.

Defaults None.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(18)IXG	This command was introduced.
	12.4(15)SW2	
	12.2(33)IRB	

Examples The following example includes output from the **show cs7 mlr options** command:

```
ITP# show cs7 mlr options
CS7 MLR Options:
[cs7 instance 0 mlr options]
preserve-opc
exclude-concatSM-from-multiMsgDialogue
[cs7 instance 1 mlr options]
insert-dpc-in-cdpa
```

Related Commands	Command	Description
	cs7 mlr options	Enables CS7 MLR options configuration mode.
	insert-dpc-in-cdpa	Inserts a DPC into the CdPA PC for packets routed with MLR.
	preserve-opc (cs7 mlr options)	Preserves the original originating point code (OPC) when an MLR is selected.
	exclude-concatSM-from-multiMsgDialogue	Allows SMS-MO messages that are concatenated at the SMS layer to be routed with MLR directly.

show cs7 mlr result

To display multilayer SMS routing result information, use the **show cs7 mlr result** privileged EXEC command.

show cs7 [*instance-number*] **mlr result** *name*

Syntax Description

<i>instance-number</i>	Specifies the instance. The valid range is 0 to 7. The default instance is 0.
<i>name</i>	MLR result group name.

Defaults

The default instance is 0.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Examples

The following example includes output from the **show cs7 mlr result** command:

ITP# **show cs7 mlr result**

Result Group: MLR1 Instance: 0 Unavailable-routing: discard
Protocol: n/a Mode: dest-sme-binding

Order	Result Type	Stat	Weight	Matches
100	PC 5.5.5 ssn 8	avail	20	0
200	PC 5.5.6	avail	40	0
300	AS berm4	avail	15	0
400	PC 5.5.7	avail	60	0

Result Group: MLR3 Instance: 0 Unavailable-routing: discard
Protocol: n/a Mode: wrr

Result Type	Stat	Wgt	UseCnt Remain	Matches
AS berm4	avail	10	10	0
PC 1.2.5	unav	4	4	0
PC 1.2.6 ssn 8	unav	2	2	0
GT 12345 tt 0 gti 4 np 1 nai 4	avail	1	1	0

Related Commands

Command	Description
cs7 mlr result	Specifies a multilayer result table.

show cs7 mlr ruleset

To display multilayer routing (MLR) ruleset information, use the **show cs7 mlr ruleset** privileged EXEC command.

show cs7 [*instance-number*] **mlr ruleset** [**name** *ruleset-name*] [**detail** | **result-summary** | **rule-summary** | **sms-summary**]

Syntax Description

<i>instance-number</i>	Specifies the instance. The valid range is 0 to 7. The default instance is 0.
name	Specifies a ruleset.
<i>ruleset-name</i>	Ruleset name. A valid ruleset name is a character string with a maximum of 12 characters.
detail	Displays details about the MLR ruleset.
result-summary	Displays a summary of results within an MLR table.
rule-summary	Displays a summary of all rules and operations.
sms-summary	Displays a summary of SMS rules within an MLR table.

Defaults

The default instance is 0.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Examples

The following example includes output from the **show cs7 mlr ruleset** command with no keywords. Output for all rulesets is displayed.

```
ITP# show cs7 mlr ruleset
Name: MLR1          Instance:0  Protocol: n/a
Rule Oper  dest-sme      orig-sme      dest-smsc      Matches
---- ----  -
10  sms-mo  -              -              -              0
100 sms-mo  Tbl:MLR1      -              -              0
201 sms-mo  -              -              -              0
1000 all    n/a           n/a           n/a           0

Name: MLR2          Instance:0  Protocol: n/a      Event-trace:disabled
Rule Oper  dest-sme      orig-sme      dest-smsc      Matches
---- ----  -
2   smdpp  -              -              n/a           0
4   sms-mo Tbl:MLR1      -              -              0
7   sms-mo 2323*      -              -              0
9   sms-mo  -              -              -              0
10  sms-mo  -              -              -              0
```



```

Name: MLR3          Instance:0  Protocol: n/a      Event-trace:disabled
Rule Oper   dest-sme          orig-sme          dest-smsc         Matches
-----
10  sms-mo -                  -                  -                  0

```

The following example includes output from the **show cs7 mlr ruleset** command for a specified ruleset:

```

ITP# show cs7 mlr ruleset MLR1
Name: MLR1          Instance:0  Protocol: n/a
Rule Oper   dest-sme          orig-sme          dest-smsc         Matches
-----
10  sms-mo -                  -                  -                  0
100 sms-mo Tbl:MLR1          -                  -                  0
201 sms-mo -                  -                  -                  0
1000 all    n/a              n/a              n/a              0
1100 default-rule

```

The following example includes output from the **show cs7 mlr ruleset** with the **rule-summary** keyword:

```

router# show cs7 mlr ruleset rule-summary
Name: GEN_OPCODE    Instance:0  Protocol: n/a
Rule   Operation    Protocol  Matches  pam
-----
5      sms-mt        gsm-map   0
10     updLocation   gsm-map   0
12     alertSc       gsm-map   0
25     smdpp         ansi-41   0
26     anyTimeSubInterr gsm-map   0
27     all-operations n/a       0
30     default-rule  n/a       0

Name: MLR_RULES     Instance:0  Protocol: n/a
Rule   Operation    Protocol  Matches  pam
-----
4      sms-mo        gsm-map   0
5      sms-mo        gsm-map   0
8      sms-mo        gsm-map   0
10     sms-mo        gsm-map   0
20     sms-mo        gsm-map   0
24     sIWFSSigMod   gsm-map   0
28     networkUSSD   gsm-map   0
43     connectFollowAddress gsm-map   0
44     processUnstructSSData gsm-map   0
45     alertSc       gsm-map   0
50     all-operations n/a       0
55     default-rule  n/a       0

Name: GEN_OPC_GSM   Instance:0  Protocol: gsm-map
Rule   Operation    Protocol  Matches  pam
-----
5      alertSc       gsm-map   0
10     updLocation   gsm-map   0
18     authFailRep   gsm-map   0
20     sri-sm        gsm-map   0
23     updGprsLoc    gsm-map   0
27     sri-gprs      gsm-map   0
100    all-operations gsm-map   0
110    default-rule  n/a       0

Name: DEF           Instance:0  Protocol: n/a
Rule   Operation    Protocol  Matches  pam
-----
10     sms-mo        gsm-map   0

```

■ show cs7 mlr ruleset

```

Name: TRACE          Instance:0  Protocol: n/a      Event-trace:disabled
Rule      Operation    Protocol    Matches    pam
-----
1    updLocation      gsm-map     0
2    alertSc          gsm-map     0
3    invokeSS         gsm-map     0
4    authFailRep      gsm-map     0
5    sendInfoForOutgCall gsm-map     0
8    sri-sm           gsm-map     0
9    sIWFSSigMod      gsm-map     0
10   repSmDeliveryStatus gsm-map     0

```

```

Name: MLR_RULE_TST   Instance:0  Protocol: n/a
Rule      Operation    Protocol    Matches    pam
-----
10   smdpp            ansi-41     0

```

```

Name: GEN_OPC_SM     Instance:0  Protocol: n/a
Rule      Operation    Protocol    Matches    pam
-----
102  all-operations    n/a         0

```

```

Name: MLRRULESET4    Instance:4  Protocol: n/a
Rule      Operation    Protocol    Matches    pam
-----
20   updLocation      gsm-map     0
30   smdpp            ansi-41     0
40   all-operations    n/a         0
50   default-rule      n/a         0

```

```

Name: MLR_GSM_4      Instance:4  Protocol: gsm-map
Rule      Operation    Protocol    Matches    pam
-----
10   updLocation      gsm-map     0
19   allocHandOverNum gsm-map     0
20   all-operations    gsm-map     0
30   default-rule      n/a         0

```

The following example includes partial output from the **show cs7 mlr ruleset** command with the keywords **rule-summary gsm-map operation updLocation**. The output displays rules with the **updLocation** operation.

```
router# show cs7 mlr ruleset rule-summary gsm-map operation updLocation
```

```

Name: GEN_OPCODE     Instance:0  Protocol: n/a
Rule      Operation    Protocol    Matches    pam
-----
10   updLocation      gsm-map     0
27   all-operations    n/a         0
30   default-rule      n/a         0

```

```

Name: MLR_RULES       Instance:0  Protocol: n/a
Rule      Operation    Protocol    Matches    pam
-----
50   all-operations    n/a         0
60   default-rule      n/a         0

```

```

Name: GEN_OPC_GSM    Instance:0  Protocol: gsm-map
Rule      Operation    Protocol    Matches    pam
-----
10   updLocation      gsm-map     0
100  all-operations    gsm-map     0
110  default-rule      n/a         0

```

The following example includes partial output from the **show cs7 mlr ruleset** command with the keywords **rule-summary gsm-map operation mobileussd**. The output displays rules with the mobileUSSD operation.

```
router# show cs7 mlr ruleset rule-summary gsm-map operation mobileussd
```

```
Name: GEN_OPCODE      Instance:0  Protocol: n/a
Rule      Operation      Protocol  Matches  pam
-----
5      sms-mt      gsm-map      0
10     updLocation  gsm-map      0
12     alertSc     gsm-map      0
26     anyTimeSubInterr  gsm-map      0
27     all-operations  n/a          0
30     default-rule  n/a          0
```

```
Name: MLR_RULES      Instance:0  Protocol: n/a
Rule      Operation      Protocol  Matches  pam
-----
4      sms-mo      gsm-map      0
5      sms-mo      gsm-map      0
8      sms-mo      gsm-map      0
10     sms-mo      gsm-map      0
20     sms-mo      gsm-map      0
24     sIWFSSigMod  gsm-map      0
28     networkUSSD  gsm-map      0
43     connectFollowAddress  gsm-map      0
44     processUnstructSSData  gsm-map      0
45     alertSc     gsm-map      0
50     all-operations  n/a          0
55     default-rule  n/a          0
```

```
Name: GEN_OPC_GSM    Instance:0  Protocol: gsm-map
Rule      Operation      Protocol  Matches  pam
-----
5      alertSc     gsm-map      0
10     updLocation  gsm-map      0
18     authFailRep  gsm-map      0
20     sri-sm      gsm-map      0
23     updGprsLoc  gsm-map      0
27     sri-gprs    gsm-map      0
100    all-operations  gsm-map      0
110    default-rule  n/a          0
```

```
Name: DEF            Instance:0  Protocol: n/a
Rule      Operation      Protocol  Matches  pam
-----
10     sms-mo      gsm-map      0
```

```
Name: TRACE          Instance:0  Protocol: n/a      Event-trace:disabled
Rule      Operation      Protocol  Matches  pam
-----
1      updLocation  gsm-map      0
2      alertSc     gsm-map      0
3      invokeSS    gsm-map      0
4      authFailRep  gsm-map      0
5      sendInfoForOutgCall  gsm-map      0
8      sri-sm      gsm-map      0
9      sIWFSSigMod  gsm-map      0
10     repSmDeliveryStatus  gsm-map      0
```

```
Name: MLR_RULE_TST   Instance:0  Protocol: n/a
Rule      Operation      Protocol  Matches  pam
-----
```

show cs7 mlr ruleset

```

Name: GEN_OPC_SM      Instance:0  Protocol: n/a
Rule      Operation      Protocol  Matches  pam
-----
102  all-operations      n/a      0
105  default-rule        n/a      0

```

```

Name: MLRRULESET4     Instance:4  Protocol: n/a
Rule      Operation      Protocol  Matches  pam
-----
20   updLocation         gsm-map   0
40   all-operations      n/a      0
50   default-rule        n/a      0

```

```

Name: MLR_GSM_4       Instance:4  Protocol: gsm-map
Rule      Operation      Protocol  Matches  pam
-----
10   updLocation         gsm-map   0
19   allocHandOverNum    gsm-map   0
20   all-operations      gsm-map   0
30   default-rule        n/a      0

```

router# **show cs7 mlr ruleset detail**

```

Name: test           Instance:4  Protocol: n/a
-----
Rule      : 1          Protocol: gsm-map          Matches: 0
Operation : processUnstructSSReq
Parameters:
  Map version : 2
Result    : GRP abc

Rule      : 3          Protocol: n/a              Matches: 0
Operation : all-operations
  Allow-multi-message-dialogue
Result    : BLOCK

Rule      : 10         Protocol: n/a              Matches: 0
Operation : default-rule
Result    : CONTINUE

```

router# **show cs7 mlr ruleset result-summary**

```

Name: test           Instance:4  Protocol: n/a
Rule Operation      Result Type-Address Matches
-----
1   processUnstructSSReq  GRP abc      0
3   all-operations      BLOCK        0
10  default-rule        CONTINUE     0

```

router# **show cs7 mlr ruleset result-summary default-rule**

```

Name: rle_chl_sh     Instance:0  Protocol: n/a
Rule Operation      Result Type-Address Matches
-----
10  default-rule      CONTINUE     0

```

router# **show cs7 mlr ruleset rule-summary default-rule**

```

Name: rle_chl_sh     Instance:0  Protocol: n/a
Rule Operation      Protocol  Matches  pam
-----
10  default-rule     n/a      0

```

The file format for MLR is modified to show the default-rule when configured in the MLR.

```
ITP_251# cs7 4 save mlr disk1:mlr.sil
ITP_251# more disk1:mlr.sil
```

```
mlr 2 3 ITU 4 globe0
!
cs7 instance 4 mlr result abc mode wrp
  congestion-mode defer-to-backup
  pc 5-100-250 weight 1
  pc 5-100-253 weight 1
!
cs7 instance 4 mlr ruleset test
  rule 1 gsm-map processUnstructSSReq
    map-version 2
    result group abc
  rule 3 all-operations
    allow-multi-message-dialogue
    result block
  rule 10 default-rule
    result continue
!
!end
!
```

Related Commands

Command	Description
cs7 mlr result	Specifies a multilayer routing ruleset.

show cs7 mlr statistics

To display global MLR statistics, use the **show cs7 mlr statistics** privileged EXEC command.

show cs7 [*instance-number*] **mlr statistics** [*operations*]

Syntax Description	<i>instance-number</i>	Specifies the instance. The valid range is 0 to 7. The default instance is 0.
	operations	Displays the number of times each MAP operation was received.

Defaults	The default instance is 0.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples The following example includes output from the **show cs7 mlr statistics** command:

```
ITP# show cs7 mlr statistics
CS7 Multi-Layer Routing Statistics

Instance: 0
Total packets processed by MLR:                4977673
  Packets routed by MLR:                        871
  Packets returned to SCCP:                     4976802
  Packets MLR failed/aborted:                   0

Trigger matches
  Successful trigger matches:                   4625798
    Successful rule matches:                    872
    Blocking rule matches:                     0
    Continue rule matches:                     0
  Blocking trigger matches:                     0
  Continue trigger matches:                     0
  Result trigger matches:                      934

MLR Packets successfully parsed by operation
  GSM-MAP SMS-MO operations:                   240051
  GSM-MAP SMS-MT operations:                    0
  GSM-MAP SRI-SM operations:                    0
  GSM-MAP AlertSC operations:                   141
  ANSI-41 SMDPP operations:                    53071
  ANSI-41 SMSRequest operations:                 0
  ANSI-41 SMSNotification operations:           81509

MLR multi-message-dialogue packets successfully parsed
  Segmented Begin without component:            3545
  Begin with MMS:                               0
  Segmented Continue:                           3545
```

```

Concatenated messages:                                8920

MLR Packets routed by MLR:
  Result action AS:                                    583
  Result action GTT:                                    288
    Rewrite packet with ri=gt for result GT:           0
  Result action PC:                                    0
  Result action PC+SSN:                                0
  Failed to insert data into MSU:                       0

MLR Packets returned to SCCP:
  Unsupported SCCP message type:                        3004
  Unsupported segmented SCCP message:                   0
  Trigger action continue:                              0
  Unsupported messages:                                4251025
  Parsing error:                                        1
  Failed to match rule:                                373900
  Result action continue:                              0
  Result action route:                                 0
  No available result group member:                    1
  Failed to modify MSU:                                0
  Failed to match trigger:                             348871

MLR Packets failed or aborted:
  Unparsed SCCP message:                               0
  Result block:                                         0
  Destination unavailable                              0
  No available result group member:                    0

MLR Packets which failed modifications:                 0
  Unable to modify MAP address:                        0
  Unable to modify SCCP address:                       0
  Unable to rewrite packet with ri=gt for result GT:    0
  Unable to convert GTA address:                       0

```

The following example includes output from the **show cs7 mlr statistics** command with the **operations** keyword:

```

ITP# show cs7 mlr statistics operations
CS7 Multi-Layer Routing Statistics for instance 0

```

```

MLR Packets successfully parsed by operation
GSM-MAP sms-mo operations : 0
GSM-MAP sms-mt operations : 0
GSM-MAP sri-sm operations : 0
GSM-MAP alertSc operations : 0
GSM-MAP updLocation operations : 0
GSM-MAP cancelLocation operations : 0
GSM-MAP sendEndSig operations : 0
GSM-MAP processAccessSig operations : 0
GSM-MAP fwdAccessSig operations : 0
GSM-MAP checkIMEI operations : 0
GSM-MAP insSubData operations : 2
GSM-MAP delSubData operations : 0
GSM-MAP reset operations : 0
GSM-MAP fwdCheckSsInd operations : 0
GSM-MAP actTraceMode operations : 0
GSM-MAP deactTraceMode operations : 0
GSM-MAP sri-call operations : 0
GSM-MAP provideRoamNumber operations : 0
GSM-MAP regSS operations : 0
GSM-MAP eraseSS operations : 0
GSM-MAP actSS operations : 0

```

show cs7 mlr statistics

GSM-MAP	deactSS	operations :	0
GSM-MAP	interrSS	operations :	0
GSM-MAP	regPwd	operations :	0
GSM-MAP	getPwd	operations :	0
GSM-MAP	authFailRep	operations :	0
GSM-MAP	anyTimeMod	operations :	0
GSM-MAP	anyTimeSubInterr	operations :	0
GSM-MAP	resumeCallHandling	operations :	0
GSM-MAP	provideSIWFSNumber	operations :	0
GSM-MAP	siWFSSigMod	operations :	0
GSM-MAP	setRepState	operations :	0
GSM-MAP	statusRep	operations :	0
GSM-MAP	remoteUserFree	operations :	0
GSM-MAP	istAlert	operations :	0
GSM-MAP	istCmd	operations :	0
GSM-MAP	regCCEntry	operations :	0
GSM-MAP	eraseCCEntry	operations :	0
GSM-MAP	provideSubInfo	operations :	0
GSM-MAP	provideSubLoc	operations :	0
GSM-MAP	subLocRep	operations :	0
GSM-MAP	anyTimeInterr	operations :	0
GSM-MAP	ssInvocNot	operations :	0
GSM-MAP	prepGrpCall	operations :	0
GSM-MAP	sendGrpCallEndSig	operations :	0
GSM-MAP	processGrpCallSig	operations :	0
GSM-MAP	fwdGrpCallSig	operations :	0
GSM-MAP	updGprsLoc	operations :	0
GSM-MAP	sri-gprs	operations :	0
GSM-MAP	sri-lcs	operations :	0
GSM-MAP	failRep	operations :	0
GSM-MAP	noteMSPresentForGprs	operations :	0
GSM-MAP	noteSubDataMod	operations :	0
GSM-MAP	secureTransClass1	operations :	0
GSM-MAP	secureTransClass2	operations :	0
GSM-MAP	secureTransClass3	operations :	0
GSM-MAP	secureTransClass4	operations :	0
GSM-MAP	noteMMEEvent	operations :	0
GSM-MAP	purgeMS	operations :	0
GSM-MAP	sendId	operations :	0
GSM-MAP	prepHandover	operations :	0
GSM-MAP	prepSubsHandover	operations :	0
GSM-MAP	sendAuthInfo	operations :	0
GSM-MAP	restoreData	operations :	0
GSM-MAP	sendIMSI	operations :	0
GSM-MAP	processUnstructSSReq	operations :	0
GSM-MAP	networkUSSD	operations :	0
GSM-MAP	repSmDeliveryStatus	operations :	0
GSM-MAP	informSC	operations :	0
GSM-MAP	readyForSM	operations :	0
GSM-MAP	allocHandOverNum	operations :	0
GSM-MAP	sendHandOverRep	operations :	0
GSM-MAP	sendParams	operations :	0
GSM-MAP	setCipherMode	operations :	0
GSM-MAP	provideIMSI	operations :	0
GSM-MAP	invokeSS	operations :	0
GSM-MAP	setMsgWaitData	operations :	0
GSM-MAP	page	operations :	0
GSM-MAP	searchForMobileSub	operations :	0
GSM-MAP	sendInfoForIncCall	operations :	0
GSM-MAP	sendInfoForOutgCall	operations :	0
GSM-MAP	completeCall	operations :	0
GSM-MAP	connectFollowAddress	operations :	0
GSM-MAP	noteMSPresent	operations :	0
GSM-MAP	noteIntHandOver	operations :	0


```

GSM-MAP fwdNewTMSI operations : 0
GSM-MAP regChargingInfo operations : 0
GSM-MAP processUnstructSSData operations : 0
GSM-MAP beginSubActivity operations : 0
GSM-MAP authenticate operations : 0
GSM-MAP performHandover operations : 0
GSM-MAP performSubHandOver operations : 0
GSM-MAP traceSubAct operations : 0
GSM-MAP processAccessReq operations : 0
GSM-MAP updLocArea operations : 0
GSM-MAP detachIMSI operations : 0
GSM-MAP attachIMSI operations : 0
GSM-MAP fwdSSNot operations : 0
GSM-MAP mobileUSSD operations : 0
GSM-MAP processCallWait operations : 0
ANSI-41 smdpp operations : 0
ANSI-41 smsReq operations : 0
ANSI-41 smsNot operations : 0
Shared opcodes with UNKNOWN MAP version : 0

```

Shared opcodes with UNKNOWN MAP version show the number of times a CONTINUE is received with no dialog and, therefore, no MAP version. The CONTINUE includes a component portion with the opcode value that is shared between different MAP versions.

If a CONTINUE is received with no dialog portion, no MAP version, and the component portion has a shared opcode value, the rule match algorithm looks for matching both operations in v1 and v1+. In the case where two rules are defined for these operations and both match, then the rule with the lesser order is considered the best match.

Table 53 describes the significant fields shown in the display.

Table 53 *show cs7 mlr statistics Field Descriptions*

Field	Description
Instance	ITP instance for these MLR statistics
Total packets processed by MLR:	Total number of packets processed by MLR
Packets routed by MLR:	Number of packets routed by MLR
Packets returned to SCCP:	Number of packets returned to the SCCP layer for normal processing
Packets MLR failed or aborted:	Number of packets dropped by MLR
Trigger Matches	
Successful trigger matches:	Number of packets that matched one or more MLR triggers
Successful rule matches:	Number of packets that matched a rule
Blocking rule matches:	Number of packets that matched a rule that specifies the result block (drop the packet)
Continue rule matches:	Number of packets that matched a rule that specifies the result continue (route the message as received)
Blocking trigger matches:	Number of packets that match a trigger that specifies the trigger action block (drop the packet)
Continue trigger matches:	Number of packets that match a trigger that specifies the trigger action continue (route the message as received)
Result trigger matches	Total number of trigger matches with a result trigger action

Table 53 *show cs7 mlr statistics Field Descriptions (continued)*

Field	Description
MLR Packets successfully parsed by operation	
GSM-MAP SMS-MO operations:	Number of MAP-MO-FORWARD-SM (SMS Mobile Originated) operations
GSM-MAP SMS-MT operations:	Number of MAP-MT-FORWARD-SM (SMS Mobile Terminated) operations
GSM-MAP SRI-SM operations:	Number of SEND-ROUTING-INFO-FOR-SM operations
GSM-MAP AlertSC operations:	Number of MAP-ALERT-SERVICE-CENTER operations
ANSI-41 SMDPP operations:	Number of Short Message Delivery Point-to-Point operations
ANSI-41 SMSRequest operations:	Number of SMSRequest operations
ANSI-41 SMSNotification operations:	Number of SMSNotification operations
MLR multi-message-dialogue packets successfully parsed	Multi-message-dialogue packets are segmented TCAP messages and concatenated SMS messages that span more than 1 packet. MLR processes multi-message-dialogues for sms-mo and sms-mt operations. Multi-message-dialogues include TCAP BEGIN messages that have no component, TCAP CONTINUE messages, TCAP BEGIN or CONTINUE messages containing an INVOKE component with the More-Messages-to-Send indicator (sms-mt only), and messages that are concatenated at the SMS layer.
Segmented Begin without component:	Number of packets processed with a TCAP BEGIN message containing no components
Begin with MMS:	Number of packets processed with a TCAP BEGIN message containing an INVOKE component with the More-Messages-To-Send indicator (sms-mt only)
Segmented Continue:	Number of packets processed with a TCAP CONTINUE message (including sms-mt messages with MMS)
Concatenated messages:	Number of packets processed that are concatenated at the SMS layer. (This count is not mutually exclusive with the counts described above. A packet may be a segmented TCAP CONTINUE message and concatenated at the SMS layer.)
MLR Packets routed by MLR	
Result action AS:	Number of packets that matched a trigger and were processed by a rule that specified a result to route the message to a particular destination M3UA or SUA application server
Result action GTT:	Number of packets that matched a trigger and were processed by a rule that specified a result to route the message using an SCCP global title
Rewrite packet with ri=gt for result GT:	Number of packets matching a result GTT that required a packet rewrite to include the new GT information
Result action PC:	Number of packets that matched a trigger and were processed by a rule that specified a result to route the message using the specified destination point code (pc dpc)
Result action PC+SSN	Number of packets that matched a trigger and were processed by a rule that specified a result to route the message using the specified destination point code and subsystem number (pc dpc ssn ssn)
Failed to insert data into MSU	Number of times that data could not be inserted into a packet routed by MLR

Table 53 *show cs7 mlr statistics Field Descriptions (continued)*

Field	Description
MLR Packets returned to SCCP	
Unsupported SCCP message type:	Number of packets of unsupported SCCP message type (not UDT or XUDT)
Unsupported segmented SCCP message:	Number of unsupported segmented SCCP messages (XUDT with segmentation)
Trigger action continue:	Number of packets that matched a trigger that specifies the trigger action continue (route the message as received)
Unsupported messages:	Number of packets that MLR was unable to parse due to unsupported TCAP message type, unsupported MAP operation, and so on
Parsing error:	Number of packets that MLR was unable to parse due to malformed packet
Failed to match rule:	Number of packets that failed to match any rule
Result action continue:	Number of packets that match a rule that specifies the rule action continue (route the message as received)
Result action route:	Indicates the total number of MLR packets that select a result route specified on a rule result . These modified packets continue with their original routing.
No available result group member:	Number of packets returned to SCCP due to no available result group members. Packets are returned to SCCP for routing when no member of a result group is available to route the packet and the unavailable-routing result option is enabled in the cs7 mlr result configuration command.
Failed to modify MSU:	Indicates the total number of MSUs that failed MLR modification while modify-failure is configured as resume or sccp-error . MLR modification failures include exceeding the maximum MSU or address size when inserting new data, failures when attempting to modify the destination GT, and failures when executing a modify-profile.
Failed to match trigger:	Number of packets that did not match a trigger
MLR Packets failed or aborted	
Unparsed SCCP message:	Number of unparsed SCCP messages that MLR received and dropped
Result block:	Number of packets that match a trigger or a rule that specifies the action block (drop the packet)
Destination unavailable	Number of packets that MLR failed to route to an SCCP destination due to an unavailable destination
No available result group member:	Number of packets failed or aborted due to no available result group members. Packets are discarded when no member of a result group is available to route the packet and the unavailable-routing discard option (default) is enabled in the cs7 mlr result configuration command.
Failed to modify MSU:	Indicates the total number of MSUs that failed MLR modification while modify-failure is configured as discard (default). MLR modification failures include exceeding the maximum MSU or address size when inserting new data, failures when attempting to modify the destination GT, and failures when executing a modify-profile.

Table 53 *show cs7 mlr statistics Field Descriptions (continued)*

Field	Description
MLR Packets that failed modifications	
Unable to modify MAP address:	Indicates the total number of MSUs that failed to modify a MAP address
Unable to modify SCCP address:	Indicates the total number of MSUs that failed to modify SCCP addresses (CgPA or CdPA):
Unable to rewrite packet with ri=gt for result GT: 0	This existing statistic was moved to this new category. It indicates the total number of MSUs that failed to modify the CdPA with a GT result. In these cases, the packets were being modified from CdPA ri=ssn to CdPA ri=gt.
Unable to convert GTA address: 0	This existing statistic was moved to this new category. It indicates the total number of MSUs that failed to modify the CdPA GTA.

Related Commands	Command	Description
	rule (cs7 mlr ruleset)	Specifies the rules for a routing trigger within a multilayer ruleset table.

show cs7 mlr table

To display multilayer SMS routing information, use the **show cs7 mlr table** privileged EXEC command. The default display is rule-summary.

show cs7 [*instance-number*] **mlr table** *name* [**detail** | **result-summary** | **rule-summary** | **sms-summary**]

Syntax Description	
<i>instance-number</i>	Displays output for a specified instance. Valid range is 0 to 7.
<i>name</i>	The name of the CS7 MLR table.
detail	Displays the parameters and results associated with each routing trigger.
result-summary	Displays the result parameters associated with a particular rule along with the number of times the rule has been matched for the given trigger.
rule-summary	Displays the rule parameters associated with a particular rule along with the number of times the rule has been matched for the given trigger.
sms-summary	Displays a summary of SMS rules within an MLR table.

Defaults The default display is rule-summary.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples The following example includes output from the **show cs7 mlr table** command:

```
ITP# show cs7 mlr table MLR
Name: MLR Instance: 0
-----
Rule      Operation      Protocol      Matches
-----
5      alertSc      gsm-map      0
10     updLocation  gsm-map      0
18     authFailRep  gsm-map      0
20     sri-sm       gsm-map      0
23     updGprsLoc   gsm-map      0
27     sri-gprs     gsm-map      0
100    all-operations gsm-map      0
-----
Primary Trigger: MTP3 dpc 4.2.2
Ruleset: GEN_OPCODE Protocol: n/a Trigger Matches: 0
Rule      Operation      Protocol      Matches
-----
5      sms-mt      gsm-map      0
10     updLocation  gsm-map      0
```

show cs7 mlr table

```

12  alertSc          gsm-map          0
25  smdpp            ansi-41          0
26  anyTimeSubInterr gsm-map          0
27  all-operations   n/a             0

```

```

-----
Primary Trigger: default
Ruleset: GEN_OPC_GSM      Protocol: gsm-map      Trigger Matches: 0
Rule      Operation      Protocol      Matches
-----
5    alertSc          gsm-map          0
10   updLocation      gsm-map          0
18   authFailRep      gsm-map          0
20   sri-sm           gsm-map          0
23   updGprsLoc       gsm-map          0
27   sri-gprs         gsm-map          0
100  all-operations   gsm-map          0

```

ITP# **show cs7 1 mlr table sms-router**

Name: sms-router Instance: 1

```

-----
Primary Trigger: MTP3 dpc 1-1-1 opc n/a si 3
Ruleset: sms_rules      Trigger Matches: 0
Rule Oper  dest-sme      orig-sme      dest-smsc      Match
-----
5    smsreq  60920080      n/a           n/a            0
7    smsreq  609200800*    n/a           n/a            0
10   smdpp   38012650007149 4091254283    n/a            0
11   smdpp   *              *             ABCD           0
12   smdpp   1800*          *             *              0
13   smdpp   4082*          *             n/a            0
14   smdpp   *              1900          n/a            0
16   smdpp   *              *             n/a            0
20   smdpp   *              *             *              0
25   smdpp   SME-ADDRS      *             n/a            0
28   smsreq  *              n/a           n/a            0
30   deflt   n/a            n/a           n/a            0

```

ITP# **show cs7 mlr table SMS-WEIGHTED detail**

Name: SMS-WEIGHTED

Trigger: MTP3 DPC: 1-1-1 OPC: N/A SI: 3

Rule: 1 Matches: 5

Operation: smdpp

Protocol: IS-41

Parameters:

Dest-SME: Address-Table SME-ADDRS Orig-SME: 60920025

Dest-SMSC: * PID: *

Result:

GT Selector: E.164 (default) Digits: 9991117777

```

-----
Rule: 2      Matches: 2

```

Operation: sms-mo

Protocol: GSM MAP

Parameters:

Dest-SME: 60920080 Orig-SME: *

Dest-SMSC: * PID: *

Result:

GT Selector: e164 Digits: 9991117778

```

-----
Rule: 3      Matches: 10

```

Operation: sms-mo

Protocol: IS-41

```

Parameters:
  Dest-SME:  6092*      Orig-SME:  *
  Dest-SMSC:  *          PID:      *
Result:
  Dest PC:  3.3.3
-----
Routing Trigger: 4      Matches:  0
Operation:  sms-mo
Protocol:  IS-41
Parameters:
  Dest-SME:  *          Orig-SME:  *
  Dest-SMSC:  *          PID       *
Result:
  GT Selector:  E.164 (default)  Digits: 9991117779

```

Table 54 describes the fields in the display.

Table 54 *show cs7 mlr table Field Descriptions*

Field	Description
Name	Name of the CS7 MLR table.
Protocol	Name of the protocol.
Primary Trigger	SS7 network layer routing parameters that constitute the routing key, or trigger, used to identify traffic requiring parsing into the application layers.
Ruleset	Name of the ruleset used to process matching triggers.
Matches	Total number of matches.
Rule	The order in which the rules in the ruleset are searched.
Operation	GSM MAP operation code. The operation name represents a multilayer routing feature that may comprise one or more actual MAP operations. In the current release, sms-mo is the only valid choice for this parameter. sms-mo identifies SMS MO request messages for the table-appropriate protocol. This operation is valid for the GSM MAP, and matches all BEGIN requests containing an SMS-MO INVOKE component.
Dest-SME	Address of the destination short message entity (SME) within an SMS operation.
Orig-SME	Address of the origin SME within an SMS operation.
Dest SMSC	Address of the destination service center address within an SMS operation.
PID	Protocol identifier value for an SMS-MO rule.
Result	Specifies the processing performed on a matching packet.

Related Commands

Command	Description
cs7 mlr table	Specifies the name of the multilayer SMS routing table.

show cs7 msu-rates

To display information about SS7 MSU rates on a Cisco ITP platform, use the **show cs7 msu-rates** privileged EXEC command.

```
show cs7 msu-rates { configuration [slot] | current [slot] | distribution { msu [slot] | percentage [slot] | history [slot] }
```

Syntax Description

configuration	Displays parameter information for the MSU rates.
current	Displays the current MSU rates.
distribution	Displays the numbers of seconds within a certain percentage range or MSU range configuration.
<i>slot</i>	(Optional) Specifies the slot that contains the processor (0 to 19).
msu	Number of seconds with a certain MSU range.
percentage	Number of seconds with certain percentage.
history	Shows MSU rates history in graph format.

Defaults

None.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

Each ITP platform is rated to process a certain number of message signal units (MSUs) per second for each processor. Many high-level protocols require several MSUs per transaction. Traffic capacity planning is based on MSU rates, not on transactions. Consequently, when high CPU usage problems occur, it can be difficult to determine if the cause is directly related to high MSU rates.

The **cs7 msu-rates** commands enable the configuration, collection, and analysis of MSU rates per processor for all of the ITP platforms.

The **show cs7 msu-rates** commands display information about the configured MSU rate parameters.

Examples

The examples in this section are intended only to describe the command parameters and the fields in the output display. They do not represent recommended configurations.

The following example includes output from the **show cs7 msu-rates** command with the **configuration** keyword. Notice that the Slot and Bay field values in the output are 0, indicating a single-processor platform.

```
ITP# show cs7 msu-rates configuration
```



```

Sample Interval:                3
Notification Interval:          60
Notification Enabled:           TRUE
Global Acceptable Threshold:    100
Global Warning Threshold:       200
Global Overloaded Threshold:    300

```

```

          Acceptable Warning  Overloaded
Slot Bay Threshold Threshold Threshold
-----
    0   0         100         150         200

```

Table 55 describes the fields displayed in the **show cs7 msu-rates configuration** output.

Table 55 *show cs7 msu-rates configuration Field Descriptions*

Field	Description
Slot	Specifies the slot that contains the processor. Applies only to those ITP platforms that support multiple processors.
Bay	Specifies the bay that contains the processor. Applies only to those ITP platforms that support multiple processors.
Sample Interval	Configured interval, in seconds, over which MSU rates were calculated.
Notification Interval	Configured interval, in seconds, used to prevent excessive generation of notifications.
Notification Enabled	TRUE if enabled, FALSE if not enabled.
Acceptable Threshold	Configured rate of traffic, in MSUs per second. Traffic <i>at or below</i> this rate is acceptable.
Warning Threshold	Configured rate of traffic, in MSUs per second. Traffic <i>at or above</i> this rate and <i>below</i> the overload rate indicates a rate of traffic that may impact the device.
Overloaded Threshold	Configured rate of traffic, in MSUs per second. Traffic <i>at or above</i> this rate indicates a rate of traffic that impacts operation of the device.

The following example includes output from the **show cs7 msu-rates** command with the **current** keyword:

```

ITP# show cs7 msu-rates current
Slot Bay rx/tx  Rate  Size Max  Timestamp
-----
    1   0 receive    0   12   116 2006/06/01/14:05:15.878
    1   0  sent     0   12   116 2006/06/01/14:05:15.878
    3   0 receive    0    0    0 1900/01/01/00:00:00.000
    3   0  sent     0    0    0 1900/01/01/00:00:00.000
    6   0 receive    0   12    1 2001/12/22/18:42:33.647
    6   0  sent     0   10    1 2001/12/22/18:42:33.647
   10   0 receive    0   12  123 2006/06/01/14:05:16.090
   10   0  sent     0   12  123 2006/06/01/14:05:16.090

```

Table 56 describes the fields displayed in the **show cs7 msu-rates current** output.

Table 56 *show cs7 msu-rates current Field Descriptions*

Field	Description
Slot	Specifies the slot that contains the processor. Applies only to those ITP platforms that support multiple processors.
Bay	Specifies the bay that contains the processor. Applies only to those ITP platforms that support multiple processors.
rx/tx	Transmitted/Received MSUs.
Rate	Current rate of MSUs per second.
Size	Average size of MSU over last interval.
Max	Maximum rate of MSUs per second since last clear command.
Timestamp	Time and date when maximum rate of MSUs per second occurred.

The following example includes output from the **show cs7 msu-rates** command with the **distribution** keyword:

```
ITP# show cs7 msu-rates distribution 6
Slot Bay Percent RX-Seconds TX-Seconds
-----
  6  0  >=090           0           0
  6  0  080-089           0           0
  6  0  070-079           0           0
  6  0  060-069          114          114
  6  0  050-059           0           0
  6  0  040-049           6           6
  6  0  030-039           0           0
  6  0  020-029           3           3
  6  0  010-019           3           3
  6  0  000-009        320631        320631
```

[Table 57](#) describes the fields displayed in the **show cs7 msu-rates distribution** output.

Table 57 *cs7 msu-rates distribution Field Descriptions*

Field	Description
Slot	Slot that contains the processor on this ITP platform.
Bay	Bay that contains the processor (applies only to a FlexWAN device in the Cisco 7600 series platform; 0 indicates this field is not applicable for this platform).
RX-Seconds	Number of seconds that the receive MSU rate for this processor was within the specified range.
TX-Seconds	Number of seconds that the transmit MSU rate for this processor was within the specified range.

Related Commands

Command	Description
cs7 msu-rates notification-interval	Configures the notification interval, in seconds, used to prevent excessive generation of notifications.
cs7 msu-rates sample-interval	Configures the sample interval, in seconds, over which MSU rates are calculated.
cs7 msu-rates threshold-default	Configures the global MSU rate threshold ranges and defaults for all processors in the ITP platform.
cs7 msu-rates threshold-proc	Configures MSU rate threshold ranges for a specific processor, overriding the global thresholds.

show cs7 mtp2

To display current modify-profiles and their statistics, use the **show cs7 mtp2** privileged EXEC command.

show cs7 mtp2 [**congestion** | **state** | **statistics** | **timers** | **variant**] *serial interface*

Syntax Description

congestion	MTP2 congestion status.
state	MTP2 state machine status.
statistics	MTP2 link statistics.
timers	MTP2 timer values.
variant	MTP2 protocol variant.
serial interface	Serial interface number.

Defaults

None.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Examples

This section includes samples of output from the **show cs7 mtp2** command using the keywords **congestion**, **state**, **statistics**, **timers**, and **variant**.

The following example includes output from the **show cs7 mtp2** command using the **congestion** keyword:

```
ITP# show cs7 mtp2 congestion serial0/1/0:0
CS7 MTP2 congestion status for interface Serial0/1/0:0
Protocol version for interface Serial0/1/0:0 is ITU-T Q.703 (1996) (White Book)
```

```
Layer3 congestion status      = Abate

CongestionRxInd              = Abate
CongestionTxInd              = Abate (Level0)

CongestionTxOnset Level1     = 250 ( 50% of xmitQ maxDepth)
CongestionTxOnset Level2     = 350 ( 70% of xmitQ maxDepth)
CongestionTxOnset Level3     = 450 ( 90% of xmitQ maxDepth)
CongestionTxOnset Level4     = 500 (100% of xmitQ maxDepth)

XmitQ depth (max-used)       = 1
XmitQ depth (max-allowed)    = 500
```

[Table 58](#) describes the fields in the display.

Table 58 **show cs7 mtp2 congestion Field Descriptions**

Field	Description
Layer3 congestion status	Receive congestion status at Layer 3 (that is, MTP3). Possible values are: • Abate =. MTP3 not congested. MTP2 may forward packets to MTP3. • Onset = MTP3 congested. MTP2 may <i>not</i> forward packets to MTP3. During Layer 3 congestion onset, MTP2 sends SIBs to the remote to indicate the route is “Busy” and cannot accept input packets.
CongestionRxInd	Receive congestion status at Layer 2 (that is, MTP2). Possible values are: • Abate = MTP2 not congested. Remote may send packets to MTP2. • Onset = MTP2 congested. Remote may <i>not</i> send packets to MTP2. During MTP2 congestion onset, MTP2 sends SIBs to the remote to indicate the route is “Busy” and cannot accept input packets.
CongestionTxInd	Transmit congestion status at Layer 2 (that is, MTP2). Possible values are: • Abate (Level0) = MTP2 not congested. MTP3 may send packets to MTP2. • Onset (Level1) = MTP2 congested. MTP3 may send priority 1+ packets. • Onset (Level2) = MTP2 congested. MTP3 may send priority 2+ packets. • Onset (Level3) = MTP2 congested. MTP3 may send priority 3+ packets. • Onset (Level4) = MTP2 congested. MTP3 may <i>not</i> send packets to MTP2. The levels correspond to ANSI congestion levels. (ITU has a similar option.) MTP3 packets have an associated priority (0 to 3). For example, if CongestionTxInd is Onset (Level2), MTP3 may continue sending packets with a priority of 2 or higher, but must drop any packets with a priority of 1 or lower.

Table 58 *show cs7 mtp2 congestion Field Descriptions (continued)*

Field	Description
CongestionTxOnset Level1	MTP2 transmit congestion level thresholds.
CongestionTxOnset Level2	MTP2 determines its txCongestion level as a percentage of packets waiting on its transmitQ (that is, XmitQ depth (max-allowed)).
CongestionTxOnset Level3	The thresholds are documented in this output (and may <i>not</i> be configured or changed by the user). The XmitQ depth (max-allowed) value is configurable by the user and the new threshold values are reflected in the output. For example, if you configure a new xmitQ maxDepth via cs7 mtp2 transmitQ 256: CongestionTxOnset Level1 = 128 (50% of xmitQ maxDepth) CongestionTxOnset Level2 = 179 (70% of xmitQ maxDepth) CongestionTxOnset Level3 = 230 (90% of xmitQ maxDepth) CongestionTxOnset Level4 = 256 (100% of xmitQ maxDepth)
CongestionTxOnset Level4	
XmitQ depth (max-used)	Maximum number of packets that have waited on the xmitQ This count indicates how much of the xmitQ is being used and may help guide configuration of the XmitQ depth (max-allowed) value.
XmitQ depth (max-allowed) = 500	Maximum-allowed depth of xmitQ: (used by MTP2 to determine txCongestion thresholds).

The following example includes output from the **show cs7 mtp2** command using the **state** keyword:

```

ITP# show cs7 mtp2 state serial0/1/0:0
CS7 MTP2 states for interface Serial0/1/0:0
Protocol version for interface Serial0/1/0:0 is ITU-T Q.703 (1996) (White Book)

Link State Control (LSC)           = In Service
Initial Alignment Control (IAC)     = Idle
Transmission Control (TXC)         = In Service
Reception Control (RC)              = In Service
Signal Unit Error Rate Monitor (SUERM) = Monitoring
Alignment Unit Error Rate Monitor (AERM) = Idle
Congestion (CONG)                  = Idle

Layer3 link status                  = Started
Layer3 congestion status            = Abate

```

[Table 59](#) describes the fields in the display.

Table 59 **show cs7 mtp2 state Field Descriptions**

Field	Description
Link State Control (LSC) = In Service Initial Alignment Control (IAC) = Idle Transmission Control (TXC) = In Service Reception Control (RC) = Inservice Signal Unit Error Rate Monitor (SUERM) = Monitoring Alignment Unit Error Rate Monitor (AERM) = Idle Congestion (CONG) = Idle	Each state represents the state machines that run the MTP2 protocol and are defined in the ANSI/ITU specifications for MTP2.
Link3 link status = Started	Indicates status of the link from Layer 3 perspective. Values are: Started or Stopped
Layer3 congestion status = Abate	Indicates the congestion status from Layer 3 perspective. Values are: - Abate = MTP3 not congested. MTP2 may forward packets to MTP3. - Onset = MTP3 congested. MTP2 may <i>not</i> forward packets to MTP3.

The following example includes output from the **show cs7 mtp2** command using the **statistics** keyword:

```
ITP# show cs7 mtp2 statistics serial0/1/0:0
CS7 MTP2 Statistics for interface Serial0/1/0:0
Protocol version for interface Serial0/1/0:0 is ITU-T Q.703 (1996) (White Book)
```

```
OMtimeINSV (secs)      = 1591
OMtimeNotINSV (secs)   = 200
```

```
OMIACAlignAttemptCount = 7
OMIACAlignFailCount    = 2
OMIACAlignCompleteCount = 2
```

```
OMMSU_L3_XMIT_Count    = 82
OMMSU_XMIT_Count       = 82
OMMSUBytesTransmitted  = 1654
OMMSU_RE_XMIT_Count    = 0
OMMSUBytesRetransmitted = 0
```

```
OMMSU_RCV_Count        = 80
OMMSUBytesReceived     = 1636
```

```
OMFISU_XMIT_Count      = 82
OMFISU_RCV_Count       = 327
```

```
OMLSSU_XMIT_Count      = 23
OMLSSU_XMIT_SINCount   = 0
OMLSSU_XMIT_SIECount   = 4
OMLSSU_XMIT_SIOCount   = 7
OMLSSU_XMIT_SIOSCount  = 12
OMLSSU_XMIT_SIPOCount  = 0
OMLSSU_XMIT_SIBCount   = 0
```

```

OMLSSU_RCV_Count      = 20
OMLSSU_RCV_SINCount    = 8
OMLSSU_RCV_SIECount    = 0
OMLSSU_RCV_SIOCount    = 8
OMLSSU_RCV_SIOSCount   = 4
OMLSSU_RCV_SIPOCount   = 0
OMLSSU_RCV_SIBCount    = 0

OMT1_TMO_Count        = 0
OMT2_TMO_Count        = 0
OMT3_TMO_Count        = 1
OMT4_TMO_Count        = 2
OMT5_TMO_Count        = 0
OMT6_TMO_Count        = 0
OMT7_TMO_Count        = 0

OMAERMCount           = 2
OMAERMFailCount       = 0
OMSUERMCount          = 2
OMSUERMFailCount      = 0

OMCongestionRxCount   = 0
OMCongestionTxCount   = 0
OMRemote_Congestion_Cnt = 0

OMxmitQ_maxcount      = 1

OMNACK_XMIT_Count     = 0
OMNACK_RCV_Count      = 0

OMunreasonableFSN_rcvd = 0      (error)
OMunreasonableBSN_rcvd = 0      (error)
OMabnormalBSN_rcvd     = 0      (error)
OMabnormalFIB_rcvd     = 0      (error)

OMFISU_notAccepted    = 0      (packets dropped)
OMMSU_notAccepted     = 0      (packets dropped)
OMFISU_congestionDrops = 0      (packets dropped)
OMMSU_congestionDrops = 0      (packets dropped)
OMMSU_too_long         = 0      (packets dropped)
OMMSU_unexpectedFSN   = 0      (packets dropped)
OMMSU_discarded        = 0      (packets dropped)

```

Table 60 describes the fields in the display.

Table 60 *show cs7 mtp2 statistics Field Descriptions*

Field	Description
OMtimeINSV (secs)	Length of time link has been in service
OMtimeNotINSV (secs)	Length of time link has been out of service
OMIACAlignAttemptCount	Number of times IAC has attempted link alignment
OMIACAlignFailCount	Number of times alignment attempt has failed
OMIACAlignCompleteCount	Number of times alignment attempt has succeeded
OMMSU_L3_XMIT_Count	Number of MSUs queued from Layer 3 for transmit
OMMSU_XMIT_Count	Number of MSUs actually transmitted (includes retransmits)
OMMSUBytesTransmitted	Number of MSU bytes transmitted (includes retransmits)

Table 60 **show cs7 mtp2 statistics Field Descriptions (continued)**

Field	Description
OMMSU_RE_XMIT_Count	Number of MSU retransmitted
OMMSUBytesRetransmitted	Number of MSU bytes retransmitted
OMMSU_RCV_Count	Number of MSUs received
OMBytesReceived	Number of MSU bytes received
OMFISU_XMIT_Count	Number of FISUs transmitted (not counting autoTx-FISU)
OMFISU_RCV_Count	Number of FISUs received (not counting filtered-FISU)
OMLSSU_XMIT_Count	Number of LSSUs transmitted (not counting autoTx-LSSU)
OMLSSU_XMIT_SINCount	Number of SINS transmitted (not counting autoTx-LSSU)
OMLSSU_XMIT_SIECount	Number of SIEs transmitted (not counting autoTx-LSSU)
OMLSSU_XMIT_SIOCount	Number of SIOs transmitted (not counting autoTx-LSSU)
OMLSSU_XMIT_SIOSCount	Number of SIOSs transmitted (not counting autoTx-LSSU)
OMLSSU_XMIT_SIPOCount	Number of SIPOs transmitted (not counting autoTx-LSSU)
OMLSSU_XMIT_SIBCount	Number of SIBs transmitted (not counting autoTx-LSSU)
OMLSSU_RCV_Count	Number of LSSUs received (not counting filtered-LSSU)
OMLSSU_RCV_SINCount	Number of SINS received (not counting filtered-LSSU)
OMLSSU_RCV_SIECount	Number of SIEs received (not counting filtered-LSSU)
OMLSSU_RCV_SIOCount	Number of SIOs received (not counting filtered-LSSU)
OMLSSU_RCV_SIOSCount	Number of SIOSs received (not counting filtered-LSSU)
OMLSSU_RCV_SIPOCount	Number of SIPOs received (not counting filtered-LSSU)
OMLSSU_RCV_SIBCount	Number of SIBs received (not counting filtered-LSSU)
OMT1_TMO_Count	Number of times T1 timer has expired
OMT2_TMO_Count	Number of times T2 timer has expired
OMT3_TMO_Count	Number of times T3 timer has expired
OMT4_TMO_Count	Number of times T4 timer has expired
OMT5_TMO_Count	Number of times T5 timer has expired
OMT6_TMO_Count	Number of times T6 timer has expired
OMT7_TMO_Count	Number of times T7 timer has expired
OMAERMCCount	Number of times AERM has been activated
OMAERMFaileCount	Number of times AERM has failed
OMSUERMCount	Number of times SUERM has been activated
OMSUERMFaileCount	Number of times SUERM has failed
OMCongestionRxCount	Number of times link has entered RxCongestionOnset
OMCongestionTxCount	Number of times link has entered TxCongestionOnset
OMRemote_Congestion_Cnt	Number of times remote has gone into RxCongestion
OMxmitQ_maxcount	Maximum number of packets that were allowed to wait on xmitQ
OMNACK_XMIT_Count	Number of negative acknowledgements transmitted on link

Table 60 *show cs7 mtp2 statistics Field Descriptions (continued)*

Field	Description
OMNACK_RCV_Count	Number of negative acknowledgements received on link
OMunreasonableFSN_rcvdv	Number of invalid FSNs received from remote
OMunreasonableBSN_rcvd	Number of invalid BSNs received from remote
OMabnormalBSN_rcvd	Number of abnormal BSNs received from remote (2 invalid BSNs in a row)
OMabnormalFIB_rcvd	Number of abnormal FIBs received from remote (2 invalid FIBs in a row)
OMFISU_notAccepted	Number of FISUs dropped due to MTP2 NoAccept state
OMMSU_notAccepted	Number of FISUs dropped due to MTP2 NoAccept state
OMFISU_congestionDrops	Number of FISU packets dropped due to rxCongestion
OMMSU_congestionDrops	Number of MSU packets dropped due to rxCongestion
OMMSU_too_long	Number of MSUs dropped due to exceed max pakSize
OMMSU_unexpectedFSN	Number of MSU packets dropped due to unexpected FSN received
OMMSU_discarded	Number of MSUs dropped (total)

The following example includes output from the **show cs7 mtp2** command using the **timers** keyword. The variant is TTC.

```
ITP# show cs7 mtp2 timers serial0/1/0:0
CS7 MTP2 Timers for interface Serial0/1/0:0 (in milliseconds)
Protocol version for interface Serial0/1/0:0 is ITU-T Q.703 (1996) (White Book)

t1 (aligned/ready)      = 15000
t2 (not aligned)        = 5000
t3 (aligned)            = 3000
t4 (emergency proving)   = 3000
t4 (normal proving)      = 200
t5 (sending SIB)        = 100
t6 (remote congestion)  = 3000
t7 (excess ack delay)   = 3000
tx (TTC timers)         = 24
```

Table 61 describes the fields in the display.

Table 61 *show cs7 mtp2 timers Field Descriptions*

Field	Description
T1 (aligned/ready) = 40000	Alignment ready timer. ANSI default is 13000 milliseconds. ITU default is 40000 milliseconds.
T2 (not aligned) = 5000	Not aligned timer. ANSI default is 11500 milliseconds. ITU default is 5000 milliseconds.
T3 (aligned) = 1500	Aligned timer. ANSI default is 11500 milliseconds. ITU default is 1500 milliseconds.
T4 (emergency proving) = 500	Emergency proving period timer. ANSI default is 600 milliseconds. ITU default is 500 milliseconds.

Table 61 *show cs7 mtp2 timers Field Descriptions (continued)*

Field	Description
t4 (normal proving) = 8200	Normal proving period timer. ANSI default is 2300 milliseconds. ITU default is 8200 milliseconds.
t5 (sending SIB) = 100	Sending SIB timer. ANSI default is 80 milliseconds. ITU default is 100 milliseconds.
t6 (remote congestion) = 3000	Remote congestion timer. ANSI default is 1000 milliseconds. ITU default is 3000 milliseconds.
t7 (excess ack delay) = 1000	Excessive delay of acknowledgment timer. ANSI default is 1000 milliseconds. ITU default is 1000 milliseconds.
tx (TTC timers) = 24	TTC timers (TA, TF, TO, TS). Default is 20 milliseconds.

**Note**

Ranges are defined by ANSI or ITU.

The following example includes output from the **show cs7 mtp2** command using the **variant** keyword:

```
ITP# show cs7 mtp2 variant serial0/1/0:0
Protocol version for interface Serial0/1/0:0 is ITU-T Q.703 (1996) (White Book)
```

[Table 62](#) describes the fields in the display.

Table 62 *show cs7 mtp2 variant Field Descriptions*

Field	Description
Protocol version for interface Serial0/1/0:0 is ITU-T Q.703 (1996) (White Book)	Identifies the variant supported on the interface. Possible values are: - ansi ANSI SS7 protocol variant - china CHINA SS7 protocol variant - itu ITU SS7 protocol variant - ttc Japan TTC SS7 protocol variant

Related Commands

Command	Description
mtp2-timer	Tunes MTP2 encapsulation timers or specifies the threshold for transmit congestion.

show cs7 mtp3 counters

To display the MTP3 counter for MSUs dropped due to failed OPC verification, use the **show cs7 mtp3 counters** EXEC command.

show cs7 [*instance-number*] **mtp3 counters**

Syntax Description

<i>instance-number</i>	Specifies the instance. The valid range is 0 to 7. The default instance is 0.

Defaults

The default instance is 0.

Command Modes

EXEC

Command History

Release	Modification
12.2(18)IXG	This command was introduced.
12.4(15)SW2	
12.2(33)IRB	

Examples

The following example includes output from the **show cs7 mtp3 counters** command:

```
ITP# show cs7 mtp3 counters
Instance: 0
Counter Value
-----
OPC Verif Fail 99999
```

Related Commands

Command	Description
show cs7 mtp3 event-history	Displays MTP3 logged events.

show cs7 mtp3 errors

To display a list of MTP errors, use the **show cs7 mtp3 errors** EXEC command.

show cs7 mtp3 errors

Syntax Description This command has no arguments or keywords

Defaults None.

Command Modes EXEC

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples The following example includes output from the **show cs7 mtp3 errors** command. The error type is preceded by the number of occurrences of the error.

```
ITP# show cs7 mtp3 errors
32      - Undefined Error Type
19      - SLT undefined OPC
4       - MTP3 Management process not started
```

[Table 63](#) provides descriptions of the various types of MTP errors encountered on the devices supporting the IP Transfer Point product. The errors are listed in alphabetical order.

Table 63 *show cs7 mtp3 errors*

Error	Description
ACL received linkset match	Access list applied to all MSUs arriving on a linkset matched and the result was to drop MSUs.
ACL send linkset match	Access list applied to all MSUs to be transmitted on a linkset matched and the result was to drop MSUs.
AS not found for routingContext	Unable to locate routing context for application service. No error message is issued and packet is dropped.
Denied	Packet was received and an output linkset was selected. The destination point code was denied (TFP) or an access list outbound linkset indicated that packet should be dropped.
Detected looping packet	A packet was received that specified OPC that matches the signaling points primary or secondary point codes. The packet is dropped and no messages are issued.

Table 63 *show cs7 mtp3 errors (continued)*

Error	Description
Failure inserting M3UA headers in message	Unable to insert necessary information into header of M3UA message. No error message is issued and packet is dropped.
Failure to locate active ASP	Unable to locate active application server process. No error message is issued and packet is dropped.
HMRT event overflow	The signaling message handling - message routing queue has reached limit and MSU is discarded without error message being issued.
Incorrect HO value in SLTC message	A packet was received that contained an incorrect value for H0 field. An error message is logged to console indicating source of packet and packet is dropped.
Incorrect H1 value in SLTC message	A packet was received that contained an incorrect value for H1 field. An error message is logged to console indicating source of packet and packet is dropped.
Incorrect link type	A packet was received that contained an undefined link type in "lp->type" field, probably because of a software error. Packet is dropped without issuing error message.
Incorrect Network Indicator received in packet	A packet was received with a different network indicator. The packet is dropped.
Incorrect peer protocol	Error type not currently used.
Incorrect SCTP link status	Error type not currently used.
Incorrect SCTP stream number	Error type not currently used.
Invalid packet size (MSU size exceeded)	An MSU was received that exceeded specified limit. No error message is issued and packet is dropped.
Link event discarded (verification failed)	An MTP3 event was queued for processing. However, event cannot be processed because the target resource does not exist. This situation can occur when links or linkset are not configured. MTP3 event is discarded without issuing error message.
Local Point Code not defined	A packet was received before local point code was defined. The packet is dropped.
MTP3 Management process not started	A packet was received and did not contain a valid link pointer in packet.
Multi-layer Routing abort	An MSU processed by multilayer routing has matched rule indicating it should be aborted. No error message is issued and packet is dropped.
No instance	An MSU was received on a link and the instance information is inconsistent. This situation can occur when instances are removed or linksets are moved between instances. It may also occur as a byproduct of some software error. MSU is discarded without issuing message to log.
No link	An MSU was received that specified a destination point code. The output linkset did not have any operational links. MSU is dropped and no error messages are displayed.

Table 63 *show cs7 mtp3 errors (continued)*

Error	Description
No link pointer in packet	A packet was received and did not contain a valid link pointer in packet.
No linkset	An MSU was received that specified a destination point code. The destination was either unavailable from the reception of TFP or no route had been configured to destination. MSU is dropped and no error messages are displayed.
No memory for cs7_info chunk	An MSU was received but could not be processed because necessary additional storage was unavailable. No error message is issued. Packet is dropped.
No memory for SCTP buffer	A packet was received but could not be processed because the SCTP layer was unable to obtain packet buffer. No error message is issued. Packet is dropped.
Received partial SCTP buffer	A partial packet was received and could not be processed by SCTP layer. No error message is issued. Packet is dropped.
Remote congestion	A link used to transport MSU to next Signaling point is congested. MSUs are discarded as required by congestion control. Messages are logged to console when link enters and exits congestions.
Send failure	An error occurred when attempting to send packet on link. Packet is dropped without issuing error message.
SLT failed	A Signaling Link Test Message failed. This error occurs when the sender of the SLT messages did not receive a response in the required time frame. • The variant is misconfigured. • The link has some type of mismatch on configuration. • Link has some type of hardware problem.
SLT incorrect network indicator	A Signaling Link Test Message was received with a different network indicator. An error message is logged to console indicating link receiving SLTM.
SLT incorrect OPC	A Signaling Link Test Message was received from a different Origination Point-Code than was expected for the linkset containing link. For example, a linkset is configured to connect to point code 1.1.1 and received a response from 1.2.1. Error messages are logged to console indicating the linkset on which link was received and the linkset that should have received SLTM.
SLT incorrect SLC	A Signaling Link Test Message was received from a different Signaling Link Code than was expected for the link. For example, a link is configured with SLC of 5 and is incorrectly connected to link with SLC of 15.2.1. Error messages are logged to console indicating the link that was misconfigured.
SLT invalid	A Signaling Link Test Message that contained incorrectly formatted data and could not be processed.

Table 63 *show cs7 mtp3 errors (continued)*

Error	Description
SLT received bad pattern	A Signaling Link Test Message received with an incorrectly formatted pattern. This situation can occur in the following situations: • The variant is incorrectly configured. • The link has some type of mismatch on configuration. • Link has some type of hardware problem.
SLT received from non-adjacent OPC	A Signaling Link Test Message was received from an Origination Point-Code that could not be accessed by directly attached linkset and the OPC is specified in the routing table indicating the OPC is not directly attached to device. Error messages are logged to console indicating the linkset on which this SLTM was received.
SLT undefined OPC	A Signaling Link Test Message was received from an Origination Point-Code that is not defined to any linkset.
SLT undefined SLC	A Signaling Link Test Message was received from a Signaling Link Code not in use for linkset. An error message is logged indicating which link received SLTM messages and the incorrect SLC.
Undefined Error Type	An error unknown error type was encountered that probably indicates some type of software problem has occurred.
Unlock requested lock count!=0 cs7_info	An internal software error has occurred during the processing of an MSU. No error message is issued. Packet is dropped.
Unsupported management messages	Error type not currently used.
Variant not defined	A packet was received before all variant information has been defined. The packet is dropped.

Related Commands

Command	Description
show cs7 mtp3 event-history	Displays MTP3 logged events.
show tech-support	Collects and displays a large amount of ITP configuration information that can be used for troubleshooting.

show cs7 mtp3 event-history

The events exchanged among the three MTP components—traffic, link, and route management—are logged in memory by default. To display logged events, use the **show cs7 mtp3 event-history** EXEC command.

show cs7 [*instance-number*] **mtp3 event-history** *number*

Syntax Description	<i>instance-number</i>	Specifies the instance. The valid range is 0 to 7. The default instance is 0.
	<i>number</i>	Number of events to display. Valid numbers range from 0 to 5000.

Defaults The default instance is 0.

Command Modes EXEC

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines To capture all events in one display, configure the **terminal length** EXEC command to 0.

Examples The following example includes output from the **show cs7 mtp3 event-history** command with the number of events to display (*number* argument) being **10**:

```
ITP# show cs7 mtp3 event-history 10
22:26:01 CS7 MTP3 MGMT event history. Max configured to be saved: 1024
Num of events currently saved: 16. Num to be displayed: 10
NOTE: Event history logging will be suspended while events are being displayed

00:00:13 LOG MTP3 Event: To: TPRC Fm: MGMT Ev: SP_restart_indication
00:00:13 LOG MTP3 Event: To: LLSC Fm: TPRC Ev: restart_begins tony
00:00:13 LOG MTP3 Event: To: LLSC Fm: TPRC Ev: restart_begins michael
00:00:13 LOG MTP3 Event: To: TSRC Fm: TPRC Ev: restart_begins
00:00:13 LOG MTP3 Event: To: TSFC Fm: TPRC Ev: restart_begins
00:00:13 LOG MTP3 Event: To: TLAC Fm: TPRC Ev: restart_begins tony 0
00:00:13 LOG MTP3 Event: To: TLAC Fm: TPRC Ev: restart_begins michael 0
00:00:13 LOG MTP3 Event: To: RSRT Fm: TPRC Ev: restart_begins
00:00:13 LOG MTP3 Event: To: LSAC Fm: LLSC Ev: activate_link tony 0
00:00:13 LOG MTP3 Event: To: LSAC Fm: LLSC Ev: activate_link michael 0
```

Related Commands	Command	Description
	show cs7 mtp3 timers	Displays the values of MTP3 timers.

show cs7 mtp3 timers

To display the values of MTP3 timers, use the **show cs7 mtp3 timers** EXEC command.

show cs7 [*instance-number*] **mtp3 timers**

Syntax Description	<i>instance-number</i>	Specifies the instance. The valid range is 0 to 7. The default instance is 0.

Defaults	The default instance is 0.

Command Modes	EXEC

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	The Scope field shows all global MTP3 timers and all linkset and link timers that have been defined at the global level. Linkset timers have the value “ls” in the scope field and link timers have the value “link” in the scope field.

Examples	The following example includes output from the show cs7 mtp3 timers command:

```
ITP# show cs7 mtp3 timers
CS7 MTP3 Timers global timers in milli-seconds
Timer   Value(ms) Description                               Scope
-----
t06      800 (avoid mis-seq. on controlled rerouting)      global
t08     1000 (transfer-prohibited inhibited timer)      global
t10    45000 (waiting to repeat route-set-test message)  global
t11    60000 (transfer-restricted)                     global
t15     2500 (repeat signaling route set congestion test) global
t16     1700 (waiting for route-set congestion update)  global
t18    30000 (MTP restart link supervision)            global
t20    60000 (MTP restart timer at the signaling point) global
```

Related Commands	Command	Description
	show cs7 mtp3 event-history	Displays MTP3 logged events.

show cs7 nso

To display NSO (Nonstop Operation) information, use the **show cs7 nso** privileged EXEC command.

show cs7 nso {counters [detailed] | state}

Syntax Description	counters	Displays counters maintained by NSO.
	detailed	Displays detailed output.
	state	Displays NSO state information.

Defaults None.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples The following example shows how to display NSO state information:

```
ITP# show cs7 nso state
ITP NSO state information:
  Current State:                operative
  Operating Redundancy Mode:    sso
  Configured Redundancy Mode:  sso
  Redundancy State:            ACTIVE
  Peer Redundancy State:       STANDBY HOT
  Checkpointing state:
    Last seq # sent:            143657
    Last seq # rcvd:            0
    Congested:                  FALSE
    Current send queue depth: 0
```

[Table 64](#) describes the significant fields shown in the display.

Table 64 *show cs7 nso Field Descriptions*

Field	Description
Current State	Fields describe the current state
Operating Redundancy Mode	Current operational redundancy mode
Configured Redundancy Mode	Current setting of redundancy mode command
Redundancy State	Current redundancy state
Peer Redundancy State	Current redundancy state of other Route Processor

Table 64 *show cs7 nso Field Descriptions (continued)*

Field	Description
Checkpointing state	Fields describe current state of checkpointing
Last seq # sent	Sequence number of last NSO Checkpointing message sent to other Route Processor
Last seq # rcvd:	Sequence number of last NSO Checkpointing message received from other Route Processor
Congested	TRUE if congestion is present on communication to other Route Processor
Current send queue depth	Number of messages waiting to be sent to other Route Processor

Related Commands

Command	Description
cs7 nso	Enables ITP Nonstop Operation (NSO).
show tech-support	Collects and displays a large amount of ITP configuration information that can be used for troubleshooting.

show cs7 offload

To display the current status, counters, and events maintained by the cs7 offload feature, use the **show cs7 offload instance EXEC** command.

show cs7 offload instance

Syntax Description	offload	The transfer of data operations.

Defaults	None.

Command Modes	EXEC

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	The show cs7 offload instance command is used for a Cisco ITP FlexWan. For use on the Cisco ITP Supervisor Module the user enters the command execute-on {flex-wan-number all-flex} all show cs7 offload instance .

Examples	The following output excerpt includes some of the most significant output fields for the show cs7 offload instance command. Table 65 defines these output fields.

```
ITP# show cs7 offload instance

Instance 1
Point Code          235-33-0:1
SS7 Variant         ANSI

Dropped MSUs:
-----
bufferedPak_drops   0
bufferedPak_flushes 0
mgmt_pak_drops      0
tfc_attempt_drops   0
    tfc_attempt_count 0
loop_detected_drops 0
in_acl_drop         0
dcs7_route_pak_fail 125
no_route_link       124
out_acl_drop        0
alias_route_pak_fail 0
no_olink_err        0
invalid_pak_size_drops 0
circ rt detection drops 0
```

```

opc verification drops 0
no_rt_handle
current interval      0      total 6

```

Table 65Significant Output Fields for the **show cs7 offload** command

Field	Description
bufferedPak_drops	Cisco ITP has capability to buffer packets at link level equal to bufferPak_threshold per instance. If the packets to be buffered exceed this threshold for an instance, ITP drops these packets and increase this counter.
bufferedPak_flushes	When the link or route is removed, then Cisco ITP flushes the packets if any are already buffered for that link/route. This counter is increased for every packet flushed.
tfc_attempt_drops	Increases to count number of times TFC was dropped.
tfc_attempt_count	Increases to count number of times TFC was send.
loop_detected_drops	Increases for packets drop due to loop detection by ITP.
in_acl_drop	Increases for the packet dropped due to inbound ACL/GWS.
dcs7_route_pak_fail	Increases when the routing of the packet is unsuccessful because no link is available in a linkset.
no_route_link	Increases when current route is not available due to the non-availability of the links in a linkset.
out_acl_drop	Increases for the outbound packet dropped due to ACL/GWS.
alias_route_pak_fail	Increases when the routing to the alias pc failed.
no_olink_err	Increases when the outgoing link is not
invalid_pak_size_drops	Increases when the sizeof mtp3 packet received at ITP is invalid.
circ rt detection drops	Increases when MSUs dropped due to CRD
mgmt_pak_drops	Increases when MGMT paks drop
opc verification drops	Increase for packet drop due to opc verification failed when CRD is enabled.
no_rt_handle/Count/total	Increases when there is no route info for the destination.

The following output is from the **execute-on {flex-wan-number | all-flex} all show cs7 offload instance** command. The **execute-on {flex-wan-number | all-flex} all show cs7 offload instance** command is the version of the **show cs7 offload instance** command used on the supervisor module.

```

ITP_251#execute-on 3 all show cs7 offload instance
----- slot:3 cpu:0 command:show cs7 offload instance -----

```

```

Global configuration:
=====
dcs7_tfc_exceeding_max_rate(LC pacing): 0

```

```

Origination table is disabled

```

```

Instance specific configuration:
=====
Instance 0
Point Code      3.1.1:0

```

```

SS7 Variant          ITU
Network Indicator    national
Secondary PCs        3.2.2
Capability PCs
C-link linkset       (none)
C-link linkset secondary (none)
Total Linksets       7
Available Linksets   2
Total Links          7
Available Links       0
Ok to activate links  T
natopt_tfr           F
natopt_multcon       F
sccp_unsequenced     T
sccp_sequenced       T
natopt_rct           F
natopt_cls_ls        T
use_summary_routing  T
mgmt_sls_value        0
itu_sls_shift_opc_dpc F    opc shift = 0    dpc shift = 0
itu_sls_shift         0
Circular rt detection F
sccp_class1_loadshare F
sccp_class1_wrr       F
mgmt_sls_type         Round Robin
remote_cong_msgs      T
punt                  F
mlr enabled           F
gws enabled           F
Large MSU Support     F
bufferedPak_count     0
bufferedPak_count_peak 0
bufferedPak_threshold 20000

```

Dropped MSUs:

```

-----
bufferedPak_drops      0
bufferedPak_flushes   0
mgmt_pak_drops         0
tfc_attempt_drops     0
    tfc_attempt_count  0
loop_detected_drops    0
in_acl_drop            0
dcs7_route_pak_fail    0
no_route_link          0
out_acl_drop           0
alias_route_pak_fail   0
no_olink_err           0
invalid_pak_size_drops 0
circ rt detection drops 0
opc verification drops 0
no_rt_handle
current interval      0    total 0

```

Informational Counts:

```

-----
alias_instance_punt     0
olink_punt              0
invalid_pak_size (bytes) 0
dcs7_send_vip_pak_fails 0

```

show cs7 offload mtp3

To display the current status, counters, and events maintained by the MTP3 offload feature, use the **show cs7 offload mtp3** EXEC command.

show cs7 offload mtp3 [*slot*] [**detailed**] [**events** [**combined**] [**detailed**]]

Syntax Description

<i>slot</i>	Line card slot number. Valid numbers range from 0 to 12.
events	Displays all the events logged in the maintenance of the configuration and status on the line card. If the slot number and combined keyword are not specified, then the events are displayed independently for each line card.
detailed	Displays the counters maintained for the configuration download to the line card. When the detailed keyword is specified with the events keyword, additional information related to the event is also displayed.
combined	When specified without a slot number, displays the events for all line cards in the timestamp order in which they occurred.

Defaults

None.

Command Modes

EXEC

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Examples

The following example includes output from the **show cs7 offload mtp3** command. The output indicates that MTP3 offload is enabled on line cards 2 and 4, and is functioning normally.

```
ITP# show cs7 offload mtp3
```

```
MTP3 offload enabled.
```

```
Slot  Status    Offload
2      Normal     Enabled
4      Normal     Enabled
```


Table 67 describes the fields in the display, including the possible values that can be displayed in the Status and Offload columns.

Table 66 *show cs7 offload mtp3 Field Descriptions*

Field	Description
Slot	Line card slot.
Status	Indicates which phase is currently applicable for the MTP3 offload on each line card. The possible values that can be displayed in the Status column are Disabled , Init , Normal , and PermDisabled .
Disabled	MTP3 offload is temporarily disabled on the line card. This status is indicated when error recovery is in progress.
Init	MTP3 offload is being initialized on the line card.
Normal	MTP3 offload is enabled and operating normally.
PermDisabled	MTP3 offload has been permanently disabled on the line card. This status is indicated when excessive errors have been encountered on the line card and repeated error recovery attempts have failed. When a line card enters this state, the status of all links on the line card is displayed as “sys-shutdown” when the show cs7 linkset command is executed. A line card in this state can be restarted manually by issuing the cs7 offload mtp3 restart command.
Offload	The Offload column indicates whether or not MTP3 is operational on the line card. The possible values that can be displayed in the Offload column are DisabledSys and Enabled .
DisabledSys	MTP3 offload has been disabled by the system. This status is displayed whenever the ITP is performing error recovery or when MTP3 offload has been permanently disabled on the line card.
Enabled	MTP3 offload has been enabled on the line card.

Related Commands

Command	Description
cs7 offload mtp3	Enables MTP3 offload on all line cards.

show cs7 pc-conversion

To display mapping of real point codes to alias point codes, use the **show cs7 pc-conversion** EXEC command.

show cs7 [*instance-number*] **pc-conversion** [*point-code*]

Syntax Description

<i>instance-number</i>	Instance number.
<i>point-code</i>	Point code.

Defaults

None.

Command Modes

EXEC

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

This command can be issued either globally or on an instance.

Examples

The following example includes output from the **show cs7 pc-conversion** command:

```
ITP# show cs7 0 pc-conversion
PC                ALIAS PC
-----
1.84.1:1          0.85.7:4
1.84.4:4          1.85.7:1
```

Related Commands

Command	Description
cs7 instance pc-conversion	Enables the conversion of packets between instances on the ITP.
cs7 mtp3 tuning rx-congestion-threshold	Enables multiple instances of of a variant and network indicator combination.

show cs7 ping

To display output from a ping test, use the **show cs7 ping** privileged EXEC command.

show cs7 ping *point-code*

Syntax Description	<i>point-code</i>	Point code of the device to ping.

Defaults	None.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples The following example includes output from the **show cs7 ping** command:

```
ITP# show cs7 ping
 10.44.156      running state Generating, 5 seconds left
      current send sequence 4, receive seq 4
```

Related Commands	Command	Description
	ping cs7	Starts a ping to a point code.

show cs7 pmp

To display PMP-related errors, use the **show cs7 pmp** privileged EXEC command.

show cs7 pmp [**errors** | **context** {**as** *as-name* | **linkset** *ls-name*}]

Syntax Description		
errors		Displays link and/or ASP context ID, and inbound/outbound/dropped PMP packets.
as		Specifies an AS.
<i>as-name</i>		Name of the AS.
linkset		Specifies a linkset.
<i>ls-name</i>		Name of the linkset.

Defaults	None.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.4(15)SW3	This command was introduced.
	12.2(33)IRC	

Examples The following example includes output from the **show cs7 pmp error** command:

```
ITP#sh cs7 pmp errors
12          - No active DCS
```

The following example includes output from the **show cs7 pmp context** command used on a specific linkset:

```
ITP#sh cs7 pmp context linkset to_halley_6
SLC  Context  PMP In      PMP Out      PMP Drops
---  -
0    66        26355       26355        0
1    67        26338       26339        0
2    68        26336       26336        0
3    69        26335       26335        0
```

The following example includes output from the **show cs7 pmp context** command used on a specific AS:

```
ITP#sh cs7 pmp context as as_to_bal_1
ASP Name      Context  PMP In      PMP Out      PMP Drops
-----
asp_to_bal12  57       2           4            0
asp_to_bal_1  55       64          5            7
```

Related Commands

Command	Description
cs7 pmp	Turns probeless monitoring on for all linksets and ASes.
cs7 pmp hold-queue	Sets the integer range of PMP hold queue thresholds.
cs7 dcs-group	Identifies a name to associate with a DCS group.
cs 7 dcs	Identifies a name to associate with a DCS node.
show cs7 dcs-group	Displays information about the DCS group.
show cs7 dcs	Displays information about the DCS node.

show cs7 point-codes

To display the point codes that this router is responding to, use the **show cs7 point-codes** privileged EXEC command.

show cs7 [*instance-number*] **point-codes** [**event-history** | **ssn** | **statistics**]

Syntax Description

<i>instance-number</i>	Specifies the instance. The valid range is 0 to 7. The default instance is 0.
event-history	Displays point code history.
ssn	Displays SUA point code/SSN status.
statistics	Displays XUA point code statistics.

Defaults

The default instance is 0.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The **show cs7 point-codes** command displays the point codes that this router is responding to. These point codes include the local point code, secondary point code, capability point code, AS point codes (DPC in the routing key), and AS Route point codes.

Examples

The following example includes output from the **show cs7 point-codes** command:

ITP# **show cs7 point-codes**

```

CS7 Point Code      Type      Status
-----
0.0.4               local     active
0.0.4               AS        M3UA inactive
0.0.3               secondary active
0.0.3               AS        M3UA inactive
0.0.6               AS        M3UA inactive
1.2.3               AS        M3UA active
7.8.9               AS        M3UA inactive
8.7.5               AS Route  M3UA inactive
8.8.8               AS Route  M3UA restricted
9.9.9               AS        M3UA active

```

Related Commands

Command	Description
clear cs7 pointcode event-history	Clears the CS7 M3UA or SUA point code measurements.
show tech-support	Collects and displays a large amount of ITP configuration information that can be used for troubleshooting.

show cs7 qos

To display the QoS class information, use the **show cs7 qos** privileged EXEC command.

show cs7 [*instance-number*] **qos** {**class** *class* | **statistics** *ls-name*}

Syntax Description

<i>instance-number</i>	Specifies the instance. The valid range is 0 to 7. The default instance is 0.
class	Specifies a QoS class.
<i>class</i>	QoS class identifier. Valid range is 0 to 7.
statistics	Displays QoS link usage statistics.
<i>ls-name</i>	Linkset name.

Defaults

The default instance is 0.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Examples

The following example includes output from the **show cs7 qos** command with the **class** keyword:

```

ITP# show cs7 qos class
  QoS  Prec  DSCP  Acc-Grp  MatchType      Input Linkset
  ---  ---  ---  ---  ---  ---
    0     1         none
    1         14      any      to_nyc
    2     3      2701 access-group to_la
    3     4         none

```

[Table 67](#) describes the fields in the display.

Table 67 *show cs7 qos class Field Descriptions*

Field	Description
QoS	QoS class
Prec	IP precedence value assigned to QoS class
DSCP	Differential services code point assigned to QoS class
Acc-Grp	Access group assigned to QoS class
Match Type	Packet matching criteria assigned to QoS class
Input Linkset	Input linkset where packet matching criteria are defined

The following example includes output from the **show cs7 qos** command with the **statistics** keyword:

```
ITP# show cs7 qos statistics michael
lsn=michael      apc=3.3.3      state=avail      available/links=2/3
  SLC  QoS      MSU In      MSU Out      Drops  ByteCnt In  ByteCnt Out
  00   0         520        488          0      10320      8784
  01   1         488        520          0       8784     10320
  02   2          0          0          0          0          0
```

Table 68 describes the fields in the display.

Table 68 *show cs7 qos statistics Field Descriptions*

Field	Description
SLC	Signal Link Code
QoS	QoS class assigned to this link
MSU In	MSUs received on this link
MSU Out	MSUs sent on this link
Drops	MSUs dropped
ByteCnt In	Byte count of MSUs received
ByteCnt Out	Byte count of MSUs sent

Related Commands

Command	Description
cs7 qos class	Specifies a CS7 QoS class.

show cs7 rate-limit

To display the rate-limit status of MTP overflow when under loadsharing through the GTT application group and MTP overflow and loadsharing via MTP routing, use the **show cs7 rate-limit** in privileged EXEC command.

show cs7 [*instance instance-number*] **rate-limit** {*pc pc* | *asname asname*}

Syntax Description	<i>instance-number</i>	Specifies the instance. The valid range is 0 to 7. The default instance is 0.
	rate-limit	Displays the rate-limit of DPC/AS in GTT application group wide.
	asname	Filters on AS name.
	<i>asname</i>	AS name.

Defaults None.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.4(15)SW4	The command was introduced.
	12.2(33)IRD	

Examples The following example includes output from the **show cs7 rate-limit** command:

```
ITP# show cs7 rate-limit pc 7.7.7
# of limited point: 2
    node id: 1503
    rate limit: 1000
configuration type: SCCP Global
point-code: 7.7.7:0

SLOT    QUOTA    IN_PKTS
1/0      300         0
1/1      300         0
2/0      300         0
2/1      300         0
```

Related Commands	Command	Description
	cs7 gtt application-group	Specifies a GTT application group.
	show cs7 gtt consistency	Displays GTT point codes that do not have routes provisioned for them.
	cs7 rate-limit	Limits traffic rate to a specified DPC/AS in an MTP over-flow load-share that uses a GTT application group. Adds or changes a point code and optional subsystem number in the application group

Command	Description
pc (cs7 gtt application group)	Adds or changes a point code and optional subsystem number in the application group.
asname (cs7 gtt application group)	Assigns an M3UA or SUA AS directly to a global title.

show cs7 route

To display the ITP routing table, use the **show cs7 route** EXEC command.

show cs7 [*instance-number*] **route** [*pc* [**summary-routes**]] [**circular**] [**brief** | **detailed**]

Syntax Description

<i>instance-number</i>	Required only if the cs7 multi-instance feature is enabled. Specifies the instance. The valid range is 0 to 7. The default instance is 0.
<i>pc</i>	Point code.
summary-routes	Displays summary routes information for the specified pc.
circular	Displays only those routes that are flagged as prohibited due to circular route detection.
brief	Displays a brief form of the output.
detailed	Displays a detailed form of the output including marking any route prohibited due to CRD procedures with CIRC for route status.

Defaults

The default instance is 0.

Command Modes

EXEC

Command History

Release	Modification
12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.
12.2(18)IXC 12.4(11)SW 12.2(33)IRA	The displayed XUA point code status added the MTP destination status of that point code.
12.2(18)IXG 12.4(15)SW2 12.2(33)IRB	The detailed keyword was modified so that any route prohibited due to CRD procedures is marked with CIRC for route status.
12.2(18)IXG 12.4(15)SW2 12.2(33)IRB	The show cs7 route command was enhanced with a new optional keyword, circular , to display only those routes that are flagged as prohibited due to circular route detection.
12.4(15)SW6 12.2(33)IRF	The show cs7 route command output was enhanced with a new <i>Load Share</i> column that indicates whether the linkset load sharing feature is enabled.

Usage Guidelines

The output of the **show cs7 route** command varies based on the options specified, the variant, the masks used to configure routes, and the configuration options.

Routes are two basic types. The first type of route is fully qualified. A fully qualified route has a mask specifying all of the allowed bits of the destination point code. For example, a fully qualified route for the ANSI variant has a mask of 255.255.255 or a mask length of 24 bits. When the variant is ITU, the fully qualified route has a mask of 7.255.7 or a mask length of 14 bits. The second type of route is a

summary route that represents a group of destination point codes. For example, with a variant of ITU, a point code of 5.11.0, and a mask of 7.255.0, the route represents all points in the range of 5.11.0 to 5.11.7. A special type of summary route is a cluster route. Cluster routes are only defined for the ANSI variant and mask; the mask must be 255.255.0.

In ITP release 12.2(18)IXC, the displayed XUA point code status includes the MTP destination status of that point code.

The following configuration options affect the route and destination status information:

summary-routing-exception

This option indicates whether to use the summary routes when the fully qualified route is not available. By default, this option is off and summary route can be used to route MTP3 messages. In this case, when a summary route is available and a fully qualified route is unavailable, the destination status for the fully qualified route is restricted rather than unavailable. When this option is enabled, the destination status for the fully qualified route is unavailable.

max-dynamic-routes

This option defines the maximum number of dynamic routes allowed for the signaling point. If the limit is reached, the status of some routes does not reflect the information reflected in the MTP3 management packets.

national-options TFR

This option applies only to ITU and China variants and indicates whether transfer-restricted MTP3 management messages will be exchanged between signaling points. When this option is enabled, route and destination statuses can display the restricted state.

national-options multiple-congestion



Note

Changing any of the global configuration options on an operational box does not update all route and destination statuses. Routing behavior changes correctly, although it might not match what is indicated by some destination statuses. These options are intended to be a one-time configuration before the box is put in service.

Examples

The **show cs7 route** command without options produces a list of destinations and the associated routes used to access each destination. The following examples include output from the **show cs7 route** command executed with no modifying keywords. The Load Share column was introduced in 12.2(33)IRF and 12.4(15)SW6 and indicates that the linkset load sharing feature is enabled.

```
ITP# show cs7 route
Destination          Prio Linkset Name      Route Load Share
-----
1.1.1/14             acces  1 m2pa_194_00         avail  T
                   1 m2pa_194_01         avail  T
1.1.0/12             acces  2 m2pa_194_00         avail  F
1.1.5/14             acces  1 VirtualLS0-4        avail  F
```

The **show cs7 route** command with the **brief** keyword produces only a list of destinations. The following example includes output from the **show cs7 route** command executed with the **brief** keyword.

```
ITP# show cs7 route brief
Routing table = system

Destination          Cong
```

```

-----
1.1.0/11      acces
1.1.1/14      acces
3.1.1/14      acces

Routing table = XUA

Destination      Type
-----
2.1.1/14      INACC  AS
2.2.2/14      RESTR  AS Route
4.1.1/14      INACC  AS
4.4.4/14      RESTR  AS Route

```

The **show cs7 route** command with the **detailed** option produces a list of destinations and associated routes with the available management information. Any route that is prohibited due to CRD procedures is marked with CIRC to make it distinct from ordinary prohibited status. The following example includes output from the **show cs7 route** command with the **detailed** keyword.

```

ITP# show cs7 route detailed
Dynamic Routes 0 of 1000
Routing table = system Destinations = 3 Routes = 4
C=Cong Q=QoS P=Prio
Destination C Q P Linkset Name Linkset Non-adj Route
-----
1.10.1/14 INACC 1 sunset avail PROHIB CIRC

```

The **show cs7 route** command with the optional **circular** keyword displays only those routes that are flagged as prohibited due to circular route detection. The following example includes output from the **show cs7 route** command with the **circular** keyword.

```

Router#show cs7 route circular
Dynamic Routes 0 of 1000
Routing table = system Destinations = 3 Routes = 4
Destination Prio Linkset Name Route
-----
1.10.1/14 INACC 1 sunset CIRC

```

The following example includes output from the **show cs7 route** command executed with a destination point code (*pc* argument) of 4.1.1:

```

ITP# show cs7 route 4.1.1
Routing table = XUA

```

```

Destination      Type
-----
4.1.1/14      INACC  AS

```

The **show cs7 route** command with a point-code destination argument (*pc*) and **summary-routes** keyword produces a list of routes matching the specified destination. The following example includes output from the **show cs7 route** command executed with the *pc* argument and **summary-routes** keyword.

```

ITP# show cs7 route 1.1.1 summary-routes detail
Routing table = system
C=Cong Q=QoS P=Prio
Destination      C Q P Linkset Name Linkset Non-adj Route
-----
1.1.0/11      acces      1 barbados      avail      allowed avail
1.1.1/14      acces      1 bermuda       avail      allowed avail
5 bimini avail allowed avail

```

Table 69 describes the fields in the display.

Table 69 **show cs7 route Field Descriptions**

Field	Description						
Destination	This field is displayed in the format "dpc/masklength status." <i>dpc</i> is the destination point code. <i>masklength</i> is the number of significant leading bits in the point code. <i>status</i> can be one of the following states: <table> <tr> <td>acce</td><td>Accessible</td></tr> <tr> <td>INACC</td><td>Inaccessible</td></tr> <tr> <td>RESTR</td><td>Restricted</td></tr> </table> The restricted status is available only under the ITU variant when the cs7 national-options TFR configuration option has been specified. The destination information is followed by one or more routes to that destination in the default and detailed views.	acce	Accessible	INACC	Inaccessible	RESTR	Restricted
acce	Accessible						
INACC	Inaccessible						
RESTR	Restricted						
C	Congestion information appears when the brief or detailed keyword has been specified. This information is the destination congestion status. Normally, the congestion status is zero and nothing is displayed. In ANSI networks, or in ITU networks with the national option for multiple congestion levels turned on, this field displays the congestion level with the numbers 1, 2, or 3. In ITU networks with the national option for multiple congestion levels turned off, this field displays the number 1 if the destination is congested.						
Q	QoS class assigned to the destination, a decimal number in the range 1 to 7.						
P	Route priority, a decimal number in the range 1 to 9.						
Linkset Name	Linkset for a route to the destination.						
Linkset	Linkset status can be one of the following states: <table> <tr> <td>avail</td><td>Available</td></tr> <tr> <td>UNAVAIL</td><td>Unavailable</td></tr> </table>	avail	Available	UNAVAIL	Unavailable		
avail	Available						
UNAVAIL	Unavailable						

Table 69 *show cs7 route Field Descriptions (continued)*

Field	Description														
Non-adj	The nonadjacent status shows the accessibility of the destination from the adjacent point code at the remote end of the linkset. The status can be one of the following states: <table> <tr> <td>allowed</td><td>Allowed</td></tr> <tr> <td>RESTRIC</td><td>Restricted</td></tr> <tr> <td>PROHIB</td><td>Prohibited</td></tr> </table>	allowed	Allowed	RESTRIC	Restricted	PROHIB	Prohibited								
allowed	Allowed														
RESTRIC	Restricted														
PROHIB	Prohibited														
Route	Route status. This status can be one of the following states: <table> <tr> <td>avail</td><td>Available</td></tr> <tr> <td>RESTRIC</td><td>Restricted</td></tr> <tr> <td>UNAVAIL</td><td>Unavailable</td></tr> </table> The route status is derived from the linkset status and the nonadjacent status. The latter are displayed in the detailed view. If the linkset is unavailable, the route is unavailable. If the linkset is available, the nonadjacent status is mapped to Route Status as follows: <table> <tr> <th>Non-Adjacent</th><th>Route</th></tr> <tr> <td>allowed</td><td>available</td></tr> <tr> <td>restricted</td><td>restricted</td></tr> <tr> <td>prohibited</td><td>unavailable</td></tr> </table>	avail	Available	RESTRIC	Restricted	UNAVAIL	Unavailable	Non-Adjacent	Route	allowed	available	restricted	restricted	prohibited	unavailable
avail	Available														
RESTRIC	Restricted														
UNAVAIL	Unavailable														
Non-Adjacent	Route														
allowed	available														
restricted	restricted														
prohibited	unavailable														

Related Commands

Command	Description
cs7 host	Maps a hostname to a point code.
show tech-support	Collects and displays a large amount of ITP configuration information that can be used for troubleshooting.
update route (route-table)	Updates the route table.

show cs7 sample sls

To display the results from the latest SLS sample, use the **show cs7 sample sls** privileged EXEC command.

show cs7 sample sls

Syntax Description	sls	Field in MSUs used for load sharing.

Defaults	None.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.2(18)IXF	This command was introduced.
	12.4(15)SW1	
	12.2(33)IRA	

Usage Guidelines	This command fails if: - No sample has been performed. - A sample is currently in progress. - The link or linkset that was last sampled has been deleted.

Examples	The following example includes output from the show cs7 sample sls command:

```
router# show cs7 sample sls
SLS Received Report for linkset LS-A from Nov 27 2007 13:44:32
  SLS number      SLS number      SLS number      SLS number
    rcvd          rcvd          rcvd          rcvd
 000 0002        004 0002        008 0000        012 0000
 001 0002        005 0002        009 0000        013 0000
 002 0002        006 0002        010 0000        014 0000
 003 0002        007 0002        011 0000        015 0000
```

The next example shows ANSI output. ANSI uses 8-bit SLS, so it has 256 SLS values. This amount differs from ITU, China, and Japan's TTC Variants, which use 4-bit SLS and have 16 SLS values.

The following example includes output from the **show cs7 sample sls** command:

```
router# show cs7 sample sls
SLS Received Report for linkset LS-B from Nov 27 2007 13:44:32
SLS number      SLS number      SLS number      SLS number
    rcvd          rcvd          rcvd          rcvd
 000 0037        064 0004        128 0005        192 0005
 001 0005        065 0004        129 0005        193 0005
```

 show cs7 sample sls

002	0005	066	0004	130	0005	194	0005
003	0005	067	0004	131	0005	195	0005
004	0004	068	0004	132	0005	196	0005
005	0004	069	0004	133	0005	197	0005
006	0004	070	0004	134	0005	198	0005
007	0004	071	0004	135	0005	199	0005
008	0004	072	0004	136	0005	200	0005
009	0004	073	0004	137	0005	201	0005
010	0004	074	0004	138	0005	202	0005
011	0004	075	0005	139	0005	203	0005
012	0004	076	0005	140	0005	204	0005
013	0004	077	0005	141	0005	205	0005
014	0004	078	0005	142	0005	206	0005
015	0004	079	0005	143	0005	207	0005
016	0005	080	0004	144	0005	208	0005
017	0005	081	0004	145	0005	209	0005
018	0005	082	0004	146	0005	210	0005
019	0004	083	0004	147	0005	211	0005
020	0004	084	0004	148	0005	212	0005
021	0004	085	0004	149	0005	213	0005
022	0004	086	0004	150	0005	214	0005
023	0004	087	0004	151	0005	215	0005
024	0004	088	0004	152	0005	216	0005
025	0004	089	0004	153	0005	217	0005
026	0004	090	0004	154	0005	218	0005
027	0004	091	0005	155	0005	219	0005
028	0004	092	0005	156	0005	220	0005
029	0004	093	0005	157	0005	221	0005
030	0004	094	0005	158	0005	222	0005
031	0004	095	0005	159	0005	223	0005
032	0004	096	0005	160	0005	224	0005
033	0004	097	0005	161	0005	225	0005
034	0004	098	0005	162	0005	226	0005
035	0004	099	0005	163	0005	227	0005
036	0004	100	0005	164	0005	228	0005
037	0004	101	0005	165	0005	229	0005
038	0004	102	0005	166	0005	230	0005
039	0004	103	0005	167	0005	231	0005
040	0004	104	0005	168	0005	232	0005
041	0004	105	0005	169	0005	233	0005
042	0004	106	0005	170	0005	234	0005
043	0004	107	0005	171	0005	235	0005
044	0004	108	0005	172	0005	236	0005
045	0004	109	0005	173	0005	237	0005
046	0004	110	0005	174	0005	238	0005
047	0004	111	0005	175	0005	239	0005
048	0004	112	0005	176	0005	240	0005
049	0004	113	0005	177	0005	241	0005
050	0004	114	0005	178	0005	242	0005
051	0004	115	0005	179	0005	243	0005
052	0004	116	0005	180	0005	244	0005
053	0004	117	0005	181	0005	245	0005
054	0004	118	0005	182	0005	246	0005
055	0004	119	0005	183	0005	247	0005
056	0004	120	0005	184	0005	248	0005
057	0004	121	0005	185	0005	249	0005
058	0004	122	0005	186	0005	250	0005
059	0004	123	0005	187	0005	251	0005
060	0004	124	0005	188	0005	252	0005
061	0004	125	0005	189	0005	253	0005
062	0004	126	0005	190	0005	254	0005
063	0004	127	0005	191	0005	255	0005

Related Commands

Command	Description
cs7 sample linkset	Samples all traffic coming in or out of a link or linkset and then reports the number of MSUs for each SLS value.

show cs7 sami ip

To verify the ITP configuration, use the **show cs7 sami ip** command in global configuration mode.

show cs7 sami ip

Syntax Description	sami	Cisco IOS software application module that runs Cisco ITP.
Defaults	None.	
Command Modes	Global configuration	
Command History	Release	Modification
	12.2(33)IRA	This command was introduced.

Examples

The following example includes output from the **show cs7 sami ip** command:

ITP# **show cs7 sami ip**

```

SAMI Module 5
IP-Address      Mask                Vlan Sup IP
-----
209.165.202.129 255.255.255.224 12 209.165.200.253
209.165.202.131 255.255.255.224 10 209.165.200.252
209.165.202.132 255.255.255.224 3 209.165.200.251
209.165.202.133 255.255.255.224 772 209.165.200.250

IP-Net          Mask                Next Hop
-----
SAMI Module 11
IP-Address      Mask                Vlan Sup IP
-----
209.165.202.134 255.255.255.224 3 209.165.200.247
209.165.202.135 255.255.255.224 4 209.165.200.244
209.165.202.136 255.255.255.224 6 209.165.200.243
209.165.202.137 255.255.255.224 10 209.165.200.241

IP-Net          Mask                Next Hop
-----
209.165.202.140 255.255.255.224 209.165.200.240
209.165.202.141 255.255.255.224 209.165.200.239

```

[Table 70](#) describes the fields in the display.

Table 70 *show cs7 sami ip Fields Display*

Field	Description
SAMI Module	Specific SAMI module
Sup IP	IP address of supervisor module

show cs7 sccp gti-conversion

To display the CS7 GTI conversion table, use the **show cs7 sccp gti-conversion** privileged EXEC command.

show cs7 sccp gti-conversion [measurements]

Syntax Description	measurements	Displays a count of how many MSUs matched each rule in the GTI table.

Defaults	None.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	If the measurements keyword is specified, a count of how many MSUs matched each rule in the GTI table is displayed. This count is cleared by the clear cs7 all command

Examples	The following example includes output from the show cs7 sccp gti-conversion command:

```
ITP# show cs7 sccp gti-conversion
SCCP GTI Conversion Table: gti4
```

GTI	TT	SSN	NP	NAI	ES	-->	OUT-GTI	OUT-TT	OUT-SSN	OUT-NP	OUT-NAI	OUT-ES
2	10	*	-	-	-		4	11	*	1	1	2
2	250	*	-	-	-		4	34	*	1	3	2

```
SCCP GTI Conversion Table: gti2
```

```
-OUT
```

GTI	TT	SSN	NP	NAI	ES	-->	OUT-GTI	OUT-TT	OUT-SSN	OUT-NP	OUT-NAI	OUT-ES
2	250	*	-	-	-		2	0	10	-	-	-

The following example includes output from the **show cs7 sccp gti-conversion** command with the **measurements** keyword:

```
ITP# show cs7 sccp gti-conversion measurements
SCCP GTI Conversion Table: gti4
```

GTI	TT	SSN	NP	NAI	ES	-->	USED
2	10	*	-	-	-		1239
2	250	*	-	-	-		11

```
SCCP GTI Conversion Table: gti2
```

GTI	TT	SSN	NP	NAI	ES	-->	USED
2	250	*	-	-	-		187

Related Commands

Command	Description
clear cs7 all	Clears all accounting, statistics, and GTT measurements.
cs7 sccp gti-conversion	Configures a GTI conversion table.

show cs7 sccp instance-conversion

To display the CS7 SCCP instance conversion table, use the **show cs7 sccp instance-conversion** privileged EXEC command.

show cs7 sccp instance-conversion [measurements]

Syntax Description

measurements	Displays a count of how many SCCP MSUs were converted from one instance to another.

Defaults

None.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

If the **measurements** keyword is specified, a count of how many SCCP MSUs were converted from one instance to another is displayed. This count is cleared by the **clear cs7 all** command.

Examples

The following examples include output from the **show cs7 sccp instance-conversion** command:

ITP# **show cs7 sccp instance-conversion**

InInst->OutInst	GTI-CONV	SSN-CONV	ADDR-CONV	MsgHandling	NatInd
0 -> 6	test	none	none	return-on-e	0
0 -> 1	none	ssn1	none	no-chg	1
1 -> 0	none	ssn0	none	no-chg	no-chg
3 -> 4	gti4	none	addr4	no-chg	no-chg
4 -> 3	gti2	none	addr3	no-chg	no-chg

ITP# **show cs7 sccp instance-conversion measurements**

InInst->OutInst	PKTS
0 -> 6	0
0 -> 1	133393
1 -> 0	0
3 -> 4	0
4 -> 3	3934984

Related Commands

Command	Description
clear cs7 all	Clears all accounting, statistics, and GTT measurements.
cs7 sccp gti-conversion	Configures a CS7 SCCP GTT conversion table.

show cs7 sccp ssn-conversion

To display the SSN conversion table, use the **show cs7 sccp ssn-conversion** privileged EXEC command.

show cs7 sccp ssn-conversion

Syntax Description This command has no arguments or keywords.

Defaults None.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples The following example includes output from the **show cs7 sccp ssn-conversion** command:

ITP# **show cs7 sccp ssn-conversion**

SCCP SSN Conversion Table: ssn0

IN-SSN	OUT-SSN
10	250
200	20
*	200

SCCP SSN Conversion Table: ssn1

IN-SSN	OUT-SSN
250	255

Related Commands	Command	Description
	cs7 sccp ssn-conversion	Creates a subsystem mapping table.

show cs7 sgmp

To display Signaling Gateway Mate Protocol (SGMP) information, use the **show cs7 sgmp** privileged EXEC command.

show cs7 [*instance-number*] **sgmp** *local-port*

Syntax Description	<i>instance-number</i>	Specifies the instance. The valid range is 0 to 7. The default instance is 0.
	<i>local-port</i>	Local port number for SGMP link offloaded to line card.

Defaults The default instance is 0.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.
	12.2(18)IXH 12.4(15)SW3 12.2(33)IRC	Enhanced the command output to include the running SGMP version.

Examples The following example includes output from the **show cs7 sgmp** command:

```
ITP# show cs7 sgmp
SGMP Local port: 14002      State: active      SCTP instance handle: 5
Local ip address:          172.18.48.39
Number of active SGMP peers: 0
Max number of inbound streams allowed: 17
Local receive window:      5555
Max init retransmissions:   8
Max init timeout:          1000 ms
Unordered priority:         equal
Offload to FlexWAN: No      Slot: -1
SCTP defaults for new associations
  Transmit queue depth:    1000      Cumulative sack timeout: 200 ms
  Assoc retransmissions:   17        Path retransmissions:    4
  Minimum RTO:             1000 ms   Maximum RTO:            1000 ms
  Bundle status:           on        Bundle timeout:          5 ms
  Keep alive status:       true      Keep alive timeout:      500 ms
  Initial cwnd:            3000      Idle cwnd rate:          50
  Retrans cwnd rate:        50       Retrans cwnd mode:       RFC
  FastRetrans rate:        50
SGMP Offload Version: 1
```

Related Commands

Command	Description
cs7 sgmp	Establishes an association to the mated-signaling gateway and enters cs7 sgmp submode.

show cs7 sms address-table

To display SMS address table information, use the **show cs7 sms address-table** privileged EXEC command.

show cs7 sms address-table [**addr** *address*] [**name** *name*] [**prefix** *digits*]

Syntax Description		
addr		Filters on matching addresses.
<i>address</i>		Digit string.
name		Filters on address table name.
<i>name</i>		Address table name.
prefix		Filters on addresses prefixed with a specified digit string.
<i>digits</i>		Digit string.

Defaults None.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples The following example includes output from the **show cs7 sms address-table** command:

```
ITP#show cs7 sms address-table
```

```
Name: shortcodes      Instance: 0    Address Count: 4
```

Address	Matches	Result
11112*	0	GRP grp2
1111*	4000	GRP grp1
2222*	1000	GRP grp1
5551212	0	GRP grp3

[Table 71](#) describes the significant fields shown in the display.

Table 71 *show cs7 sms address-table* Field Descriptions

Field	Description
Name	Address table name.
Instance	Instance number.

Table 71 *show cs7 sms address-table Field Descriptions (continued)*

Field	Description
Address	Address as specified in the address table. The asterisk (*) indicates that longer addresses that match this prefix are considered a match.
Matches	Indicates the number of times this address has been invoked where this address matched the value in the request.
Result	Indicates the result, if specified, that will be executed when a match occurs.

Related Commands

Command	Description
cs7 sms address-table	Specifies an SMS address table.

show cs7 sms dest-sme-binding

To display SMS information about the specified dest-sme address, use the **show cs7 sms dest-sme-binding** privileged EXEC command.

show cs7 sms dest-sme-binding *dest-sme* [*result-group-name*]

Syntax Description	<i>dest-sme</i>	Specifies the dest-sme address whose result you want to display. Valid addresses are from 1 to 20 hexadecimal characters in length. Only the last four digits of the address are needed to determine the dest-sme-binding result.
	<i>result-group-name</i>	Specifies which result group to use. If <i>result-group-name</i> is not specified, then this display outputs the dest-sme-binding result for the input dest-sme for each result group in dest-sme-binding mode.

Defaults	None.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.

Examples The following example includes output from the **show cs7 sms dest-sme-binding** command:

```
ITP#show cs7 sms dest-sme-binding 12345035
Dest-sme: 12345035
Instance: 0   Result Group: SMS1
Order: 200   Result: GT 12345 tt 0 gti 4 np 1 nai 4

Dest-sme: 12345035
Instance: 0   Result Group: SMS4
Order: 100   Result: PC 5.5.5
```

Related Commands	Command	Description
	cs7 sms group	Configures an SMS result group.

show cs7 sms gsm-map

To display SMS GSM MAP transport information, use the **show cs7 sms gsm-map** privileged EXEC command.

show cs7 sms gsm-map [*ssn ssn*] [**statistics** [**detail** [**sms-mo** | **sms-mt** | **sri-sm**]]]

Syntax Description

ssn	Displays GSM MAP information for a specific subsystem.
<i>ssn</i>	Subsystem number in the range 2 to 255.
statistics	Displays SMS GSM transport statistics.
detail	Includes operation-specific statistics.
sms-mo	Displays statistics related to SMS MO proxy procedures.
sms-mt	Displays statistics related to SMS MT procedures.
sri-sm	Displays statistics related to SRI SM procedures.

Defaults

None.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Examples

The following example includes output from the **show cs7 sms gsm-map** command with the **ssn** keyword:

```
ITP#show cs7 sms gsm ssn 8
SMS GSM MAP Transport
SSN: 8
map-source-addr: use national digits 9193922900 tt 10 gti 2
Invoke Timer:    10 SMSC MAP Version:    3
```

The following example includes output from the **show cs7 sms gsm-map** command with the **statistics** and **detail** keywords:

```
ITP#show cs7 sms gsm statistics detail
GSM MAP Statistics:

Total outstanding SMS dialogues:                                0

Total SMS-MO ForwardSM indications:                            1510
  Outstanding / Max:                                           0 /      10
  Empty Begin received:                                         0
  Command TPDUs received:                                       0
  Unsupported PID                                              0
```



```

Unsupported DCS                                0
Result_last responses (successful):            1510
Return_error responses:                        0
  Unexpected data value:                       0
  System failure:                             0
  Data missing:                               0
  Facility not supported:                     0
  SM delivery failure:                        0
    invalid SME address:                      0
    unknown service centre:                   0
    service centre congestion:                 0
    subscriber not service centre sub:         0
    equipment protocol error:                  0
ABORT responses:                               0
  Procedure error:                           0
  Resource unavailable                         0
  Application procedure cancellation:           0
  Congestion:                                0

Total SMS-MO Proxy procedures initiated:        0
  Outstanding / Max:                          0 /      0
  Confirmations received:                     0
  Version Negotiations:                       0
  Errors received:                            0
  Rejects received:                           0
  Cancels received:                           0
  Notices received:                           0
  Aborts received:                            0
  Expirations:                                0
  Provisioning error:                         0
ABORT responses:                               0
  Procedure error:                           0
  Resource unavailable                         0
  Application procedure cancellation:           0
  Congestion:                                0

Total SMS-MT procedures initiated:              13214
  FDA Outstanding / Max:                      0 /      50
  Stat Report Outstanding / Max:               0 /      10
  SRI-SM Requests sent:                       13214
  SRI-SM Confirmations received:               13214
  SRI-SM Version Negotiations:                 0
  SRI-SM Errors received:                     0
  SRI-SM Rejects received:                    0
  SRI-SM Cancels received:                     0
  SRI-SM Notices received:                    0
  SRI-SM Aborts received:                     0
  MT-ForwardSM Requests sent:                  13214
  MT-ForwardSM Segmented dialogues sent:        0
  MT-ForwardSM Confirmations received:          13214
  MT-ForwardSM Version Negotiations:            0
    MSC Confirmations received:                13214
    SGSN Confirmations received:                0
  MT-ForwardSM Errors received:                 0
    MSC Errors:                               0
    SGSN Errors received:                      0
    Alternate Path Attempted:                  0
  MT-ForwardSM Rejects received:                0
    MSC Rejects:                              0
    SGSN Rejects:                             0
  MT-ForwardSM Cancels received:                0
    MSC Cancels:                              0
    SGSN Cancels:                             0
  MT-ForwardSM Notices received:                0

```

show cs7 sms gsm-map

```

MSC Notices:                                0
SGSN Notices:                              0
MT-ForwardSM Remote Aborts received:        0
MSC Aborts:                                0
SGSN Aborts:                                0
Expirations:                                0
Unknown Input:                              0
ABORT responses:                             0
  Procedure error:                           0
  Resource unavailable                         0
  Application procedure cancellation:          0
  Congestion:                                0

Origin IMSI Retrieval procedures initiated: 1510
Outstanding / Max:                           0 /      0
Origin IMSI already known:                   1510
SRI-SM Requests sent:                        0
SRI-SM Confirmations received:               0
SRI-SM Version Negotiations:                 0
SRI-SM Errors received:                      0
SRI-SM Rejects received:                     0
SRI-SM Cancels received:                     0
SRI-SM Notices received:                     0
SRI-SM Aborts received:                      0

Remote U-ABORT indications:                  0
Remote P-ABORT indications:                  0
Local U-ABORT indications:                   0
Local P-ABORT indications:                   0
Local Cancel indications:                    0
Notice indications:                          0

```

Related Commands

Command	Description
cs7 sms gsm-map	Specifies the GSM transport for the SMS subsystem.

show cs7 sms group

To display SMS routing group information, use the **show cs7 sms group** privileged EXEC command.

show cs7 sms group *name*

Syntax Description	<i>name</i>	SMS group name.

Defaults	None.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples

The following example includes output from the **show cs7 sms group** command:

ITP# **show cs7 sms group proxy**

Instance: 0 Group: proxy Type: smsc
Protocol: ansi-41 Mode: broadcast

Result	Status	Weight	Matches
PC 1.5.5 ssn 11	avail	1	4700
PC 2.40.0 ssn 11	avail	1	4700
PC 2.40.0 ssn 12	avail	1	4700
PC 1.5.5 ssn 8	unav	1	4700
GT 1111111 tt 10 gti 2	avail	1	4700
GT 2222222 tt 10 gti 2	avail	1	4700

[Table 72](#) describes the significant fields shown in the display.

Table 72 **show cs7 sms group Field Descriptions**

Field	Description
Result	Describes the result group member.
Weight	Weight assigned to the result group member for weighted round robin load-balancing purposes.
Matches	Number of times this result group member has been chosen for routing.

Related Commands	Command	Description
	cs7 sms group	Specifies an SMS result group.

show cs7 sms route-table

To display attributes of the SMS route table, use the **show cs7 sms route-table** privileged EXEC command.

show cs7 [*instance-number*] **sms route-table** [**gsm-map** [*sms-mo*]]

Syntax Description

<i>instance-number</i>	Specifies the instance. The valid range is 0 to 7. The default instance is 0.
gsm-map	Displays information regarding handling of inbound GSM MAP messages.
sms-mo	Displays information regarding handling of inbound SMS MO operations.

Defaults

The default instance is 0.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The only currently supported protocol-operation-correlation filter is gsm-map/sms-mo.

Examples

The following examples include output from the **show cs7 sms route-table** command with no keywords:

ITP# **show cs7 sms route-table**

SMS Route-table

Transaction-timer: 60

Traffic-rate-timer: 60 CDR-Service: pds

Protocol: ansi41 Operation: smsNot

Ruleset: proxy Status: Enabled

ITP# **show cs7 sms route-table**

SMS Route-table

Transaction-timer: 0

Traffic-rate-timer: 60 CDR-Service: pds

Protocol: gsm-map Operation: sms-mo

Ruleset: smsc-rules Status: Enabled

Proxy-error-use: True Max-messages: 2500

Modify Prefix: Dest-sme * Ton:0 Np:1

Result ton 1

Result np 3

Protocol: ucp Operation: submit-sm

Ruleset: ao-rules Status: Enabled

The following example includes output from the **show cs7 sms route-table** command with the **gsm-map** and **sms-mo** keywords:

```
ITP# show cs7 sms route-table gsm-map sms-mo
SMS Route-table
Transaction-timer: 300          CDR-Service: pds

Protocol:          gsm-map Operation:  sms-mo Correlator: SSN 8
Ruleset:           smsc-rules Status: Enabled
map-source-addr:   use national digits 9193923943 tt 10 gti 2
Invoke Timer:      30 Max-messages:    0
SMSC MAP Version:  3 Proxy-error-use: True
MNP Primary TT:    11 Secondary TT:    10
GPRS Delivery:     Prefer MSC
```

Table 73 describes the significant fields shown in the display.

Table 73 *show cs7 sms route-table Field Descriptions*

Field	Description
Transaction-timer: 300	Displays the configured maximum lifetime of a message transaction in seconds.
CDR-Service: pds	Displays the name of the CDR service used by the SMS routing subsystem.
Protocol: gsm-map	Identifies the protocol routing instance. Currently, only gsm-map is supported.
Operation: sms-mo	Identifies the SMS MO operation.
Correlator: SSN 8	Identifies the subsystem number.
Ruleset: smsc-rules	Identifies the configured SMS ruleset name.
Status: enabled	Indicates that the protocol is enabled.
map-source-addr	Identifies the address used as the calling party address for all MAP-generated messages.
Invoke Timer	Indicates the timer value, in seconds, configured to supervise initiated dialogs.
Max-messages	Indicates the maximum number of open SMS MO messages allowed before a congestion response is generated.
SMSC MAP Version	Indicates the SMSC MAP version.
Proxy-error-use: True	Specifies to return the error received from the last MO Proxy procedure.
MNP Primary TT	Identifies the primary tt in the SCCP called party address used to send all SRI-SM messages to the HLR.
Secondary TT	Identifies the secondary tt, to be used to send a second request if the response to a message sent with the MNP primary tt contains the error "Unknown Subscriber."
GPRS Delivery	Indicates that DSMR will attempt SMS MT delivery to the SGSN address when the HLR provides both MSC and SGSN addresses in an SRI confirmation.

Related Commands

 show cs7 sms route-table

Command	Description
cs7 sms route-table	Configures an SMS route table.

show cs7 sms ruleset

To display the attributes of a configured SMS ruleset, use the **show cs7 sms ruleset** privileged EXEC command.

show cs7 sms ruleset [*name ruleset-name*] [**detail** | **result-summary** | **rule-summary**]

Syntax Description	name	Specifies a ruleset name.
	<i>ruleset-name</i>	Ruleset name.
	detail	Displays detailed SMS ruleset information.
	result-summary	Displays a summary of the results within an SMS ruleset.
	rule-summary	Displays a summary of the rules within an SMS ruleset.

Defaults The default display is **result-summary** mode.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples The following example includes output from the **show cs7 sms ruleset** command filtered on ruleset **name** PROXY and no other keyword. The default display is **result-summary** mode.

```
itp#show cs7 sms ruleset name proxy
Name: proxy          Instance:0  Protocol: n/a

Rule Result                                Rule    Rule    Result
Checked   Matches   Successful
-----
10  GRP proxy                                4700    4700    4700
```

The following example includes output from the **show cs7 sms ruleset** command filtered on ruleset **name** SMS-RULES2 and no other keyword. The default display is **result-summary** mode.

```
ITP#show cs7 sms ruleset name SMS-RULES2
Name: SMS-RULES2     Instance:0  Protocol: n/a

Rule Result                                Rule    Rule    Result
Checked   Matches   Successful
-----
100  GT 123 tt 12  gti 2                                0        0        0
250  BLOCK                                0        0        0
480  GT 123456789123456 tt 0  gti 4 np 4  nai 0        0        0
```

The following example includes output from the **show cs7 sms ruleset** command filtered on ruleset **name SMS-RULES2** and displayed in **rule-summary** mode:

```
ITP#show cs7 sms ruleset name SMS-RULES2 rule-summary
```

```
Name: SMS-RULES2 Instance:0 Protocol: n/a
```

Rule	Oper	dest-sme	orig-sme	More Param	Rule Matches
100	sms-mo	123*	1234	+	0
250	sms-mo	*	*	+	0
480	sms-mo	12345678901234567890	1234567891234567*	+	0

The following example includes output from the **show cs7 sms ruleset** command filtered on ruleset **name SMS-RULES2** and displayed in **detail** mode:

```
ITP#show cs7 sms ruleset name SMS-RULES2 detail
```

```
Name: SMS-RULES2 Instance:0 Protocol: n/a
```

```
-----
Rule      : 100      Protocol: gsm-map
Rule Checked Count      :      0
Rule Matched Count      :      0
Result Successful Count :      0
CDR Service Queue      : -
Operation : sms-mo
Parameters:
  Destination SME : 123*      Noa:0 Np:0
  Origination SME : 1234      Noa:5 Np:2
  Destination SMSC: 12345*    MinDigits:6 MaxDigits:10 Noa:0 Np:0
  Origin IMSI      : 123*
  Protocol ID      : 35
  Destination Port: 30
Result      : GT 123 tt 12 gti 2

Rule      : 250      Protocol: gsm-map
Rule Checked Count      :      0
Rule Matched Count      :      0
Result Successful Count :      0
CDR Service Queue      : -
Operation : sms-mo
Parameters:
  Destination SME : -
  Origination SME : -
  Destination SMSC: -
  Origin IMSI      : 123456
  Protocol ID      : -
  Destination Port: -
Result      : BLOCK

Rule      : 480      Protocol: gsm-map
Rule Checked Count      :      0
Rule Matched Count      :      0
Result Successful Count :      0
CDR Service Queue      : unavailable
Operation : sms-mo
Parameters:
  Destination SME : 12345678901234567890* MinDigits:20 MaxDigits:20 Noa:0 Np:4
  Origination SME : 1234567891234567*      MinDigits:16 MaxDigits:16 Noa:0 Np:4
  Destination SMSC: 1234567891234567*      MinDigits:16 MaxDigits:16 Noa:0 Np:4
  Origin IMSI      : 1234567891234567*      MinDigits:16 MaxDigits:16
  Protocol ID      : 254
  Destination Port: 65534
Result      : GT 123456789123456 tt 0 gti 4 np 4 nai 0
```


Table 74 describes the significant fields shown in the display.

Table 74 *show cs7 sms ruleset Field Descriptions*

Field	Description
Name	Ruleset name
Instance	Instance number
Protocol	Protocol
Rule	Rule number
Result	Configured result for this rule
Oper	Operator
dest-sme	Destination SME
orig-sme	Originating SME
More Param	Configuration includes more parameters (the detail keyword shows the entire configuration)
Rule Checked Count	Number of rules that were checked
Rule Matched Count	Number of rules that were matched
Result Success Count	Number of times the configured result was successfully used
Operation	SMS-MO
Parameters	Configured parameters

Related Commands

Command	Description
cs7 sms ruleset	Specifies a name and an application layer protocol for the ruleset.

show cs7 sms statistics

To display SMS statistics, use the **show cs7 sms statistics** privileged EXEC command.

show cs7 sms statistics [**detail** | **rate**]

Syntax Description	detail	Includes detailed statistics.
	rate	Displays traffic rate information for the previous collection interval.

Defaults	None.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples The following example includes output from the **show cs7 sms statistics** command with no keywords:

```
ITP# show cs7 sms statistics
CS7 SMS Routing Statistics
```

```
Instance: 0
```

```
Total routing requests received:          60857
  from GSM:                               5791
  from IS-41:                             0
  from UCP:                               55066
  from SMPP:                              0
```

```
Total routing requests completed:         60857
  Successfully delivered:                 60856
    Delivered via SMPP:                   0
    Delivered via UCP:                    0
    Delivered via GSM:                    60856
    Deferred via GSM:                     0
    Status Reports sent via GSM:           5791
    Notifications sent via UCP:            55066
    Delivery Receipts sent via SMPP:       0
    Notifications proxied via ANSI-41:     0
  Error/aborted/not delivered:            1
    Routing not configured:                0
    No result succeeded:                   1
    Internal error:                        0
    Parse/receive error:                   0
    Resource shortage:                     0
    Provisioning error:                    0
    Destination not reachable:             0
    Destination signaled error:            0
```

```

Timed out:          0
Blocked:            0

```

The following example includes output from the **show cs7 sms statistics** command with the **rate** keyword:

```

ITP# show cs7 sms statistics rate
CS7 SMS Traffic Rate          Per second  Raw count  Highwater
-----
Instance: 0

Total routing requests received:      74      4474      74
  from GSM:                          9       590      10
  from IS-41:                        0        0        0
  from UCP:                          64     3884      64
  from SMPP:                         0        0        0

Total routing requests completed:     74     4481      74
  Successfully delivered:             74     4481      74
    Delivered via SMPP:               0        0        0
    Delivered via UCP:                0        0        0
    Delivered via GSM:               74     4481      74
    Deferred via GSM:                 0        0        0
    Status Reports sent via GSM:      10       600      10
    Notifications sent via UCP:       64     3882      64
    Del. Receipts sent via SMPP:      0        0        0
    Notifs proxied via ANSI-41:       0        0        0
  Error/aborted/not delivered:         0        0        0
    Routing not configured:           0        0        0
    No result succeeded:              0        0        0
    Internal error:                   0        0        0
    Parse/receive error:              0        0        0
    Resource shortage:                0        0        0
    Provisioning error:               0        0        0
    Destination not reachable:        0        0        0

```

Related Commands

Command	Description
traffic-rate-timer	Configures the data collection interval used to calculate traffic rate information.

show cs7 sua

To display SUA node information, use the **show cs7 sua** privileged EXEC command.

show cs7 [*instance-number*] **sua** *local-port*

Syntax Description	<i>instance-number</i>	Specifies the instance. Valid range is 0 to 7. The default instance is 0.
	<i>local-port</i>	SUA local port number. Valid range is 4096 to 32767.

Defaults The default instance is 0.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples The following example includes output from the **show cs7 sua** command. This SUA instance is offloaded to the line card in slot 6.

This SUA version uses SIGTRAN SUA draft version 15.

This SUA instance (local port 6000) is active. The instance handle (2) can be used in **show ip sctp** commands.

```
ITP# show cs7 sua 6000
Sigtran SUA draft version: 15
```

```
SUA Local port: 6000          State: active          Sctp instance handle: 2
Local ip address:              10.10.20.3
Number of active SUA peers:    0
Max number of inbound streams allowed: 17
Local receive window:         64000
Max init retransmissions:     8
Max init timeout:              1000 ms
Unordered priority:            equal
Offload to FlexWAN:           Yes   Slot: 6

Sctp defaults for new associations
Transmit queue depth: 1000          Cumulative sack timeout: 200 ms
Assoc retransmissions: 10           Path retransmissions: 4
Minimum RTO: 1000 ms               Maximum RTO: 1000 ms
Bundle status: on                   Bundle timeout: 5 ms
Keep alive status: true             Keep alive timeout: 30000 ms
Initial cwnd: 1234567               Idle cwnd rate: 50
Retrans cwnd rate: 30                Retrans cwnd mode: RFC
FastRetrans cwnd rate: 10
```

Related Commands

Command	Description
cs7 sua	Specifies the local port number for SUA and enters cs7 sua submode.
show tech-support	Collects and displays a large amount of ITP configuration information that can be used for troubleshooting.

show cs7 tcap

To display CS7 TCAP information, use the **show cs7 tcap** privileged EXEC command.

show cs7 tcap [**statistics** | **transactions**]

Syntax Description	statistics	Displays TCAP statistics.
	transactions	Displays outstanding TCAP transaction information.

Defaults	None.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples The following example includes output from the **show cs7 tcap** command with the no keywords:

```
ITP# show cs7 tcap
TCAP protocol layer is up
TCAP variant is ANSI
  554600 bytes input, 1969300 bytes output
  0 active transactions/dialogues
  42300 transaction/dialogue requests
  23500 transaction/dialogue indications
  0 total error conditions detected
New transaction work queue is not congested: depth 0
  0 P-ABORTs sent due to queue backlog
  0 BEGINS dropped due to queue backlog
```

Related Commands	Command	Description
	clear cs7 tcap statistics	Clears CS7 TCAP measurements.
	cs7 tcap tid-timer	Sets the minimum expiration time for TCAP transactions.

show cs7 version

To display the ITP version that is running on the Supervisor and on all the line cards on the system, use the **show cs7 version** EXEC command.

show cs7 version

Syntax Description This command has no arguments or keywords.

Defaults None.

Command Modes EXEC

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples The following example includes output from the **show cs7 version** command:

```
ITP#show cs7 version
CS7 Version
-----
      Major      Minor
Sup          1         2
Peer Sup      1         1
LC 1          1         2
LC 2          1         1
LC 3          1         1
```

[Table 75](#) describes the fields in the display.

Table 75 *show cs7 version Field Descriptions*

Field	Description
Major	Major version
Minor	Minor version
Sup	Supervisor
Peer Sup	[as different from Sup?]
LC	Line card

Related Commands	Command	Description
	show tech-support	Collects and displays a large amount of ITP configuration information [that can be used for troubleshooting?].

show cs7 virtual-linkset

To display information about virtual linksets, including link utilization and associated measurements, use the **show cs7 virtual-linkset** privileged EXEC command.

show cs7 virtual-linkset [*linkset-name*] [**brief**] [**routes**] [**statistics**] | [**utilization**]

Syntax Description	<i>linkset-name</i>	Displays information about a specific linkset.
	brief	Displays output in brief format. Does not display individual links.
	routes	Displays all routes using the linkset.
	statistics	Displays link usage statistics.
	utilization	Displays link utilization for the linkset.

Defaults None.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines A virtual linkset is a connection from one instance to another. In ITP, any two instances have two virtual linksets between them. For example, between instanceX and instanceY are virtual linksets VirtualLSx-y and VirtualLSy-x. VirtualLSx-y appears to be a linkset in Instance x, and it will appear in Instance x's route table for alias destinations whose true point code exists in Instance y. VirtualLSy-x appears to be a linkset in Instance y, and it will appear in Instance y's route table for alias destinations whose true point code exists in Instance x.

Virtual linksets are not the same as real linksets. Virtual linksets do not have queues, and are not limited by bandwidth.

Virtual linksets are created automatically when a new instance is created. When an alias point code is defined, the alias point code is automatically entered in the alias instance's routing table using the virtual linkset.

Examples The following example includes partial output from the **show cs7 virtual-linkset** command with no keywords:

```
ITP# show cs7 virtual-linkset
lsn=VirtualLS1-0      apc=0.30.1:0      state=avail      avail/links=1/1
  SLC  Interface      Service  PeerState      Inhib
   00   Virtual      avail    -----      ----

lsn=VirtualLS0-1      apc=1.30.1:1      state=avail      avail/links=1/1
```

show cs7 virtual-linkset

SLC	Interface	Service	PeerState	Inhib
00	Virtual	avail	-----	----

The following example includes output from the **show cs7 virtual-linkset** command with the **brief** keyword:

```
ITP# show cs7 virtual-linkset brief
lsn=VirtualLS1-0      apc=0.30.1:0      state=avail      avail/links=1/1
lsn=VirtualLS3-0      apc=0.30.1:0      state=avail      avail/links=1/1
lsn=VirtualLS0-1      apc=1.30.1:1      state=avail      avail/links=1/1
lsn=VirtualLS3-1      apc=1.30.1:1      state=avail      avail/links=1/1
lsn=VirtualLS0-3      apc=3.30.1:3      state=avail      avail/links=1/1
lsn=VirtualLS1-3      apc=3.30.1:3      state=avail      avail/links=1/1
```

The following example includes output from the **show cs7 virtual-linkset** command with the **routes** keyword:

```
ITP# show cs7 virtual-linkset routes
lsn=VirtualLS1-0      apc=0.30.1:0      state=avail      avail/links=1/1
Destination           Cong Prio QoS Route  Route Table
-----
0.1.1/24              acces          1      avail  system1

lsn=VirtualLS3-0      apc=0.30.1:0      state=avail      avail/links=1/1
Destination           Cong Prio QoS Route  Route Table
-----
0.1.2/14              acces          1      avail  system3

lsn=VirtualLS0-1      apc=1.30.1:1      state=avail      avail/links=1/1
Destination           Cong Prio QoS Route  Route Table
-----
1.2.1/24              acces          1      avail  system

lsn=VirtualLS3-1      apc=1.30.1:1      state=avail      avail/links=1/1
Destination           Cong Prio QoS Route  Route Table
-----

lsn=VirtualLS0-3      apc=3.30.1:3      state=avail      avail/links=1/1
Destination           Cong Prio QoS Route  Route Table
-----
3.2.1/24              acces          1      avail  system

lsn=VirtualLS1-3      apc=3.30.1:3      state=avail      avail/links=1/1
Destination           Cong Prio QoS Route  Route Table
-----
```

The following example includes output from the **show cs7 virtual-linkset** command with the **statistics** keyword:

```
ITP# show cs7 virtual-linkset VirtualLS0-1 statistics
lsn=VirtualLS0-1      apc=1.30.1:1      state=avail      avail/links=1/1
SLC      MSU In      MSU Out Drops  LSSU In  LSSU Out  ByteCnt In  ByteCnt Out
00              0              0      0              0              0              0              0
```

The following example includes output from the **show cs7 virtual-linkset** command with the **utilization** keyword:

```

ITP# show cs7 virtual-linkset VirtualLS0-1 utilization
Sample Interval(seconds):61/7  Thresholds onset/abate:40/30
lsn=VirtualLS0-1      apc=1.30.1:1      state=avail      avail/links=1/1
  Link Utilization Thresholds Plan-capacity      Kbps      Cong
  SLC  Rec  Sent  Rec  Sent  Rec  Sent      Rec  Sent  Lvl
    0   0   0   40   40  256  256   0    0    0
  all   0   0   ---  ---  256  256   0    0    ---

```

Table 76 describes the fields shown in the display.

Table 76 *show cs7 virtual-linkset Field Descriptions*

Field	Description
lsn=VirtualLS1-0	Linkset name; in this example, a virtual linkset from instance 1 to instance 0.
apc=0.30.1:0	Adjacent point code. This point code is the alias point code, 0.30.1 instance 0.
state=avail	State of the virtual linkset; in this example, available. Allowed states are avail and UNAVAIL. The virtual linkset is unavailable when all real linksets to instance are down.
avail/links=1/1	Number of links available in the virtual linkset. A virtual linkset contains only 1 virtual link. In this example, the link is available.
SLC	Signal Link Code. Valid range is 0 to 15.
Interface	Interface type. This interface is a virtual interface.
Service	Status of the service. In this example, the service is available. Allowed states are avail and UNAVAIL.
PeerState	This field is always blank.
Inhib	This field is always blank. No inhibit commands for virtual linksets.

Related Commands

Command	Description
cs7 instance pc-conversion	Enables instance translation, creating a virtual link between the instance of the real point code and the instance of the alias point code.
show cs7 pc-conversion	Displays a mapping of real to alias point codes.

show hosts

To display information about a host, use the **show hosts** privileged EXEC command.

show hosts

Syntax Description This command has no arguments or keywords.

Defaults None.

Command Modes Privileged EXEC

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Examples

The following example includes output from the **show hosts** command:

```
ITP# show hosts
Default domain is not set
Name/address lookup uses static mappings

Codes: u - unknown, e - expired, * - OK, ? - revalidate
        t - temporary, p - permanent

  Port St Host                Age  Type    Address(es)
* NA   p bologna              **   SS7     5121
* None p topsail              **   IP      172.18.44.155
```

```
ITP# show hosts
Default domain is not set
Name/address lookup uses static mappings

Codes: u - unknown, e - expired, * - OK, ? - revalidate
        t - temporary, p - permanent

  Port St Host                Age  Type    Address(es)
* NA   p bari                 0    SS7     1.1.1.1
          1234:0
* NA   p bologna              0    SS7     5121:0
* None p topsail              41   IP      172.18.44.155
```

```
ITP# show cs7 route
Dynamic Routes 0 of 500 with 0 drops

Routing table = system Destinations = 5 Routes = 5
Instance = 0
Destination          Prio Linkset Name      Route
```

```

-----
666/14          INACC  1  one          UNAVAIL
bari            INACC  5  one          UNAVAIL
bologna         INACC  5  one          UNAVAIL
5120/11         INACC  5  one          UNAVAIL
5221/14         INACC  5  one          UNAVAIL

```

Dynamic Routes 0 of 500 with 0 drops

Routing table = system1 Destinations = 2 Routes = 2

Instance = 1

```

Destination          Prio Linkset Name      Route
-----
bari                  INACC  5  two          UNAVAIL
3.3.3/24              INACC  1  two          UNAVAIL

```

Related Commands

Command	Description
cs7 host	Maps a hostname to a point code.

show ip sctp

To display ITP SCTP statistics, use the **show ip sctp** EXEC command.

show ip sctp { **association** [**list** | **parameters** *assoc-id* | **statistics** *assoc-id*] | **errors** | **instances** *local-port* | **statistics** }

Syntax Description

association	Specifies an SCTP connection.
list	Current SCTP association.
parameters	SCTP association parameters.
<i>assoc-id</i>	Association ID number. Valid range is 0 to 1024.
statistics	SCTP association statistics.
errors	SCTP error statistics.
instances	SCTP local peer instances.
statistics	SCTP internal statistics.

Defaults

None.

Command Modes

EXEC

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Examples

This section shows sample output from various forms of the **show ip sctp** command. Each example is followed by a table describing the fields in the output display.

The following example includes output from the **show ip sctp** command using the **association** and **list** keywords:

```
ITP# show ip sctp association list
** SCTP Association List **

AssocID:0, Instance ID:0x30010043
Current state:ESTABLISHED, uptime:00:21:24
Local port:9000, Addrs:172.18.44.162
Remote port:9000, Addrs:172.18.44.170
```

[Table 77](#) describes the fields in the **show ip sctp association list** display.

Table 77 *show ip sctp association list Field Descriptions*

Field	Description
AssocID	SCTP association identifier.
Current state	State of SCTP association.
uptime	Duration of time association has been active.
Local Port	Local port number
Addrs	Local or remote peer addresses
Remote Port	Remote port number

The following example includes output from the **show ip sctp** command using the **association** and **parameters** keywords with *assoc-id* 0:

```
ITP# show ip sctp association parameters 0

** SCTP Association Parameters **

AssocID:0 Context:2167490164 InstanceID:0
Assoc state:ESTABLISHED Uptime:07:10:58
Local port:9000
Local addresses:172.18.44.162

Remote port:9000
Primary dest addr:172.18.44.170
Effective primary dest addr:172.18.44.170
Destination addresses:

172.18.44.170: State: ACTIVE
Heartbeats: Enabled Timeout:30000 ms
RTO/RTT/SRTT:1000/0/0 ms TOS:0 MTU:1500
cwnd:3000 ssthresh:64000 outstand:0
Num retrans:0 Max retrans:4 Num times failed:0

Local vertag:E170819 Remote vertag:5A3F8A70
Num inbound streams:2 outbound streams:2
Max assoc retrans:10 Max init retrans:8
CumSack timeout:200 ms Bundle timeout:5 ms
Min RTO:1000 ms Max RTO:1000 ms
LocalRwnd:64000 Low:63982 RemoteRwnd:64000 Low:63980
Congest levels:4 current level:0 high mark:2
```

[Table 78](#) describes the fields in the **show ip sctp association parameters** display.

Table 78 *show ip sctp association parameters Field Descriptions*

Field	Description
AssocID	SCTP association ID
Context	Internal upper layer handle
InstanceID	Instance ID
Assoc state	SCTP association state
Uptime	Duration of time association active
Local port	Local port number

Table 78 *show ip sctp association parameters Field Descriptions (continued)*

Field	Description
Local addresses	Local IP addresses
Remote port	Remote port number
Primary dest addr	Primary destination address
Effective primary dest addr	Current primary destination address
Heartbeats	Status of hearbeats
Timeout	Heartbeat timeout
RTO/RTT/SRTT	Retransmission timeout/Round trip time/Smoothed round trip time
TOS	IP precedence setting
Cwnd	Congestion window
Ssthresh	Slow start threshold
Outstand	Number of outstanding bytes
Num inbound streams	Maximum inbound streams
Outbound streams	Maximum outbound streams
LocalRwnd/Low	Local receive window/Lowest local receive window reported
RemoteRwnd/Low	Remote receive window/Lowest remote receive window reported
Current level/high mark	Current congestion level/Highest number of packets queued

The following example includes output from the **show ip sctp** command using the **association** and **statistics** keywords with *assoc-id* 0:

```
ITP# show ip sctp association statistics 0
```

```
** Sctp Association Statistics **
```

```
AssocID/InstanceID:0/0
Current State:ESTABLISHED
Control Chunks
  Sent:3574  Rcvd:2717
Data Chunks Sent
  Total:875  Retransmitted:0
  Ordered:875  Unordered:0
  Avg bundled:0  Total Bytes:15740
Data Chunks Rcvd
  Total:1456  Discarded:0
  Ordered:1456  Unordered:0
  Avg bundled:1  Total Bytes:25615
  Out of Seq TSN:0
ULP Dgrams
  Sent:875  Ready:1456  Rcvd:1456
DataGrams Sent:3854  DataGrams Rcvd:1454
RexmitTO:0  RexmitFAST:0
```

[Table 79](#) describes the fields in the **show ip sctp association statistics** display.

Table 79 *show ip sctp association statistics Field Descriptions*

Field	Description
AssocID/InstanceID	Association and instance IDs
Current State	SCTP association state
Control Chunks	SCTP control chunks send/receive
Data Chunks Sent	SCTP data chunks sent
Data Chunks Rcvd	SCTP data chunks received
ULP Dgrams	Number of datagrams sent/received by Upper Layer Protocol
DataGrams Sent/Rcvd	Total number of datagrams sent/received
RexmitTO	Retransmits due to retransmission timer timeout
RexmitFast	Retransmits due to fast retransmit

The following example includes output from the **show ip sctp** command using the **errors** keyword:

```
ITP# show ip sctp errors
```

```
** Sctp Error Statistics **
```

```

Not Ready:                               1
Rcvd Dgram too small:                    272
Invalid verification tag:                 30
Rcvd dgram unconfig local addr:          30
Out-of-the-blue dgrams:                  7716072
Communication Lost:                       463
Destination Address Failed:              481
Unknown INIT params rcvd                 480
Peer restarted:                           69
No Listening instance:                     2608

```

Table 80 describes all possible fields of the **show ip sctp errors** output. In actual output, each field includes a value that represents the number of times the error has occurred since errors were last cleared.

Table 80 *show ip sctp errors Field Descriptions*

Field	Description
Not Ready	SCTP is not initialized.
Memory Unavail	No memory available.
Attempt to Free Null Ptr	Attempt to free a null pointer.
Attempt to Free Not In Use	Attempt to free memory that is not in use.
Rcvd Dgram too small	Received datagram length is invalid; too small.
Partial chunk rcvd	Received datagram contains a partial chunk.
Dgram with no chunks	Received datagram does not contain any chunks.
Invalid Adler checksum	Adler checksum of received datagram is invalid.
Invalid Crc32 checksum	CRC32 checksum of received datagram is invalid.
Invalid bundled chunks	Received datagram contains chunks that cannot be bundled together.
Invalid verification tag	Received datagram contains invalid verification tag.
Rcvd dgram unconfig local addr	Received a datagram with an unconfigured local address.
Out-of-the-blue dgrams	Received an unexpected datagram based on state of the association.
Invalid stream rcvd	Received chunk has invalid stream number.
Unknown Appl Req type	Unknown internal application request.
Communication Lost	Association failed because communication was lost to peer.
Destination Address Failed	Destination address marked unreachable due to max number retries.
Unknown INIT params rcvd	Unknown parameter field found in Init or Init-Ack chunk
Null Timer Id specified	Invalid timer ID. Internal error
Unknown Timer type expired	Unknown timer expiration. Internal error.
Chunk ordering errors	Chunks received in datagram are out of order as specified in RFC.
ECNE chunk type rcvd	Explicit congestion notification echo chunk received.
CWR chunk type rcvd	Congestion window reduced chunk received.
Unknown chunk type rcvd	Unknown chunk type detected in received datagram.
Unknown Init params rcvd	Unknown parameter field found in Init or Init-Ack chunk.
Invalid cookie signature	Invalid cookie signature computed.
Expired cookie	Cookie lifetime expired. Cookie is invalid.
Peer restarted	Received cookie chunk while association was already established.
Incoming assoc disallowed	Association denied because port instance is being deleted.
No Listening Instance	No port instance found for incoming datagram.
Invalid linktype rcvd	Received datagram link type is not IP.
IPv6 addr params rcvd	IPv6 parameters received in Init or Init-Ack chunks.
Invalid stream error rcvd	Invalid stream error cause received in error chunk.

Table 80 *show ip sctp errors Field Descriptions*

Field	Description
Missing param error rcvd	Missing parameter error cause received in error chunk.
Stale cookie error rcvd	Stale cookie error cause received in error chunk.
Out of resource error rcvd	Out of resource error cause received in error chunk.
Unresolvable addr err rcvd	Unresolved address error cause received in error chunk.
Unrecognized chunk err rcvd	Unrecognized error type received in error chunk.
Invalid param err rcvd	Invalid mandatory parameter error cause received in error chunk.
Unrecognized param err rcvd	Unrecognized parameter error cause received in error chunk.
No user data error rcvd	No user data error cause received in error chunk.
Cookie in shutdown err rcvd	Cookie received while shutting down error cause received in error chunk.
Chunk too small	Received chunk is too small.
Chunk too large	Received chunk is too large.
Missing parameters	Parameter missing from received chunk.
No room for incoming data	Local receive window is full.
Low IO memory	I/O memory is low. Packets are dropped.

The following example includes output from the **show ip sctp** command using the **instances** keyword:

```
ITP# show ip sctp instances

** SCTP Instances **

Instance ID:9000 Local port:9000
Instance state:available
Local addrs:172.18.44.162
Default streams inbound:2 outbound:2
Current associations: (max allowed:100)
  AssocID:0 State:ESTABLISHED Remote port:9000
    Dest addrs:172.18.44.170
```

[Table 81](#) describes the fields in the **show ip sctp instances** display.

Table 81 *show ip sctp instances Field Descriptions*

Field	Description
Instance ID	CTP instance ID, which is equal to the local port number
Local Port	Local port number
Instance state	SCTP instance state
Local Addrs	Local IP address
Default streams	Default inbound and outbound streams
Current Associations	Current SCTP associations

The following example includes output from the **show ip sctp** command using the **statistics** keyword:

```
ITP# show ip sctp statistics
```

show ip sctp

```

** Sctp Overall Statistics **
Total Chunks Sent:          5359
Total Chunks Rcvd:         4491
Received Ordered Data Chunks: 1549
Received UnOrdered Data Chunks:0
Total Data Chunks Sent:    1009
Total Data Chunks Rcvd:    1549
Total Data Bytes Sent:     18085
Total Data Bytes Rcvd:     27407
Total Data Chunks Discarded: 6
Total Data Chunks Retrans: 12

Total Sctp Datagrams Sent:  4237
Total Sctp Datagrams Rcvd:  4134
Total ULP Datagrams Sent:   954
Total ULP Datagrams Ready:  1549
Total ULP Datagrams Rcvd:   1549

```

Table 82 describes the fields in the **show ip sctp statistics** display.

Table 82 *show ip sctp statistics Field Descriptions*

Field	Description
Total Chunks Sent	Total chunks sent
Total Chunks Rcvd	Total chunks received
Received Ordered Data Chunks	Number of ordered data chunks received
Received UnOrdered Data Chunks	Number of unordered data chunks received
Total Data Chunks Sent	Total number of data chunks sent
Total Data Chunks Rcvd	Total number of data chunks received
Total Data Bytes Sent	Total data bytes sent
Total Data Bytes Rcvd	Total data bytes received
Total Data Chunks Discarded	Total data chunks discarded
Total Data Chunks Retrans	Total data chunks retransmitted
Total Sctp Datagrams Sent	Total Sctp datagrams sent
Total Sctp Datagrams Rcvd	Total Sctp datagrams received
Total ULP Datagrams Sent	Total Upper Layer Protocol datagrams sent
Total ULP Datagrams Ready	Total Upper Layer Protocol datagrams ready
Total ULP Datagrams Rcvd	Total Upper Layer Protocol datagrams received

show ip sctp association appl-name dead

To display Sctp monitor measurements for those associations that have failed, use the **show ip sctp association appl-name dead EXEC** command.

show ip sctp association appl-name dead

Syntax Description	appl-name	Application name.
	dead	Failed state.

Defaults	None.

Command Modes	EXEC

Command History	Release	Modification
	12.2(18)IXH	This command was introduced.
	12.4(15)SW3	
	12.2(33)IRC	

Examples This example includes output from the **show ip sctp association appl-name dead** command:

```
Router# show ip sctp association appl-name dead
```

```
** Sctp Association List Total: 4 active: 4 dead: 0 **
```

Application Name	AssocID	State
to-RTP:0	0x00010001	FAILED
to-CRDC:1	0x00010002	FAILED

Related Commands	Command	Description
	clear ip sctp statistics	Resets all Sctp global counters and clears counters for all Sctp associations.
	clear ip sctp association	Clears the errors, statistics, and monitor values for the specified Sctp association.

show ip sctp association monitor

To display the SCTP association history monitor data graph, use the **show ip sctp association monitor EXEC** command.

```
show ip sctp association monitor [ assoc-id ] [ all | application | cwnd-hw | cwnd-lw | dup-chunks
| fast-retrans | octets-rx | octets-tx | oor-chunks | packets-rx | packets-tx | rto | rtt-avg |
rtt-max | rwnd-local-hw | rwnd-local-lw | rwnd-remote-hw | rwnd-remote-lw | ulpd-hw |
ulpd-lw ]
```

Syntax Description

<i>assoc-id</i>	Association ID number. Valid range is 0 to 1024.
all	Displays all measurement history.
application	Displays application-processing history.
cwnd-hw	Displays congestion window high-mark history.
cwnd-lw	Displays congestion window low-mark history.
dup-chunks	Displays duplicate-chunks history.
fast-retrans	Displays fast-retransmission history.
octets-rx	Displays octet received history.
octets-tx	Displays octet sent history.
oor-chunks	Displays out-of-order chunks history.
packets-rx	Displays packet received history.
packets-tx	Displays packet sent history.
rto	Displays retransmission timeout history.
rtt-avg	Displays round-trip-time average history.
rtt-max	Displays round-trip-time maximum history.
rwnd-local-hw	Displays local receive window high-mark history.
rwnd-local-lw	Displays local receive window low-mark history.
rwnd-remote-hw	Displays remote receive window high-mark history.
rwnd-remote-lw	Displays remote receive window low-mark history.
ulpd-hw	Displays upper level datagram high-mark history.
ulpd-lw	Displays upper level datagram low-mark history.

Defaults

None.

Command Modes

EXEC

Command History

Release	Modification
12.2(18)IXH	This command was introduced.
12.4(15)SW3	
12.2(33)IRC	

Usage Guidelines

The output from the **show ip sctp association monitor** command is displayed in the form of a graph. The Y-axis of the graph is the round trip time (RTT) value. The X-axis of the graph is the increment within the period displayed in the graph; for example, the individual minutes during the previous hour.

Examples

This example includes output from the **show ip sctp association monitor** command detailing a 1-hour RTT measurement. The most recent measurement is on the left end of the X-axis. The top three rows, read vertically, displays the highest value as it exceeds the maximum of the Y-axis value.

```

2          2
          2      1
          0      4
210      * *      *          * *          *
190      * * *      *          * *          **
170      * * *      *          * * * *          * * * *
150      * * *      **          * * * * * *          * * * *
130      * * *      **          * * * * * *          * * * *
110      ** * *      **          * * * * * *          * * * *
90       ** **      ***          * * * * * *          * * * *
70      *** ** *      *** ** * * * * * * * * * * * *
50      *** * * * * * * * * * * * * * * * * * * * *
30      *** ## * * * * * * * * * * * * * * * * * * *
10      ##### * * * * * * * * * * * * * * * * * * *
0...5...1...1...2...2...3...3...4...4...5...5...6
    0    5    0    5    0    5    0    5    0    5    0    5    0
RTT average(ms) for last 60 minutes
* = maximum # = average

```

Related Commands

Command	Description
clear ip sctp statistics	Resets all SCTP global counters and clears counters for all SCTP associations.

show monitor event-trace

To display event trace messages for Cisco IOS software subsystem components, use the **show monitor event-trace** privileged EXEC command.

```
show monitor event-trace [all-traces] [component {all | back time | clock time | from-boot
[seconds | detail] | latest | parameters}]
```

Syntax Description		
all-traces		Displays all event trace messages in memory to the console.
<i>component</i>		Name of the Cisco IOS software subsystem component that is the object of the event trace. To display event trace messages for the ITP Group feature, enter itp-group as the component. To display event trace messages for the ITP MLR Call Trace feature, enter cs7 mlr as the component. To get a list of components that support event tracing in this release, use the monitor event-trace ? command.
all		Displays all event trace messages currently in memory for the specified component.
back		Specifies how far back from the current time you want to view messages. For example, you can gather messages from the last 30 minutes.
<i>time</i>		Length of time in hours and minutes (hh:mm).
clock		Displays event trace messages starting from a specific clock time.
<i>time</i>		Time from which to display messages in hours and minutes (hh:mm).
from-boot		Displays event trace messages starting from a specified number of seconds after booting.
<i>seconds</i>		Number of seconds since the networking device was last booted (uptime). To view the uptime, enter the show monitor event-trace component from-boot ? command.
detail		Displays information in detailed format.
latest		Displays only the event trace messages since the last show monitor event-trace command was entered.
parameters		Displays the trace parameters. Currently, the only parameter displayed is the size (number of trace messages) of the trace file.

Defaults None.

Command Modes Privileged EXEC

Command History

Release	Modification
12.0(18)S	This command was introduced.
12.2(8)T	This feature was integrated into Cisco IOS Release 12.2(8)T.
12.2(25)SW3	The itp-group component was added.
12.2(25)SW5	The cs7 mlr component was added.

Usage Guidelines

Use the **show monitor event-trace** command to display trace message information.

The trace function is not locked while information is being displayed to the console, which means that new trace messages can accumulate in memory. If entries accumulate faster than they can be displayed, some messages can be lost. If this situation occurs, the **show monitor event-trace** command generates a message indicating that some messages might be lost; however, messages will continue to display on the console. If the number of lost messages is excessive, the **show monitor event-trace** command stops displaying messages.

Examples

The following example includes output from the **show monitor event-trace** command with **itp-group** as the *component* argument and the **all** keyword:

```
ITP# show monitor event-trace itp-group all
00:00:15.581: ITP Group: starting 60 sec peer timer
00:00:37.485: ITP Group: transport event - DDT transport is UP
00:00:37.485: ITP Group: FSM event - PEER_COMM in Init state
00:00:37.485: ITP Group: stopping peer timer
00:00:38.487: ITP Group: sending nego msg - state Negotiating uptime 00000016.E7
D7CDC1
00:00:38.487: ITP Group: sent Negotiation message
00:00:38.487: ITP Group: starting 30 sec negotiation timer
00:00:38.487: ITP Group: FSM result - new state is Negotiating
00:00:38.519: ITP Group: rcvd Negotiation message
00:00:38.519: ITP Group: rcvd nego msg - state Negotiating, peer state Negotiat
ng, uptime 00000016.E7D7CDC1, peer uptime 00000005.2B2E9281
00:00:38.519: ITP Group: stopping negotiation timer
00:00:38.519: ITP Group: negotiated to Manager role
00:00:38.519: ITP Group: FSM event - NEGO_MANAGER in Negotiating state
00:00:38.519: ITP Group: FSM result - new state is Manager
00:00:41.219: ITP Group: transport event - RF transport is UP
00:00:41.219: ITP Group: transport event - CHKPT transport is UP
00:00:41.219: ITP Group: clearing sys-shut on distributed links
00:00:47.942: ITP Group: RF_PROG_ACTIVE - state ACTIVE, peer DISABLED, op 0
00:00:47.942: ITP Group: RF_STATUS_PEER_COMM - state ACTIVE, peer DISABLED, op 1
00:00:49.485: ITP Group: RF_PROG_STANDBY_BULK - state ACTIVE, peer STANDBY COLD,op 0
```

The following example includes output from the **show monitor event-trace** command with **cs7 mlr** as the *component* argument and the **all** keyword. In this example, the command displays all the traces in the current buffer.

```
ITP# show monitor event-trace cs7 mlr all
1722646: Dec 2 18:44:34:MLRI:0 to_berm dpc:1.1.2 opc:4.4.4 cdPa:123450 2/0
ssn:0 cgPa:3.2.2 ssn:8 BEG otid:0x0
1722647: Dec 2 18:44:34:MLRE:0 to_berm dpc:1.1.2 opc:4.4.4 cdPa:123450 2/0
ssn:0 cgPa:3.2.2 ssn:8 BEG otid:0x0 <Result> Resume
SCCP routing Type:No Result Error:No OTID
1844450: Dec 2 18:55:59:MLRI:0 rule:4 to_berm dpc:1.1.2 opc:4.4.4 cdPa:123450
2/0 ssn:0 cgPa:3.2.2 ssn:8 BEG otid:0xD200D3 SMS-MO
```

show monitor event-trace

```

Subm dstSme:1800 0/1 orgSme:4091254283 1/1 dstSmsc:409
2008000 1/1 smRpUiLen:15
1844451: Dec  2 18:55:59:MLRE:0 rule:4 to_berm dpc:1.1.2 opc:4.4.4 cdPa:123450
2/0 ssn:0 cgPa:3.2.2 ssn:8 BEG otid:0xD200D3 <Result>
Routing failure Group:MLR5 Type:GROUP Error:No
available member in result group Matched:MLR1 rule 100
1844452: Dec  2 18:56:47:MLRI:0 rule:4 to_berm dpc:1.1.2 opc:4.4.4 cdPa:123450
2/0 ssn:0 cgPa:3.2.2 ssn:8 BEG otid:0xD200D3 SMS-MO
Subm dstSme:1800 0/1 orgSme:4091254283 1/1 dstSmsc:409
2008000 1/1 smRpUiLen:15
1844453: Dec  2 18:56:47:MLRO:0 rule:4 to_berm dpc:4.4.4 opc:1.1.2 cdPa:123450
2/0 ssn:0 cgPa:3.2.2 ssn:8 BEG otid:0xD200D3 <Result>
Route to MLR destination Group:MLR5 Type:PC Matched:ML
R1 rule 100
1844454: Dec  2 18:57:45:MLRI:0 rule:2 to_berm dpc:1.1.2 opc:4.4.4 cdPa:123450
2/12 ssn:0 cgPa:0.64.2 ssn:11 BEG otid:0xD1040662
SMDPP smsOrigDstSme:1800687634 0/0/1 smsOrigOrgSme:405
3688187 0/0/1 smsDataLen:20
1844455: Dec  2 18:57:45:MLRO:0 rule:2 to_berm dpc:4.4.4 opc:1.1.2 cdPa:123450
2/12 ssn:0 cgPa:0.64.2 ssn:11 BEG otid:0xD1040662
<Result> Route to MLR destination Group:MLR1 Type:AS
berm4 Matched:MLR1 rule 1000

```

The following example includes output from the **show monitor event-trace** command with **cs7 mlr** as the *component* argument and the **all** keyword. Notice the “one or more entries lost” message. The trace function is not locked while information is being displayed to the console, which means that new trace messages can accumulate in memory. If entries accumulate faster than they can be displayed, some messages can be lost. If this situation occurs, the “one or more entries lost” message is displayed in the output.

```

ITP# show monitor event-trace cs7 mlr all
36: Dec  8 03:30:43: MLRI:0 rule:4 to_berm dpc:1.1.2 opc:4.4.4 cdPa:123450 2/0
    ssn:0 cgPa:3.2.2 ssn:8 BEG otid:0xD200D3 SMS-MO Subm
    dstSme:1800 0/1 orgSme:4091254283 1/1 dstSmsc:4092008000
    1/1 smRpUiLen:15
37: Dec  8 03:30:43: MLRO:0 rule:4 to_berm dpc:4.4.4 opc:1.1.2 cdPa:123450 2/0
    ssn:0 cgPa:3.2.2 ssn:8 BEG otid:0xD200D3 <Result> Route to
    MLR destination Group:MLR5 Type:PC Matched:MLR1 rule 100
.. one or more entries lost ..

426: Dec  8 03:30:44: MLRI:0 rule:4 to_berm dpc:1.1.2 opc:4.4.4 cdPa:123450 2/0
    ssn:0 cgPa:3.2.2 ssn:8 BEG otid:0xD200D3 SMS-MO Subm
    dstSme:1800 0/1 orgSme:4091254283 1/1 dstSmsc:4092008000
    1/1 smRpUiLen:15
427: Dec  8 03:30:44: MLRO:0 rule:4 to_berm dpc:4.4.4 opc:1.1.2 cdPa:123450 2/0
    ssn:0 cgPa:3.2.2 ssn:8 BEG otid:0xD200D3 <Result> Route to
    MLR destination Group:MLR5 Type:PC Matched:MLR1 rule 100

```

The following example includes output from the **show monitor event-trace** command with **cs7 mlr** as the *component* argument and the **parameters** keyword. The example shows that the trace is enabled and the size of the trace memory.

```

ITP# show monitor event-trace cs7 mlr parameters
Trace has 10000 entries
Stacktrace is disabled by default
Trace is enabled in instance 0 with ruleset MLR2

```

Syntax of MLR Call Trace Records

The **show monitor event-trace cs7 mlr** command displays three types of MLR call trace records: MLRI (inbound message record), MLRO (outbound message record), and MLRE (error record). The syntax of the information contained in call records is provided in the following list:

- Syntax for information common to all MLR trace records. The fields are described in [Table 83](#).

```
{MLRI | MLRO | MLRE}:instance-number rule:order ils-name dpc:dpc opc:opc cdPa:cdPa
cgPa:cgPa tcapMsg otid:otid [dtid:dtid]
```

- Syntax for MLRI sms-mo operation-specific information. The fields are described in [Table 84](#).

```
SMS-MO [pduType] dstSme:dest-sme orgSme:orig-sme dstSmsc:dest-smsc imsi:imsi
smRpUiLen:len
```

- Syntax for MLRI smdpp operation-specific information. The fields are described in [Table 85](#).

```
SMDPP dstSme:dest-sme orgSme:orig-sme [min min] [imsi:imsi] smsDataLen:len
```

- Syntax for MLRO result-specific information. The fields are described in [Table 86](#).

```
Result {Resume SCCP routing | Resume SCCP GTT modified | Route to MLR destination}
[Group:result-group-name] Type:result-type Matched:ruleset-name rule number
```

- Syntax for MLRE result-specific information. The fields are described in [Table 87](#).

```
Result {Resume SCCP routing | Routing failure} [Group:result-group-name]
Type:result-type Error:error-description [Matched:ruleset-name rule number]
```

[Table 83](#) describes the syntax of fields common to all MLR trace records.

Table 83 *show monitor event-trace Fields Common to all MLR Trace Records*

Field	Description
MLRI:instance-number MLRE:instance-number MLRO:instance-number	Trace type and CS7 instance number: MLRI MLR Inbound message MLRE MLR Error message MLRO MLR Outbound message instance-number CS7 instance number (0 to 7)
rule:order	Matching rule number from the event-trace ruleset
ils-name	Configured inbound linkset name
dpc:dpc	Destination point code
opc:opc	Origin point code
cdPa:cdpa ssn:number	Called party address. Displayed only for si=SCCP. ssn:number cdPa subsystem number If ri = gt, then the following syntax applies. GTA is truncated to 15 digits. cdpa:gta gti [/tt [/np/nai]] tt is displayed for gti=2 or gti=4. np/nai is displayed only for gti=4.

Table 83 *show monitor event-trace Fields Common to all MLR Trace Records (continued)*

Field	Description
cgPa: <i>cgpa ssn:number</i>	Calling party address. Displayed only for si=SCCP. ssn:number cgPa subsystem number If ri = gt, then the following syntax applies. GTA is truncated to 15 digits. cgpa: <i>gta gti [/tt [/np/nai]]</i> <i>tt</i> is displayed for gti=2 or gti=4. <i>np/nai</i> is displayed only for gti=4. If ri=pc/ssn, then display cdpa point code.
<i>tcap-msg</i>	TCAP message: BEG TCAP BEGIN CONT TCAP CONTINUE
otid: <i>otid</i>	Originating TID, present for BEGIN and CONTINUE <i>otid</i> Hexadecimal number
dtid: <i>dtid</i>	Destination TID, present for CONTINUE <i>dtid</i> Hexadecimal number

[Table 84](#) describes the fields for MLRI SMS-MO operation-specific information.

Table 84 *show monitor event-trace Fields in SMS-MO Operation MLRI Trace Records*

Field	Description
SMS-MO	Operation type SMS-MO
<i>pdu-type</i>	PDU type: Subm Submit Cmd Command
dstSme: <i>address ton/np</i>	B-address, destination SME, TP-DA, type-of-number/numbering plan identification
orgSme: <i>address</i>	A-address, origin SME, sm-RP-Oa
dstSmsc: <i>address</i>	Destination SMSC, sm-RP-Da
imsi: <i>address</i>	Origin IMSI
smRpUiLen: <i>number</i>	SMS MO user data length

[Table 85](#) describes the fields for MLRI SMDPP operation-specific information.

For SMDPP messages:

- The **dstSme** keyword is used to indicate which parameter was used for dest-sme rule matching. Even if multiple parameters are present in the message, only the parameter used for dest-sme rule matching is displayed.

- The **orgSme** keyword also indicates which parameter was used for dest-sme rule matching. Even if multiple parameters are present in the message, only the parameter used for orig-sme rule matching is displayed.

Table 85 *show monitor event-trace Fields in SMDPP Operation MLRI Trace Records*

Field	Description
SMDPP	Operation type SMDPP
<i>pdu-type</i>	PDU type: Subm Submit Cmd Cmd
Command displays one of the following fields: smsOrigDstSme:address natureInplencoding smsDstSme:address natureInplencoding minDstSme:address imsiDstSme:address cdPaDstSme	dest-sme rule matching: SMS_OriginalDestiationAddress SMS_DestinationAddress MobileIdentificationNumber IMSI Indicates that the called party address was used for dest-sme matching.
Command displays one of the following fields: smsOrigOrgSme:address natureInplencoding smsOrgSme:address natureInplencoding cgPaOrgSme	orig-sme rule matching: SMS_OriginalOriginatingAddress SMS_OriginatingAddress Indicates that the calling party address was used for orig-sme matching.
min number	Mobile Identification Number.
imsi number	International Mobile Station ID (min and imsi displayed only if present in the message and not used in dest-sme matching).
smsDataLen number	SMS bearer data length.

Table 86 describes the fields for MLRO result-specific information.

Table 86 *show monitor event-trace MLRO Result-Specific Field Descriptions*

Field	Description
<Result> <i>result</i>	<Result> Indicates that a Result description follows. <i>result</i> One of the following results: • Route to MLR destination—Packet is routed to new MLR destination. • Resume SCCP GTT modified—Packet is routed to new MLR GT destination. Resume SCCP routing with new GT result. • Resume SCCP Routing—For MLRO, this result indicates that a ‘continue’ result was selected. • Routing failure—Packet is discarded. For MLRO, this result indicates that a ‘block’ result was selected.
Group: <i>result-group-name</i>	Indicates that the specified result group was used to select the final MLR result.
Type: <i>result-type</i>	Indicates the result type. Possible types include: • PC • PC/SSN • AS <i>asname</i> • GT • GROUP • BLOCK • CONTINUE • No Result
Matched: <i>ruleset-name rule number</i>	Indicates the MLR ruleset and rule number selected for this packet.

[Table 87](#) describes the fields for MLRE result-specific information.

Table 87 *show monitor event-trace MLRE Result-Specific Field Descriptions*

Field	Description
<Result> <i>result</i>	<Result> Indicates that a Result description follows. <i>result</i> One of the following results: - Resume SCCP Routing–Packet resumes SCCP routing. See error descriptions. For MLRE, this result generally indicates that no available results were present in a result group and ‘unavailable-routing resume’ is configured. - Routing failure–Packet is discarded. For MLRE, see the error description for the reason for this failure.
Group: <i>result-group-name</i>	Indicates that the specified result group was selected before the error was encountered.
Type: <i>result-type</i>	Indicates that the specified result group was selected before the error was encountered. Result types include: - PC - PC/SSN - AS <i>asname</i> - GT - GROUP - BLOCK - CONTINUE - No Result
Error: <i>error-description</i>	Indicates that MLR detected an error when processing this packet. The description indicates which error was detected.
Matched: <i>ruleset-name rule number</i>	Indicates that the MLR matched the specified ruleset and rule number before the error was encountered.

Related Commands

Command	Description
cs7 group	Configures the ITP group name and port number and enables group configuration mode.
cs7 mlr ruleset	Specifies sets of rules used to process traffic that matches triggers defined in a multilayer routing table.
monitor event-trace cs7 mlr (EXEC)	Controls event trace functions for a specified Cisco IOS software subsystem component.

show redundancy states

To display information about the redundancy state of the Cisco 7600 ITP platform during the Non-Disruptive Upgrade process, use the **show redundancy states** privileged EXEC command.

show redundancy states

Syntax Description This command has no arguments or keywords.

Defaults None.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples The following output shows the redundancy state on the active supervisor before the switchover:

```
ITP#show redundancy states
    my state = 13 -ACTIVE
    peer state = 8  -STANDBY HOT
        Mode = Duplex
        Unit = Primary
        Unit ID = 5
Redundancy Mode (Operational) = sso
Redundancy Mode (Configured)  = sso
Redundancy State               = sso

    Split Mode = Disabled
    Manual Swact = Enabled
    Communications = Up

    client count = 62
    client_notification_TMR = 30000 milliseconds
        keep_alive TMR = 9000 milliseconds
        keep_alive count = 1
        keep_alive threshold = 18
        RF debug mask = 0x0
```

The following output shows the redundancy state on the active supervisor after the switchover:

```
itp#sh red states
    my state = 13 -ACTIVE
    peer state = 8  -STANDBY HOT
        Mode = Duplex
        Unit = Secondary
        Unit ID = 6
Redundancy Mode (Operational) = sso
Redundancy Mode (Configured)  = sso
```



```
Redundancy State                = sso

    Split Mode = Disabled
    Manual Swact = Enabled
    Communications = Up

    client count = 64
    client_notification_TMR = 30000 milliseconds
        keep_alive TMR = 9000 milliseconds
        keep_alive count = 1
    keep_alive threshold = 19
        RF debug mask = 0x0
```

Related Commands

Command	Description
cs7 upgrade module	Upgrades the software on a line card.
cs7 upgrade analysis	Displays a report indicating the probable impact of performing a software upgrade.

show redundancy inter-device

To display redundancy information, use the **show redundancy inter-device** privileged EXEC command.

show redundancy inter-device

Syntax Description This command has no arguments or keywords.

Defaults None.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(18)IXA	This command was introduced for ITP.
	12.4(11)SW	
	12.2(33)IRA	

Examples The following example shows how to display interdevice redundancy information:

```
ITP# show redundancy inter-device
Redundancy inter-device state: RF_INTERDEV_STATE_ACT
      Scheme: Platform
      Peer present: RF_INTERDEV_PEER_COMM
```

[Table 88](#) describes the significant fields shown in the display.

Table 88 *show redundancy inter-device Field Descriptions*

Field	Description
Redundancy inter-device state	Displays internal state of interdevice redundancy finite state machine.
RF_INTERDEV_STATE_INIT	Initial state.
RF_INTERDEV_STATE_PC_NO_PLAT	Peer communication established but redundancy role has not been determined.
RF_INTERDEV_STATE_PNC_NO_PLAT	Peer communication has not been established and redundancy role has not been determined.
RF_INTERDEV_STATE_ACT	This device is the Active device.
RF_INTERDEV_STATE_STDBY	This device is the Standby device.
Scheme	Entity that determines redundancy role.
Platform	Redundancy role is determined based on platform state.
Standby	Redundancy role is determined by HSRP.
Peer Present	Fields describe communication with peer device.

Table 88 *show redundancy inter-device Field Descriptions (continued)*

Field	Description
RF_INTERDEV_PEER_COMM	Communication established with peer device.
RF_INTERDEV_PEER_NO_COMM	Communication not established with peer device.

Related Commands

Command	Description
redundancy	Configures interdevice redundancy when used with the inter-device keyword.

show sscf-nni

To display SSCF information, use the **show sscf-nni** EXEC command.

show sscf-nni [*interface*]

Syntax Description	<i>interface</i>	If no interface number is specified, all interfaces supporting SSCF-NNI are displayed.

Defaults	None.

Command Modes	EXEC

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples The following example includes output from the **show sscf-nni** command for the ATM interface:

```
ITP# show sscf-nni atm
SSCF-NNI details for interface ATM5/0/0
SSCF-NNI Current State = In Service
ULP Current State = In Service
SSCF-NNI Configured Parameters:
N1 = 90000 T1 = 5 T2 = 120
T3 = 1 SSCOP Rec = 60 Force Proving = 10
No Credit = 2 NRP = 0
SSCF-NNI Dynamic Parameters:
C1 = 0 MaxNRP = 1
MPS = 11 UPS = 4 Congestion Level = 0
SSCF-NNI Most Recent SSCOP-UU values:
Local Proving Status= 4 Local Release Status= 1
Remote Proving Status= 4 Remote Release Status= 0
SSCF-NNI Statistics:
MSU's Sent = 3334178, MSU's Received = 3346602, MSU's Ignored = 0
LSSU's Sent = 1010831, LSSU's Received = 796648, LSSU's Ignored = 0
Byte's Sent = 119636773, Byte's Received = 120107750
```

[Table 89](#) describes the fields in the **show sscf** display.

Table 89 *show sscf Field Descriptions*

Field	Description
SSCF-NNI Current State	Current state as defined in Q.2140.
ULP Current State -	Current state of Upper Layer Protocol as viewed by SSCF and as defined in Q.2140.

Table 89 *show sscf Field Descriptions*

Field	Description
Configured parameters	The configured parameters.
Dynamic parameters	Variables used by SSCF as defined in Q.2140.
SSCOP-UU values	Most recent values sent or received as defined in Q.2140.
Stats	Statistics.

show sscop

To display Service-Specific Connection-Oriented Protocol (SSCOP) details for all ATM interfaces, use the **show sscop** EXEC command.

show sscop [*interface*]

Syntax Description	<i>interface</i>	If no interface is specified, all interfaces supporting SSCOP are displayed.
Defaults	None.	
Command Modes	EXEC	
Command History	Release	Modification
	10.0	This command was introduced.

Examples

The following example includes output from the **show sscop** command:

```
ITP# show sscop
SSCOP details for interface ATM4/0/0
  Current State = Active,   Uni version = NNI
  Send Sequence Number: Current = 1118,   Maximum = 2142
  Send Sequence Number Acked = 1118
  Rcv Sequence Number: Lower Edge = 1137, Upper Edge = 1137, Max = 2161
  Poll Sequence Number = 35181, Poll Ack Sequence Number = 35181
  Vt(Pd) = 0   Vt(Sq) = 1   MaxPd = 500
  Timer_IDLE = 100 - Inactive
  Timer_CC = 200 - Inactive
  Timer_POLL = 100 - Inactive
  Timer_KEEPLIVE = 100 - Inactive
  Timer_NO-RESPONSE = 1500 - Inactive
  Current Retry Count = 0, Maximum Retry Count = 10
  AckQ count = 0, RcvQ count = 0, TxQ count = 0
  AckQ HWM = 279, RcvQ HWM = 0, TxQ HWM = 42
  Local connections currently pending = 0
  Max local connections allowed pending = 0
  Statistics -
    Pdu's Sent = 61744, Pdu's Received = 61903, Pdu's Ignored = 0
    Begin = 0/2, Begin Ack = 2/0, Begin Reject = 0/0
    End = 0/6, End Ack = 0/0
    Resync = 0/0, Resync Ack = 0/0
    Sequenced Data = 49840/49660, Sequenced Poll Data = 0/0
    Poll = 6099/5997, Stat = 5982/6099, Unsolicited Stat = 0/0
    Unassured Data = 0/0, Mgmt Data = 0/0, Unknown Pdu's = 0
    Error Recovery/Ack = 0/0, lack of credit 0
```

Table 90 describes the fields in the **show sscop** display.

**Note**

“Inactive” status (in the Timer fields) does not mean that the timer is disabled. It means that the timer is currently not running.

Table 90 *show sscop Field Descriptions*

Field	Description
SSCOP details for interface	Interface slot and port.
Current State	SSCOP state for the interface.
Uni Version	The version of the SSCF layer. For ITP, the Uni Version is NNI.
Send Sequence Number	Current and maximum send sequence number.
Send Sequence Number Acked	Sequence number of packets already acknowledged.
Rcv Sequence Number	Sequence number of packets received.
Poll Sequence Number	Current poll sequence number.
Poll Ack Sequence Number	Poll sequence number already acknowledged.
Vt(Pd)	Number of sequenced data (SD) frames sent, which triggers a sending of a poll frame.
Vt(Sq)	Transmitter connection sequence number that helps peer detect connection message retransmits.
MaxPd	Maximum number of packets sent before a poll packet is sent.
Timer_IDLE	Configured sscop idle-timer in milliseconds and the Active/Inactive status.
Timer_CC	Configured sscop cc-timer in milliseconds.
Timer_POLL	Configured sscop poll-timer in milliseconds.
Timer_KEEPAKALIVE	Configured sscop keepalive-timer in milliseconds.
Timer_NO-RESPONSE	Configured sscop noResponse-timer in milliseconds.
Connection Control	Timer used for establishing and terminating SSCOP.
Keep Alive Timer	Timer used to send keepalives on an idle link.
Current Retry Count	Current count of the retry counter.
Maximum Retry Count	Maximum value the retry counter can take.
AckQ HWM	Current number of packets waiting for acknowledgement and the high-water mark.
RcvQ HWM	Current number of packets in receive queue yet to be processed and high-water mark.
TxQ HWM	Current number of packets in transmit queue waiting to be sent.
Pdu's Sent	Total number of SSCOP frames sent.
Pdu's Received	Total number of SSCOP frames received.
Pdu's Ignored	Number of invalid SSCOP frames ignored.
Begin	Number of Begin frames sent/received.
Begin Ack	Number of Begin Ack frames sent/received.

Table 90 *show sscop Field Descriptions (continued)*

Field	Description
Begin Reject	Number of Begin Reject frames sent/received.
End	Number of End frames sent/received.
End Ack	Number of End Ack frames sent/received.
Resync	Number of Resync frames sent/received.
Resync Ack	Number of Resync Ack frames sent/received.
Sequenced Data	Number of Sequenced Data frames sent/received.
Sequenced Poll Data	Number of Sequenced Poll Data frames sent/received.
Poll	Number of Poll frames received/sent.
Stat	Number of Stat frames received/sent.
Unsolicited Stat	Number of Unsolicited Stat frames received/sent.
Unassured Data	Number of Unassured Data frames received/sent.
Mgmt Data	Number of Mgmt Data frames received/sent.
Unknown Pdu's	Number of Unknown PDU frames sent/received.
Error Recovery/Ack	Number of error recovery PDUs sent/number of error recovery ACK PDUs sent.
Lack of credit	Number of times an attempt to transmit data failed because the send window was closed by the peer.

show tech-support

To collect and display information for troubleshooting your system, use the **show tech-support** privileged EXEC command.

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.2(18)IXA	This command was enhanced to display information about ITP.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines The **show tech-support** command is useful for collecting a large amount of information about your ITP configuration for troubleshooting purposes. The output of this command can be provided to technical support representatives when reporting a problem.

The **show tech-support** command displays the output of a number of show commands at once. The output from this command will vary depending on your platform and configuration.

For information about general output, refer to the **show tech-support** entry in the “Troubleshooting and Fault Management Commands” section of the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*.

Specific ITP information collected by the following commands is displayed as output from the **show tech-support** command:

- show cs7
- show cs7 mtp3 errors
- show cs7 route
- show cs7 linkset
- show cs7 linkset statistics
- show cs7 accounting
- show cs7 gtt measurements

When M3UA or SUA is configured, output from the following commands is displayed:

- show cs7 m3ua
- show cs7 sua
- show cs7 asp
- show cs7 as

- show cs7 point-codes

When ITP Nonstop Operation (NSO) is configured, output from the following commands is displayed:

- show cs7 nso state
- show cs7 nso counters detailed

When an ITP group is configured, output from the following commands is displayed:

- show cs7 group state
- show cs7 group counters detailed
- show cs7 group transport

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Examples

The following example shows how to disable M3UA on port 2905:

```
cs7 m3ua 2905
shutdown
```

Related Commands

Command	Description
cs7 m3ua	Specifies the local port number for M3UA and enters cs7 m3ua submode.

shutdown (cs7 asp)

To disable an ASP without deleting the configuration, use the **shutdown** cs7 asp submode command. To reenable the ASP, use the **no** form of this command.

shutdown

no shutdown

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Command Modes	cs7 asp submode

Command History	Release	Modification
	12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.

Examples	The following example shows how to disable the ASP named ASP1: <pre>cs7 asp ASP1 2904 2905 m3ua shutdown</pre>

Related Commands	Command	Description
	cs7 asp	Specifies an application server process (ASP) and enables cs7 asp submode.

shutdown (cs7 dcs)

To stop sending PMP packets and pings to a DCS node, use the **shutdown** command in cs7 dcs submode. To reenale sending packets and pings, use the **no** form of this command.

shutdown

no shutdown

Syntax Description This command has no arguments or keywords.

Defaults The DCS node is shut down by default.

Command Modes cs7 dcs submode

Command History	Release	Modification
	12.4(15)SW3	This command was introduced.
	12.2(33)IRC	

Examples The following example shows how to disable the DCS node named alpha:

```
cs7 dcs alpha
shutdown
```

Related Commands	Command	Description
	cs7 pmp	Turns probeless monitoring on for all linksets and ASes.
	cs7 pmp hold-queue	Sets the integer range of PMP hold queue thresholds.
	cs7 dcs-group	Identifies a name to be associated with a DCS group.
	cs 7 dcs	Identifies a name to be associated with a DCS node.
	show cs7 pmp	Displays errors and information about the PMP.
	show cs7 dcs-group	Displays information about the DCS group.
	show cs7 dcs	Displays information about the DCS node.

shutdown (cs7 link)

To disable a link, use the **shutdown** cs7 link submode command. To bring a link into the active state (under the condition that its parent linkset is already in the active state), use the **no** form of this command.

shutdown

no shutdown

Syntax Description This command has no arguments or keywords.

Defaults None.

Command Modes cs7 link submode

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines A link can be brought back into the active state with the **no shutdown** command only if its parent link is in the active state.



Note

The **cs7 prompt enhanced** command is an optional global configuration command that changes the prompt in linkset configuration mode to display the linkset (and, where applicable, the link) that is currently being configured. This command is intended to help avoid the possibility of inadvertently shutting down the wrong linkset or link.

Examples The following example shows how to disable the link:

```
cs7 linkset michael 10.1.1
link 0 sctp 172.18.44.147 7000 7000
shutdown
```

Related Commands	Command	Description
	cs7 ignore-sccp-pcconv	Inhibits a link.
	cs7 prompt enhanced	Changes the prompt in linkset configuration mode to display the linkset (and, where applicable, the link) that is currently being configured.

shutdown (cs7 linkset)

To disable a linkset, use the **shutdown** cs7 linkset submode command. To reactivate a disabled linkset, use the **no** form of this command.

shutdown

no shutdown

Syntax Description This command has no arguments or keywords.

Defaults None.

Command Modes cs7 linkset submode

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

A linkset can be activated or deactivated with the (no) **shutdown** command.

When you deactivate a linkset with the **shutdown** command, all links in that linkset are deactivated. The linkset is shown as “SHUTDOWN” in the output of the **show term** command.

However, the links in the linkset do not appear as “SHUTDOWN” because they were not administratively shut down.

When a link is administratively shut down, it remains in the shutdown state (and is not activated, even when its linkset is activated) until a **no shutdown** command is specified for the link. The reason for requiring an explicit reactivation (no shutdown) of a link is to allow users to maintain the state of the link when linksets are activated, in case they do not want a link to be activated.



Note

The **cs7 prompt enhanced** command is an optional global configuration command that changes the prompt in linkset configuration mode to display the linkset (and, where applicable, the link) that is currently being configured. This command is intended to help avoid the possibility of inadvertently shutting down the wrong linkset or link.

Examples

The following example shows how to shut down the linkset, and all links in the linkset:

```
cs7 linkset rosebud
shutdown
```

The following example shows how to reactivate the linkset named rosebud, but all links belonging to the linkset remain deactivated until explicitly activated with the link subcommand **no shut**:

```
cs7 linkset rosebud  
no shutdown
```

Related Commands

Command	Description
cs7 linkset	Specifies a linkset.
cs7 prompt enhanced	Changes the prompt in linkset configuration mode to display the linkset (and, where applicable, the link) that is currently being configured.

shutdown (cs7 m3ua)

To shut down the M3UA protocol, use the **shutdown** cs7 m3ua submode command. To reenable the protocol, use the **no** form of this command.

shutdown

no shutdown

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Command Modes	cs7 m3ua submode

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples	The following example shows how to disable M3UA on port 2905: <pre>cs7 m3ua 2905 shutdown</pre>

Related Commands	Command	Description
	cs7 m3ua	Specifies the local port number for M3UA and enters cs7 m3ua submode.

shutdown (cs7 mated-sg)

To disable a mated SG without deleting the configuration, use the **shutdown** cs7 mated-sg submode command. To reenable the mated SG, use the **no** form of this command.

shutdown

no shutdown

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Command Modes	cs7 mated-sg submode

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples	The following example shows how to disable the mated SG named BLUE:

```
cs7 mated-sg BLUE 5000
shutdown
```

Related Commands	Command	Description
	cs7 mated-sg	Specifies a connection to a mated SG and enters cs7 mated-sg submode.

shutdown (cs7 sgmp)

To disable SGMP, use the **shutdown** cs7 sgmp submode command. To reenable the protocol, use the **no** form of this command.

shutdown

no shutdown

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Command Modes	cs7 sgmp submode

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples	The following example shows how to disable SGMP on port 5000: cs7 sgmp 5000 shutdown

Related Commands	Command	Description
	cs7 sgmp	Configures SGMP and enters cs7 sgmp submode.

shutdown (cs7 sua)

To disable the SUA protocol on a local port without deleting the configuration, use the **shutdown** cs7 sua submode command. To reenable the protocol, use the **no** form of this command.

shutdown

no shutdown

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Command Modes	cs7 sua submode

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples	The following example shows how to disable the SUA protocol on port 15000:
	<pre>cs7 sua 15000 shutdown</pre>

Related Commands	Command	Description
	cs7 sua	Specifies the local port number for SUA and enters cs7 sua submode.

shutdown (group)

To administratively disable the ITP group feature while retaining the feature configuration, use the **shutdown** group submode command. To enable the association, use the **no** form of this command.

shutdown

no shutdown

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Command Modes	Group submode

Command History	Release	Modification
	12.2(18)IXA	This command was introduced in group mode.
	12.4(11)SW	
	12.2(33)IRA	

Examples	The following example shows how to disable the interdevice association: <pre>cs7 group ITP1 3333 shutdown</pre>

Related Commands	Command	Description
	cs7 group	Configures the ITP group.

shutdown (ipc association)

To administratively disable the interdevice association, use the **shutdown** ipc association submode command. To enable the association, use the **no** form of this command.

shutdown

no shutdown

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Command Modes	ipc association submode

Command History	Release	Modification
	12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced in ipc association mode.

Examples	The following example shows how to enable the interdevice association: <pre>ipc zone default association 1 shutdown</pre>

Related Commands	Command	Description
	association	Configures an association between two devices in the IPC zone.

si

To specify a service indicator in an MTP message type table, use the **si** command in cs7 gws mtp message table configuration mode. To remove the specification, use the **no** form of this command.

```
si si mtp-msg-h0 mtp-msg-h0 mtp-msg-h1-range mtp-msg-h1-start [mtp-msg-h1-end] result
    {action action-set-name | table table-name}
```

```
no si si mtp-msg-h0 mtp-msg-h0 mtp-msg-h1-range mtp-msg-h1-start [mtp-msg-h1-end] result
    {action action-set-name | table table-name}
```

or

```
si si mtp-msg-type mtp-msg-type result {action action-set-name | table table-name}
```

```
no si si mtp-msg-type mtp-msg-type result {action action-set-name | table table-name}
```

To specify a service indicator in an SIO type table, use the **si** command in cs7 gws sio table configuration mode. To remove the specification, use the **no** form of this command.

```
si si [priority-range pri-start [pri-end]] result {action action-set-name | table table-name}
```

```
no si si [priority-range pri-start [pri-end]] result {action action-set-name | table table-name}
```

Syntax Description

<i>si</i>	Valid values: • aal2—AAL2 Sig. service indicator • bicc—BICC service indicator • b-isup—BISUP service indicator • h248—GCP/H.248 service indicator • isup—ISUP service indicator • mgmt—MTP n/w management service indicator • sat-isup—Sat-ISUP service indicator • sccp—SCCP service indicator • test1—MTP n/w testing & maint. Regular SI • test2—MTP n/w testing & maint. Special SI • tup—TUP service indicator • WORD—Spare Service indicators in hex {6, 7, 8, B, F}
mtp-msg-h0	Specifies the MTP3 message type H0

<i>mtp-msg-h0</i>	Valid values: CHM Changeover and Changeback messages DLM Sig Data Link Connection Order messages ECM Emergency Changeover messages FCM Transfer Controlled and Sig Route-set Congestion messages MIM Management Inhibit messages RSM Route-set test messages TFM Transfer Prohibited, Allowed and Restricted messages TRM Traffic Restart Allowed messages UFC User Part Flow Control message
mtp-msg-h1-range	Specifies starting H1-MTP3 message type.
<i>mtp-msg-h1-start</i>	Starting H1-MTP3 message type. Valid values are from 1 to 8.
<i>mtp-msg-h1-end</i>	Ending H1-MTP3 message type. Valid values are from 1 to 8.
mtp-msg-type	Specifies MTP message type.

<i>mtp-msg-type</i>	Valid values: CBA Changeback Acknowledgement CBD Changeback Declaration CNP Connection Not Possible CNS Connection Not Successful COA Changeover Acknowledgement COO Changeover Order CSS Connection Successful DLC Data Link Connection Order ECA Emergency Changeover Acknowledgement ECO Emergency Changeover Order EXA Ext. Changeover Acknowledgement EXO Ext. Changeover Order LFU Link Forced UnInhibit LIA Link Inhibit Acknowledgement LID Link Inhibit Denied LIN Link Inhibit LLT Link Local Inhibit Test LRT Link Remote Inhibit Test LUA Link UnInhibit Acknowledgement LUN Link UnInhibit RCT Route-set Congestion Test RSR Route Set Test Restricted RST Route Set Test TFA Transfer Allowed TFC Transfer Controlled TFP Transfer Prohibited TFR Transfer Restricted TRA Traffic Restart Allowed UPU User Part Unavailable
priority-range	Specifies a priority range.
<i>pri-start</i>	Priority start value.
<i>pri-end</i>	Priority end value.
result	Specifies the next step.
action	Screens by action set by default.
<i>action-set-name</i>	Action set name. Valid names may not exceed 12 alphanumeric characters.
table	Screens by table by default.
<i>table-name</i>	Table name. Valid names may not exceed 12 alphanumeric characters.

Defaults None.

Command Modes cs7 gws mtp message table configuration

Command History	Release	Modification
	12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.
	12.2(18)IXH 12.4(15)SW3 12.2(33)IRC	Additional service indicators were added.

Usage Guidelines The **si** command is valid in the following table types: mtp-msg-type, sio.

Examples The following example shows how to specify a management service indicator (mgmt) entry in table MTP0:

```
cs7 instance 0 gws table MTP0 type mtp-msg-type action allowed
default result action ALLOW
si mgmt mtp-msg-type CBD result table PCSSN1
si mgmt mtp-msg-type CBA result action ALLOW
```

The following example shows how to specify SCCP and ISUP service indicator (sccp and isup) entries in table SIO0:

```
cs7 instance 0 gws table SIO0 type sio action allowed
si sccp result table PCSSN1
si isup result action ALLOW
```

Related Commands	Command	Description
	cs7 gws table	Configures a gateway screening table.

sls-shift

When the variant is ITU, to shift which signaling link selection (SLS) bits are used for link and linkset selection, use the **sls-shift** command in cs7 linkset configuration mode. To disable the specification, use the **no** form of this command.

sls-shift [0-3]

no sls-shift

Syntax Description

0-3	This argument indicates a range, from least significant bit (0) to most significant bit (3) of the SLS, to be used for linkset selection within a combined linkset.

Defaults

The default is bit 0, the equivalent of the **no sls-shift** command.

Command Modes

cs7 linkset configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

This command is valid only when the variant is ITU. It affects MSUs received on the linkset, and changes which bit in the SLS is used for linkset selection.

ITP provides the ability to change which bit to use for linkset selection because ITU, unlike ANSI, does not perform SLS rotation. If all nodes in the network use the same bit for linkset selection, traffic will not balance evenly.

Examples

The following example shows how to specify that the most significant bit (3) of the SLS is to be used for linkset selection within a combined linkset:

```
cs7 linkset linkset1
sls-shift 3
```

Related Commands

Command	Description
cs7 linkset	Specifies a linkset.

smsc-map-version (cs7 sms gsm)

To specify a locally supported MAP version, use the **smsc-map-version** command in `cs7 sms gsm` configuration mode. To return to the default MAP version, use the **no** form of this command.

smsc-map-version *version*

no smsc-map-version *version*

Syntax Description	<i>version</i> GSM MAP version. Valid version numbers are 2 and 3. The default is 3.

Defaults	The default GSM MAP version is 3.

Command Modes	cs7 sms gsm configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	The version is the highest one used when establishing SMS MO dialogs with both MSCs and SMSCs.

Examples	The following example shows how to configure an SMS route table and specify a CDR service, GSM MAP routing, and GSM MAP version 3: <pre>cs7 sms gsm-map ssn 8 smsc-map-version 3</pre>

Related Commands	Command	Description
	cs7 sms gsm-map	Specifies an SMS route table.

snmp-server enable traps bits-clock

To enable Simple Network Management Protocol (SNMP) to generate notifications about the building integrated timing supply (BITS) clocking sources and modes of operations, use the **snmp-server enable traps bits-clock** global configuration command. To disable the sending of traps, use the **no** form of this command.

snmp-server enable traps bits-clock

no snmp-server enable traps bits-clock

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Command Modes	Global configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	The snmp-server enable traps bits-clock command provides support for CISCO-BITS-CLOCK-MIB.my.

Examples	The following example shows how to generate notifications to indicate when clocking sources change roles or become unavailable: <pre>snmp-server enable traps bits-clock</pre>

Related Commands	Command	Description
	snmp-server enable traps cs7	Enables sending of SNMP ITP traps.

snmp-server enable traps cs7

To enable ITP Simple Network Management Protocol (SNMP) traps to be sent, use the **snmp-server enable traps cs7** global configuration command. To disable the sending of ITP SNMP traps, use the **no** form of this command.

```
snmp-server enable traps cs7 [crd-state][dsmr-smpp-dest] [dsmr-table-load] [dsmr-ucp-dest]
[gtt-map-state] [gw-dest-r1-state] [gw-dest-state] [gw-gtt-errors] [gw-gtt-load]
[gw-isolation] [gw-link-congestion] [gw-link-state] [gw-link-utilization] [gw-linkset-state]
[gw-map-state] [gw-route-load] [gw-route-mgmt-state] [gw-route-r1-mgmt-state]
[link-congestion] [link-state] [link-utilization] [linkset-state] [mlr-table-load]
[monitor-congestion] [monitor-state] [route-state] [msu-rate] [xua-state]
```

```
no snmp-server enable traps cs7 [crd-state][dsmr-smpp-dest] [dsmr-table-load]
[dsmr-ucp-dest] [gtt-map-state] [gw-dest-r1-state] [gw-dest-state] [gw-gtt-errors]
[gw-gtt-load] [gw-isolation] [gw-link-congestion] [gw-link-state] [gw-link-utilization]
[gw-linkset-state] [gw-map-state] [gw-route-load] [gw-route-mgmt-state]
[gw-route-r1-mgmt-state] [link-congestion] [link-state] [link-utilization] [linkset-state]
[mlr-table-load] [monitor-congestion] [monitor-state] [route-state] [msu-rate] [xua-state]
```

Syntax Description	
crd-state	Enables the crd state change trap (ciscoGrtRouteCrdStateChange) in CISCO-ITP-GRT-MIB.my.
dsmr-smpp-dest	Enables the ciscoItpDsmrSmppSessionState notification from CISCO-ITP-DSMR-SMPP-MIB.my.
dsmr-table-load	Enables the ciscoItpDsmrTableLoad notification from CISCO-ITP-DSMR-MIB.my.
dsmr-ucp-dest	Enables the ciscoItpDsmrUCPSessionState notification from CISCO-ITP-DSMR-UCP-MIB.my.
gtt-map-state	Enables the gateway GTT map-state trap (ciscoGsccpGttMapStateChange) in CISCO-ITP-GSCCP-MIB.my. <i>Deprecated and replaced by gw-map-state.</i>
gw-dest-r1-state	Enables the gateway destination state change rev1 trap (ciscoGrtDestStateChange) in CISCO-ITP-GRT-MIB.my.
gw-dest-state	Enables the gateway destination state change trap (ciscoGrtDestStateChange) in CISCO-ITP-GRT-MIB.my.
gw-gtt-errors	Enables the gateway GTT errors trap in CISCO-ITP-GSCCP-MIB.my. This notification is generated whenever any global title error is encountered in the last interval specified by cgsccpGttErrorPeriod or when cgsccpInstErrorIndicator is set to false.
gw-gtt-load	Enables the gateway GTT load table trap (ciscoGsccpGttLoadTable) in CISCO-ITP-GSCCP-MIB.my.
gw-isolation	Enables the gateway isolation trap (ciscoGspIsolation) in CISCO-ITP-GSP-MIB.my.
gw-link-congestion	Enables the gateway link-congestion trap (ciscoGspCongestionChange) in CISCO-ITP-GSP-MIB.my.
gw-link-state	Enables the gateway link-state trap (ciscoGspLinkStateChange) in CISCO-ITP-GSP-MIB.my.

gw-link-utilization	Enables gateway link-utilization traps (ciscoGspLinkRcvdUtilChange, ciscoGspLinkSentUtilChange) in CISCO-ITP-GSP-MIB.my.
gw-linkset-state	Enables the gateway linkset-state trap (ciscoGspLinksetStateChange) in CISCO-ITP-GSP-MIB.my.
gw-map-state	Enables the gateway Mated Appl (MAP) state trap.
gw-route-load	Enables the gateway route table load trap (ciscoGrtRouteTableLoad) in CISCO-ITP-GRT-MIB.my.
gw-route-mgmt-state	Enables the gateway route management state change trap (ciscoGrtMgmtStateChange) in CISCO-ITP-GRT-MIB.my.
gw-route-r1-mgmt-state	Enables the gateway route management state change rev1 trap (ciscoGrtMgmtStateChange) in CISCO-ITP-GRT-MIB.my.
link-congestion	Enables the link-congestion trap (cItpSpCongestionChange) in CISCO-ITP-SP-MIB.my. <i>Deprecated and replaced by gw-link-congestion.</i>
link-state	Enables the link-state trap (cItpSpLinkStateChange) in CISCO-ITP-SP-MIB.my. <i>Deprecated and replaced by gw-link-state.</i>
link-utilization	Enables the link-utilization trap. <i>Deprecated and replaced by gw-link-utilization.</i>
linkset-state	Enables the linkset-state trap (cItpSpLinksetStateChange) in CISCO-ITP-SP-MIB.my. <i>Deprecated and replaced by gw-linkset-state.</i>
mlr-table-load	Enables the MLR table load trap in CISCO-ITP-MLR-MIB.my. This notification is generated whenever a load operation is started or completed. Route table configurations can be loaded by CLI requests. In addition, route tables can be loaded using configuration statements, which allows MLR tables to be reloaded whenever a device restarts.
monitor-congestion	Enables the ciscoItpMonitorCongestion notification in CISCO-ITP-MONITOR-MIB.my.
monitor-state	Enables the monitor-state trap in CISCO-ITP-MONITOR-MIB.my. Notification is generated when a connection changes states. The value of cItpmConnMonitorState indicates the new state.
route-state	Enables the route-state trap (cItpRouteStateChange) in CISCO-ITP-RT-MIB.my. <i>Deprecated and replaced by gw-route-mgmt-state.</i>
msu-rate	Enables the msu-rate trap.
xua-state	Enables the following traps in CISCO-ITP-XUA-MIB.my: ciscoItpXuaAspStateChange - ASP state change ciscoItpXuaSgmStateChange - Mated-SG state change ciscoItpXuaAsStateChange - AS state change ciscoItpXuaAspCongChange - ASP congestion state change ciscoItpXuaSgmCongChange - Mated-SG congestion state change

Defaults

This command is disabled.

Command Modes Global configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines When you enable CS7 traps, the default value for trap queue length (10 events) might cause traps to be lost. To avoid this situation, set the trap queue length to 100 using the **snmp-server queue-length** global configuration command.

For more information about SNMP, refer to “Configuring SNMP Support” in the Cisco IOS Release 12.1 *Configuration Fundamentals Configuration Guide*, Part 3, Cisco IOS System Management, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/fun_c/fcprt3/fcd301.htm

Examples The following example shows how to enable SNMP network management traps to be sent to the specified host for the Cisco ITP. The example also increases the trap queue length (from the default of 10 events) to 100 events to reduce the possibility of dropping traps.

```
snmp-server enable traps cs7
snmp community public R0
snmp host 64.102.86.159 version 2c public
snmp-server queue-length 100
```

Related Commands	Command	Description
	snmp-server enable traps bits-clock	Enables SNMP to generate notifications about the building integrated timing supply (BITS) clocking sources and modes of operations.

snmp-server enable traps sctp

To enable Simple Network Management Protocol (SNMP) SCTP traps to be sent, use the **snmp-server enable traps sctp** global configuration command. To disable the sending of traps, use the **no** form of this command.

snmp-server enable traps sctp [**dest-address-state**]

no snmp-server enable traps sctp [**dest-address-state**]

Syntax Description	dest-address-state Enables the destination address state change trap.	
Defaults	None.	
Command Modes	Global configuration	
Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	
Examples	The following example shows how to enable the destination address state change trap: snmp-server enable traps sctp dest-address-state	
Related Commands	Command	Description
	snmp-server enable traps bits-clock	Enables SNMP to generate notifications about the building integrated timing supply (BITS) clocking sources and modes of operations.

To specify SSCF NNI parameters for the CS7 HSL profile, use the **sscf-nni** *cs7 hsl* profile command. To remove the configuration, use the **no** form of this command.

sscf-nni {**force-proving** *minutes* | **n1** *number* | **no-credit** *seconds* | **nrp** *number* | **sscop-recovery** *minutes* | **t1** *seconds* | **t2** *seconds* | **t3** *milliseconds*}

no sscf-nni {**force-proving** *minutes* | **n1** *number* | **no-credit** *seconds* | **nrp** *number* | **sscop-recovery** *minutes* | **t1** *seconds* | **t2** *seconds* | **t3** *milliseconds*}

Syntax Description

force-proving <i>minutes</i>	Specifies the time (in minutes) to monitor the link after proving. The range is 0 to 20 minutes. The default is 10 minutes.
n1 <i>number</i>	Specifies the number of PDUs sent during proving. The range is 5 to 180000 PDUs. The default for ITU is 1000 PDUs. The default for ANSI is 60000 PDUs.
no-credit <i>seconds</i>	Specifies the time (in seconds) allowed with no credit. The range is 1 to 6 seconds. The default is 2 seconds.
nrp <i>number</i>	Specifies the maximum number of retransmissions allowed during proving. The range is 1 to 10 retransmissions. The default is 1 retransmission.
sscop-recovery <i>minutes</i>	Specifies the time (in minutes) for SSCOP recovery. The range is 30 to 1440 minutes. The default is 60 minutes.
t1 <i>seconds</i>	Specifies the time (in seconds) to reestablish connection. The range is 1 to 15 seconds. The default is 5 seconds.
t2 <i>seconds</i>	Specifies the time (in seconds) for alignment to complete. The range is 15 to 180 seconds. The default for ITU is 30 seconds. The default for ANSI is 120 seconds.
t3 <i>milliseconds</i>	Specifies the time (in milliseconds) to send proving packets. The range is 1 to 5000 milliseconds. The default is 1 millisecond.

Defaults

The default for **force-proving** *minutes* is 10 minutes.
The default for **n1** *number* is 1000 (ITU) or 60000 (ANSI).
The default for **no-credit** *seconds* is 2 seconds.
The default for **nrp** *number* is 1 retransmission.
The default for **sscop-recovery** *minutes* is 60 minutes.
The default for **t1** *seconds* is 5 seconds.
The default for **t2** *seconds* is 30 milliseconds (ITU) or 120 seconds (ANSI).
The default for **t3** *milliseconds* is 1 millisecond.

Command Modes

cs7 hsl profile, cs7 linkset

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

SSCF NNI parameters can be configured in either a CS7 HSL profile or individually under a link.

Related Commands	Command	Description
	show sscf-nni	Displays SSCF information.

sscop

To specify SSCOP parameters for the CS7 HSL profile, use the **sscop cs7 hsl** profile command.
To remove the configuration, use the **no** form of this command.

sscop {**cc-timer** *msecs* | **idle-timer** *msecs* | **keepalive-timer** *msecs* | **max-cc** *number* | **max-pd** *number* | **noResponse-timer** *msecs* | **poll-timer** *msecs* | **receive-window** *number* | **send-window** *number*}

no sscop {**cc-timer** *msecs* | **idle-timer** *msecs* | **keepalive-timer** *msecs* | **max-cc** *number* | **max-pd** *number* | **noResponse-timer** *msecs* | **poll-timer** *msecs* | **receive-window** *number* | **send-window** *number*}

Syntax Description		
cc-timer <i>msecs</i>		Specifies the time (in milliseconds) to send BGN/END/RS/ER PDU at the connection control phase. The range is 100 to 2000 milliseconds. The default is 200 milliseconds.
idle-timer <i>msecs</i>		Specifies the time (in milliseconds) to send poll PDU at the idle phase. The range is 25 to 1000 milliseconds. The default is 100 milliseconds.
keepalive-timer <i>msecs</i>		Specifies the time (in milliseconds) to send poll PDU at the transient phase. The range is 25 to 500 milliseconds. The default is 100 milliseconds.
max-cc <i>number</i>		Specifies the maximum number of retries for connection control operations. The range is 1 to 127 retries. The default is 4 retries.
max-pd <i>number</i>		Specifies the maximum number of Sd frames to send before sending a Poll. The range is 1 to 500 Sd frames. The default is 500 Sd frames.
noResponse-timer <i>msecs</i>		Specifies the time (in milliseconds) in which at least one STAT PDU must be received. The range is 200 to 2000 milliseconds. The default is 1500 milliseconds.
poll-timer <i>msecs</i>		Specifies the times (in milliseconds) to send poll PDU at the active phase. The range is 25 to 500 milliseconds. The default is 100 milliseconds.
receive-window <i>number</i>		Specifies the maximum number of Sd(p) frames a partner can send. The range is 1 to 1024 Sd(p) frames. The default is 1024 Sd(p) frames.
send-window <i>number</i>		Specifies the maximum number of Sd frames to send before waiting for acknowledgement. The range is 1 to 1024 Sd frames. The default is 1024 Sd frames.

Defaults

The default for **cc-timer** is 200 milliseconds.

The default for **idle-timer** is 100 milliseconds.

The default for **keepalive-timer** is 100 milliseconds.

The default for **max-cc** is 4 retries.

The default for **max-pd** is 500 Sd frames.

The default for **noResponse-timer** is 1500 milliseconds.

The default for **poll-timer** is 100 milliseconds.

The default for **receive-window** is 1024 SD(p) frames.

The default for **send-window** is 1024 frames.

Command Modes cs7 hsl profile, cs7 linkset

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines SSCOP parameters can be configured in either a CS7 HSL profile or individually under a link.

teleservice

To specify a particular service identifier value for an **smdpp**, **sri-sm**, or **sms-notify** operation, use the **teleservice** command in cs7 mlr ruleset configuration mode. To remove the configuration, use the **no** form of this command.

teleservice *id*

no teleservice

Syntax Description	<i>id</i> An integer ranging from 0 to 65535.						
Defaults	None.						
Command Modes	cs7 mlr ruleset configuration						
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>12.2(18)IXA</td><td rowspan="3">This command was introduced.</td></tr><tr><td>12.4(11)SW</td></tr><tr><td>12.2(33)IRA</td></tr></table>	Release	Modification	12.2(18)IXA	This command was introduced.	12.4(11)SW	12.2(33)IRA
Release	Modification						
12.2(18)IXA	This command was introduced.						
12.4(11)SW							
12.2(33)IRA							
Usage Guidelines	The value of the teleservice maps to the values specified for the SMS TeleserviceIdentifier parameter in IS-41.						
Examples	The following example shows how to set the teleservice ID to 500: <pre>teleservice 500</pre>						
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>cs7 mlr ruleset</td><td>Specifies a set of rules used to process traffic-matching triggers defined in an MLR table.</td></tr></table>	Command	Description	cs7 mlr ruleset	Specifies a set of rules used to process traffic-matching triggers defined in an MLR table.		
Command	Description						
cs7 mlr ruleset	Specifies a set of rules used to process traffic-matching triggers defined in an MLR table.						

threshold-rcvd

To configure the receive threshold for a link, use the **threshold-rcvd** *cs7* link submode command. To remove the configuration, use the **no** form of this command.

threshold-rcvd *percent*

no threshold-rcvd *percent*

Syntax Description	<i>percent</i>	Sets the receive threshold for trap generation as a percentage. The range is 0 to 100 percent.

Defaults	The threshold defaults to the value specified by the cs7 util-threshold global command.

Command Modes	cs7 link submode

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	This command is required only when the value specified by the cs7 util-threshold global command is not appropriate for a particular link.

Examples	The following example shows how to set the receive threshold for link 0 to 50 percent:

```
cs7 linkset michael 10.1.1
  link 0 sctp 172.18.44.147 7000 7000
    threshold-rcvd 50
```

Related Commands	Command	Description
	cs7 util-abate	Specifies the integer range utilization threshold.
	cs7 util-threshold	Specifies the global threshold for link utilization.
	plan-capacity-rcvd	Specifies the link receive planning capacity.
	plan-capacity-send	Specifies the link send planning capacity.
	threshold-send	Specifies the send threshold for a link.

threshold-send

To configure the send threshold for a link, use the **threshold-send** *cs7* link submode command. To remove the configuration, use the **no** form of this command.

threshold-send *percent*

no threshold-send *percent*

Syntax Description	<i>percent</i>	Sets the send threshold for trap generation as a percentage. The range is 0 to 100 percent.

Defaults	The threshold defaults to the value specified by the cs7 util-threshold global command.

Command Modes	<i>cs7</i> link submode

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	This command is required only when the value specified by the cs7 util-threshold global command is not appropriate for a particular link.

Examples	The following example shows how to set the send threshold for link 0 to 50 percent:

```
cs7 linkset michael 10.1.1
  link 0 sctp 172.18.44.147 7000 7000
    threshold-send 50
```

Related Commands	Command	Description
	cs7 util-abate	Specifies the integer range utilization threshold.
	cs7 util-threshold	Specifies the global threshold for link utilization.
	plan-capacity-rcvd	Specifies the link receive planning capacity.
	plan-capacity-send	Specifies the link send planning capacity.
	threshold-rcvd	Specifies the receive threshold for a link.

timeout-count

To set the number of times the ITP retries the ping before marking the DCS node as unavailable, use the **timeout-count** cs7 dcs configuration submode command. To stop the action, use the **no** form of this command.

timeout-count *count*

no timeout-count

Syntax Description

<i>count</i>	Number of times the ITP retries the ping before marking the DCS node as unavailable.

Defaults

The default rate is 3 retries.

Command Modes

cs7 dcs configuration submode

Command History

Release	Modification
12.4(15)SW3	This command was introduced.
12.2(33)IRC	

Examples

The following example shows how to configure two ping retries between the remote IP address and the local IP address:

```
cs7 dcs dcs5
 remote-ip 209.165.201.29 209.165.201.28 3033
 local-ip 1209.165.20127 3033
 ping-interval 5
 timeout-count 2
 udp-checksum
```

Related Commands!

Command	Description
cs7 pmp	Turns probeless monitoring on for all linksets and ASes.
cs7 pmp hold-queue	Sets the integer range of PMP hold queue thresholds.
cs7 dcs-group	Identifies a name to be associated with a DCS group.
cs 7 dcs	Identifies a name to be associated with a DCS node.
show cs7 pmp	Displays errors and information about the PMP.
show cs7 dcs-group	Displays information about the DCS group.
show cs7 dcs	Displays information about the DCS node.

timer (cs7 hs-mtp2 profile)

You can define high-speed MTP2 timers in a CS7 profile and apply the profile to a linkset. To configure high-speed MTP2 encapsulation timers in a CS7 profile, use the **timer** command in cs7 hs-mtp2 profile configuration mode. To reset the timers, use the **no** form of this command.

```
timer {t1 msec | t2 msec | t3 msec | t4e msec | t4n msec | t5 msec | t6 msec | t7 msec | t8 msec}
```

```
no timer {t1 msec | t2 msec | t3 msec | t4e msec | t4n msec | t5 msec | t6 msec | t7 msec | t8 msec}
```

Syntax Description	
t1	Alignment ready timer. ANSI range: 165 to 200 seconds. Default is 170 seconds. ITU range: 25 to 350 seconds. Default is 300 seconds.
t2	Not aligned timer. ANSI range: 5 to 14 seconds. Default is 11.5 seconds. ITU range: 5 to 150 seconds. Default is 5 seconds.
t3	Aligned timer. ANSI range: 5 to 14 seconds. Default is 11.5 seconds. ITU range: 1 to 2 seconds. Default is 1.5 seconds.
t4e	Emergency proving period timer. ANSI range: 4.5 to 5.5 seconds. Default is 5 seconds. ITU range: 400 to 600 milliseconds. Default is 500 milliseconds.
t4n	Normal proving period timer. ANSI range: 27 to 33 seconds. Default is 30 seconds. ITU range: 3 to 70 seconds. Default is 30 seconds.
t5	Sending SIB timer. ANSI range: 80 to 120 milliseconds. Default is 100 milliseconds. ITU range: 80 to 120 milliseconds. Default is 100 milliseconds.
t6	Remote congestion timer. ANSI range: 1 to 6 seconds. Default is 1 second. ITU range: 3 to 6 seconds. Default is 3 seconds.
t7	Excessive delay of acknowledgment timer. ANSI range: 500 to 2000 milliseconds. Default is 1000 milliseconds. ITU range: 500 to 2000 milliseconds. Default is 1000 milliseconds.
t8	Interval timer for errored interval monitor. ANSI range: 80 to 12000 milliseconds. Default is 100 milliseconds. ITU range: 80 to 12000 milliseconds. Default is 100 milliseconds.

Defaults

T1: ANSI = 170 seconds; ITU = 300 seconds

T2: ANSI = 11.5 seconds; ITU = 5 seconds

T3: ANSI = 11.5 seconds; ITU = 1.5 seconds

T4E: ANSI = 5 seconds; ITU = 500 milliseconds

T4N: ANSI = 30 seconds; ITU = 30 seconds

T5: ANSI = 100 milliseconds; ITU = 100 milliseconds

T6: ANSI = 1 second; ITU = 3 seconds

■ timer (cs7 hs-mtp2 profile)

T7: ANSI = 1000 milliseconds; ITU = 1000 seconds

T8: ANSI = 100 milliseconds; ITU = 100 milliseconds

Command Modes cs7 hs-mtp2 profile configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

High-speed MTP2 parameters can also be specified in cs7 linkset configuration mode.

Examples

The following example shows how to define a profile named **TIMER**. The profile supports high-speed MTP2, configures the t1 and t2 settings, and applies to all the links in the linkset named **ITP_A**.

```
cs7 profile TIMERS
  hs-mtp2
    timer t1 100
    timer t2 10
.
.
.
cs7 linkset ITP_A
  profile TIMERS
```

Related Commands

Command	Description
cs7 profile	Defines a profile of MTP2 parameters that you can apply to all the links in a linkset.
tx-queue-depth (cs7 hs-mtp2 profile)	Configures the high-speed MTP2 transmit queue depth.

timer (cs7 linkset)

To configure the ITP MTP3 management timers that control the linkset (and, optionally, a link on the linkset), use the **timer** cs7 linkset submode command. To reset a timer to its default value, use the **no** form of this command.

```
timer { retry msec | slt-t01 msec | slt-t02 msec | t01 msec | t02 msec | t03 msec | t04 msec | t05 msec  
| t12 msec | t13 msec | t14 msec | t17 msec | t19 msec | t20 msec | t21 msec | t22 msec | t23 msec  
| t24 msec | t25 msec | t28 msec | t29 msec | t30 msec | t32 msec }
```

```
no timer { retry | slt-t1 | slt-t2 | t01 | t02 | t03 | t04 | t05 | t12 | t13 | t14 | t17 | t19 | t20 | t21 | t22 |  
t23 | t24 | t25 | t28 | t29 | t30 | t32 }
```



Note

Ranges are defined by ANSI or ITU.

Syntax Description

retry msec	(ANSI, ITU) Link activation retry timer. (ANSI, ITU) Range of msec is 60000 to 90000 milliseconds. Default is 60000 milliseconds.
slt-t01 msec	(ANSI, ITU) Link test acknowledgment timer. (ANSI, ITU) ITU Range of msec is 4000 to 12000 milliseconds. Default is 8000 milliseconds.
slt-t02 msec	(ANSI, ITU) Interval timer for sending test messages. (ANSI, ITU) Range of msec is 30000 to 90000 milliseconds. (ANSI, ITU) Default is 60000 milliseconds.
t01 msec	(ANSI, ITU) Delay to avoid message missequencing. (ANSI, ITU) Range of msec is 500 to 1200 milliseconds. (ANSI, ITU) Default is 800 milliseconds.
t02 msec	(ANSI, ITU) Wait for changeover acknowledgment. (ANSI, ITU) Range of msec is 700 to 2000 milliseconds. (ANSI, ITU) Default is 1400 milliseconds.
t03 msec	(ANSI, ITU) Delay to avoid missequencing in changeback. (ANSI, ITU) Range of msec is 500 to 1200 milliseconds. (ANSI, ITU) Default is 800 milliseconds.
t04 msec	(ANSI, ITU) Wait for changeback acknowledgment (first attempt). (ANSI, ITU) Range of msec is 500 to 1200 milliseconds. (ANSI, ITU) Default is 800 milliseconds.
t05 msec	(ANSI, ITU) Wait for changeback acknowledgment (second attempt). (ANSI, ITU) Range of msec is 500 to 1200 milliseconds. (ANSI, ITU) Default is 800 milliseconds.
t12 msec	(ANSI, ITU) Wait for uninhibited acknowledgment. (ANSI, ITU) Range of msec is 800 to 1500 milliseconds. (ANSI, ITU) Default is 1150 milliseconds.
t13 msec	(ANSI, ITU) Wait for force uninhibited. (ANSI, ITU) Range of msec is 800 to 1500 milliseconds. (ANSI, ITU) Default is 1150 milliseconds.

t14 <i>msec</i>	(ANSI, ITU) Wait for inhibition acknowledgment. (ANSI, ITU) Range of <i>msec</i> is 2000 to 3000 milliseconds. (ANSI, ITU) Default is 2500 milliseconds.
t17 <i>msec</i>	(ANSI, ITU) Delay to avoid oscillation of alignment failure and link restart. (ANSI, ITU) Range of <i>msec</i> is 800 to 1500 milliseconds. (ANSI, ITU) Default is 1150 milliseconds.
t19 <i>msec</i>	(ANSI) Failed link craft referral timer. (ANSI) Range of <i>msec</i> is 480000 to 600000 milliseconds. (ANSI) Default is 540000. (ITU) Supervision timer during MTP restart. (ITU) Range of <i>msec</i> is 67000 to 69000 milliseconds. (ITU) Default is 68000 milliseconds.
t20 <i>msec</i>	(ANSI) Waiting to repeat local inhibit test. (ANSI) Range of <i>msec</i> is 90000 to 120000 milliseconds. (ANSI) Default is 105000 milliseconds.
t21 <i>msec</i>	(ANSI) Waiting to repeat remote inhibit test. (ANSI) Range of <i>msec</i> is 90000 to 120000 milliseconds. (ANSI) Default is 105000 milliseconds. (ITU) MTP restart timer at signaling point adjacent to one whose MTP restarts. (ITU) Range of <i>msec</i> is 63000 to 65000 milliseconds. (ITU) Default is 64000 milliseconds.
t22 <i>msec</i>	(ITU) Local inhibit test timer. (ITU) Range of <i>msec</i> is 180000 to 360000 milliseconds. (ITU) Default is 300000 milliseconds.
t23 <i>msec</i>	(ITU) Remote inhibit test timer. (ITU) Range of <i>msec</i> is 180000 to 360000 milliseconds. (ITU) Default is 300000 milliseconds.
t24 <i>msec</i>	(ITU) Stabilizing timer after removal of local processor outage; used in LPO latching to RPO. (ITU) Range of <i>msec</i> is 400 to 600 milliseconds. (ITU) Default is 500 milliseconds.
t25 <i>msec</i>	(ANSI) Timer at SP adjacent to restarting SP, waiting for traffic restart allowed message. (ANSI) Range of <i>msec</i> is 30000 to 35000 milliseconds. (ANSI) Default is 30000 milliseconds.
t28 <i>msec</i>	(ANSI) Timer at SP adjacent to restarting SP, waiting for traffic restart waiting message. (ANSI) Range of <i>msec</i> is 3000 to 35000 milliseconds. (ANSI) Default is 30000 milliseconds.
t29 <i>msec</i>	(ANSI) Timer started when TRA sent in response to unexpected TRA or TRW. (ANSI) Range of <i>msec</i> is 60000 to 65000 milliseconds. (ANSI) Default is 63000 milliseconds.

t30 msec	(ANSI) Timer to limit sending TFPs and TFRs in response to unexpected TRA and TRW. (ANSI) Range of <i>msec</i> is 30000 to 35000 milliseconds. (ANSI) Default is 33000 milliseconds.
t32 msec	(ANSI) Link oscillation timer - Procedure A. Range of <i>msec</i> is 60000 to 120000 milliseconds. Default is 60000 milliseconds.

Defaults

See the defaults listed in Syntax Description.

Command Modes

cs7 linkset submode

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

MTP3 timers can be defined at three levels: global, linkset, and link.

All global, linkset, and link specific timers can be defined at the global level. These values serve as defaults and are propagated down to the lower levels.

All linkset and link specific timers can be defined at the linkset level. These values serve as defaults for the linkset and all links defined within that linkset. Any values defined here override any global values.

All timers defined at the link level apply to the link and override any values for that timer defined at either the linkset or global level.

Examples

The following example shows how to set the ITP MTP3 T1 timer to 1000 milliseconds:

```
timer t01 1000
```

Related Commands

Command	Description
cs7 mtp3 timer	Globally configures all MTP3 timers.
show cs7 linkset	Displays ITP linkset information.
link-timer	Configures timers for a link.

timer (cs7 profile)

Traditional SS7 links use serial interfaces. ITP interfaces can be configured to use encapsulation MTP2. You can define several MTP2 timers in a CS7 profile and apply the profile to a linkset.

To configure MTP2 encapsulation timers in a CS7 profile, use the **timer** command in cs7 profile configuration mode. To reset the timers, use the **no** form of this command.

timer {**t1** msec | **t2** msec | **t3** msec | **t4e** msec | **t4n** msec | **t5** msec | **t6** msec | **t7** msec | **ttc** timer msec }

no timer {**t1** msec | **t2** msec | **t3** msec | **t4e** msec | **t4n** msec | **t5** msec | **t6** msec | **t7** msec | **ttc** timer msec }



Note

Ranges are defined by ANSI or ITU.

Syntax Description

t1	Alignment ready timer. ANSI default is 13000 milliseconds. ITU default is 40000 milliseconds.
t2	Not aligned timer. ANSI default is 11500 milliseconds. ITU default is 5000 milliseconds.
t3	Aligned timer. ANSI default is 11500 milliseconds. ITU default is 1500 milliseconds.
t4e	Emergency proving period timer. ANSI default is 600 milliseconds. ITU default is 500 milliseconds.
t4n	Normal proving period timer. ANSI default is 2300 milliseconds. ITU default is 8200 milliseconds.
t5	Sending SIB timer. ANSI default is 80 milliseconds. ITU default is 100 milliseconds.
t6	Remote congestion timer. ANSI default is 1000 milliseconds. ITU default is 3000 milliseconds.
t7	Excessive delay of acknowledgment timer. ANSI default is 1000 milliseconds. ITU default is 1000 milliseconds.
ttc	ttc ta timer: TTC timer for sending SIE. Valid range is 10 to 250 milliseconds. Default is 20 milliseconds. ttc te timer: TTC timer for error monitoring. Valid range is 10 to 250 milliseconds. Default is 20 milliseconds. ttc tf timer: TTC timer for sending FISU. Valid range is 10 to 250 milliseconds. Default is 20 milliseconds. ttc to timer: TTC timer for sending SIO. Valid range is 10 to 250 milliseconds. Default is 20 milliseconds. ttc ts timer: TTC timer for sending SIOS. Valid range is 10 to 250 milliseconds. Default is 20 milliseconds.

Defaults

T1: ANSI = 13000; ITU = 40000

T2: ANSI = 11500; ITU = 5000

T3: ANSI = 11500; ITU = 1500

T4E: ANSI = 600; ITU = 500

T4N: ANSI = 2300; ITU = 8200

T5: ANSI = 80; ITU = 100

T6: ANSI = 1000; ITU = 3000

T7: ANSI= 1000; ITU = 1000

Command Modes cs7 profile configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines MTP2 parameters can also be specified in cs7 linkset configuration mode.

Examples The following example shows how to define a profile named timers. The profile supports MTP2, configures the t1 and t2 settings, and applies to all the links in the linkset named itpa.

```
cs7 profile timers
 mtp2
  timer t1 15000
  timer t2 9000
.
.
.
cs7 linkset itpa
 profile timers
```

Related Commands	Command	Description
	bundling (cs7 link)	Enables and configures message bundling.
	cs7 profile	Defines a profile of MTP2 parameters that you can apply to all the links in a linkset.
	show cs7 mtp2	Displays ITP MTP2 status.
	tx-queue-depth (cs7 link)	Configures the MTP2 transmit queue depth.

traffic-mode (cs7 as)

To identify the traffic mode of operation of the ASP within an AS, use the **traffic-mode** cs7 as submode command. To remove the configuration, use the **no** form of this command.

```
traffic-mode {broadcast | loadshare [bindings [sls [opc-sls [opc-shift {opc-shift-number}]] |
cgpa-sls | bind-sccp-class2] [redistribute-active] | cic [redistribute-active] ] | roundrobin] |
override}
```

```
[no] traffic-mode {broadcast | loadshare [bindings [sls [opc-sls [opc-shift {opc-shift-number}]] |
cgpa-sls | bind-sccp-class2] [redistribute-active] | cic [redistribute-active] ] | roundrobin] |
override}
```

Syntax Description		
broadcast		Broadcast mode. In broadcast mode, the ASP receives the same messages as any other currently active ASP.
loadshare		Loadshare mode. In loadshare mode, an ASP shares in the traffic distribution with any other currently active ASPs. You can load share based on ASP bindings or using a round-robin algorithm.
bindings		Loadshare based on ASP bindings. Default setting. Bindings are established for CIC and SLS values and bindings are not redistributed when they are active on the SGMP mate.
sls		Establishes SLS bindings only.
opc-sls		Extends SLS-based ASP binding to OPC-SLS combination-based binding.
opc-shift		Shifts the OPC bits that are used.
<i>opc-shift-number</i>		Number of OPC bits that are shifted. The range is 0 to 2 for ITU variants. The range is 0 to 8 for ANSI variants. The default number is 0.
cgpa-sls		Extends SLS-based ASP binding to CGPA-SLS combination-based binding.
bind-sccp-class2		Bind SCCP class 2 packets.
cic		Establishes CIC bindings only.
redistribute-active		Redistributes bindings to a newly active ASP even when the bindings are active on the SGMP mate.
roundrobin		Loadshare based on round-robin algorithm.
override		Override mode. In override mode, one ASP takes over all traffic for an AS (primary/backup operation), possibly overriding any currently active ASP in the AS.

Defaults Load sharing is based on ASP bindings.

Command Modes cs7 as submode

Command History	Release	Modification
	12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.
	12.2(18)IXG 12.4(15)SW2 12.2(33)IRB	The cic , sls , and redistribute-active keywords were introduced.
	12.2(18)IXH 12.4(15)SW3 12.2(33)IRC	The opc-sls , opc-shift , and cgpa-sls keywords were introduced.
	12.4(15)SW9 12.2(33)IRI	The bind-sccp-class2 keyword was introduced.

Usage Guidelines None.

Syntax Description

Usage guidelines for this command fall into two categories, general and loadshare binding.

- **General usage**

Generally, this command is used to validate the traffic mode specified on ASP Active messages. ASPs fail if they connect with a different traffic mode.

The traffic mode type supported by an AS is determined dynamically. For example, if the first valid ASP Active message received from an ASP in the AS has the traffic mode type set to loadshare, the traffic mode of the AS is set to loadshare.

If no traffic mode is specified, bindings are established for CIC and SLS values and are not redistributed when they are active on the mate ITP.

- **Loadshare binding usage**

In loadshare binding mode, you can configure the **sls** and/or **cic** keyword so that traffic binds to an ASP according to those keywords. The **sls** keyword includes the following options:

- The **opc-sls** keyword extracts more bits from the OPC.
- The **opc-shift** keyword specifies where the OPC bits are extracted. For variants with a 14-bit pc format (ITU), the shift range is 0 to 2, which ensures that 12 significant bits are extracted. For variants with a 24-bit pc format (ANSI), the shift range is 0 to 8, which ensures 16 significant bits.

If the **cgpa-sls** keyword is specified, more bits are calculated from CgPA digits and combined with the SLS to generate a new hash value. The **bind-sccp-class2** keyword enables loadshare binding for SCCP class 2 packets.

If **sls** or **cic** is not specified, traffic binds according to the SLS and CIC based on the traffic type. You can specify **opc-sls** and **cgpa-sls** to indicate that SLS-based binding extends.

For traffic types such as BISUP, Satellite ISUP, AAL type 2 signaling, or GCP, only OPC-SLS options apply.

When you configure the traffic mode for an AS, if the AS's routing key is specified and the SI indicates the above SLS-based traffic type, the **cgpa-sls** keyword is not displayed. You can configure the traffic mode and specify the **cgpa-sls** keyword before the routing key configuration. Now, when

Examples

The following example shows how to set the traffic mode to loadshare mode:

```
cs7 as BLUE m3ua
  routing-key 100 10.3.8
  asp ASP1
  asp ASP2
  traffic-mode loadshare
```

The following example shows how to set the traffic mode to loadshare mode and the ASP bindings to use opc-sls with opc-shift or CIC:

```
cs7 instance 1 as AS1 m3ua
  routing-key 200 2.0.0
  asp asp1 weight 10
  asp asp2
  traffic-mode loadshare bindings opc-sls opc-shift 1
!
```

The following example shows how to set the traffic mode to loadshare mode and the ASP bindings to use cgpa-sls or CIC.

```
cs7 instance 1 as AS2 m3ua
  routing-key 201 2.0.1
  asp asp1 weight 10
  asp asp2
  traffic-mode loadshare bindings cgpa-sls
!
```

The following example shows how to set the traffic mode to loadshare mode and the ASP bindings to only use opc-sls with opc-shift:

```
cs7 instance 1 as AS3 m3ua
  routing-key 202 2.0.2
  asp asp1 weight 10
  asp asp2
  traffic-mode loadshare bindings sls opc-sls opc-shift 1
!
```

The following example shows how to set the traffic mode to loadshare mode and the ASP bindings to only use cgpa-sls:

```
cs7 instance 1 as AS4 m3ua
  routing-key 203 2.0.3
  asp asp1 weight 10
  asp asp2
  traffic-mode loadshare bindings sls cgpa-sls
!
```

Related Commands

Command	Description
cs7 as	Defines an application server (AS) and enters cs7 as submode.
cs7 asp	Specifies an application server process (ASP) and enables cs7 asp submode.
cs7 m3ua	Specifies the local port number for M3UA and enters cs7 m3ua submode.
cs7 sua	Specifies the local port number for SUA and enters cs7 sua submode.

traffic-rate-timer

To configure the data collection interval that is used to calculate traffic rate information, use the **traffic-rate-timer** command in cs7 sms route table configuration mode. To remove the configuration, use the **no** form of this command.

traffic-rate-timer *timer*

no traffic-rate-timer *timer*

Syntax Description	<i>timer</i>	Data collection interval, in seconds. Valid range is 60 to 3600 seconds. The default is 600 seconds.

Defaults	600 seconds

Command Modes	cs7 sms route table configuration.

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples	The following example shows how to set the traffic rate timer to an interval of 120 seconds:

```
cs7 sms route-table
 traffic-rate-timer 120
```

Related Commands	Command	Description
	show cs7 sms statistics	Displays SMS statistics.

transaction-timer (cs7 sms route table)

To specify the amount of time in seconds that DSMR allows any message transaction to remain open, use the **transaction-timer** command in cs7 sms route table configuration mode. To remove the configuration, use the **no** form of this command.

transaction-timer *seconds*

no transaction-timer

Syntax Description	<i>seconds</i> Maximum lifetime of a message transaction. Valid range is 5 to 3600 seconds. The default is no limit.	
Defaults	The transaction timer is disabled and there is no limit to the maximum lifetime of a message transaction.	
Command Modes	cs7 sms route table configuration	
Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	
Examples	The following example shows how to configure an SMS route table and specify a CDR service. DSMR will allow a message transaction to remain open for 120 seconds. cs7 sms route-table cdr-service cdrserv1 transaction-timer 120	
Related Commands	Command	Description
	cs7 sms route-table	Specifies an SMS route table.

trigger cdpa (cs7 mlr table)

To specify the routing key, or trigger, for a multilayer SMS routing table and indicate that the routing trigger is located in the SCCP called party address (CdPA) field of the incoming MSU, use the **trigger cdpa** command in cs7 mlr table mode. To delete a specific routing trigger, use the **no** form of this command.

```
trigger cdpa {gt addr-string [gt-addr-type] | pc point-code ssn ssn} [block | continue | ruleset
ruleset-name | result {pc pc [ssn ssn] | asname as-name | gt gt [gt-addr-type] | group
group-name}]
```

```
no trigger cdpa
```

Syntax Description	
gt	Indicates that the CdPA trigger being defined is received with RI=GT.
<i>addr-string</i>	Address string of 1 to 15 hexadecimal characters. The string is input in normal form instead of BCD-String format.
<i>gt-addr-type</i>	Parameters that identify attributes of the global title address being used as a trigger. The parameters are variant-specific, and are identical to those parameters specified on the cs7 gtt selector command. If not specified, the default is the standard E.164 address type for the network variant being used.
	tt <i>tt</i> [gti <i>gti</i>] [np <i>np</i> nai <i>nai</i>]
	tt Identifies the translation type specified within the address.
	<i>tt</i> An integer value from 0 to 255.
	gti Identifies the global title indicator value for the specified address. This value is specified only when the cs7 variant command specifies ITU or China.
	<i>gti</i> Integer value of 2 or 4.
	np Identifies the numbering plan of the specified address. Used only when the <i>gti</i> value is 4.
	<i>np</i> Integer value from 0 to 15.
	nai Identifies the nature of address indicator. Used only when the <i>gti</i> value is 4.
	<i>nai</i> Integer value from 0 to 127.
pc	Matches the trigger if it contains the specified point code. The PC within the SCCP CdPA is inspected first. If the PC is not present, then the DPC in the routing label is used.
<i>point-code</i>	Point code in variant-specific point code format.
ssn	Matches the trigger if it contains the specified subsystem.
<i>ssn</i>	Subsystem number in decimal. Valid range is 2 to 255.
block	Drops messages matching this trigger. This keyword is ignored if combination triggers are defined within cs7 mlr trigger configuration submode.

■ trigger cdpa (cs7 mlr table)

continue	Routes messages matching this trigger as received. This behavior is the same as if no primary trigger had been matched. This keyword is ignored if combination triggers are defined within cs7 mlr trigger mode.
ruleset	Specifies the MLR ruleset table that should be used if this trigger is matched and not overruled by a secondary trigger ruleset. This keyword is ignored if combination triggers are defined within cs7 mlr trigger mode.
<i>ruleset-name</i>	Name of a defined CS7 MLR ruleset table. The name is specified as a character string with a maximum of 12 characters.
result	Routes messages based on the trigger alone. If a trigger result is configured, the TCAP/MAP/SMS layers are not parsed. If a message matches a trigger with a result trigger action, then the message is redirected as indicated in the trigger result. Note: Result groups with dest-sme-binding mode are not valid trigger results.
pc	Routes based on point code.
<i>pc</i>	Point code.
ssn	Routes based on PC and subsystem number.
<i>ssn</i>	Subsystem number.
asname	Routes based on AS name.
<i>as-name</i>	AS name.
gt	Routes based on global title.
<i>gt</i>	Global title address.
group	Routes based on result group.
<i>group-name</i>	Result group name.

Defaults

If you configure a default trigger with the **trigger default** command, it is defined as the last trigger in the MLR table. The default trigger is used only if all other triggers are unmatched. If a default trigger is not configured, then packets not matching a trigger are routed according to standard SCCP or MTP3 procedures.

Command Modes

cs7 mlr table

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The **trigger cdpa** command configures a primary routing key to route or block messages based on the CdPA. (If no primary triggers are specified, the MLR table will not be created.)

Trigger Rules

- Trigger values must be unique.

- **cdpa gt** triggers must specify a defined GTT GTA or GTT selector entry.

Trigger Match Hierarchy

If primary CdPA and CgPA triggers are configured, the triggers are not searched sequentially. The first trigger match is used based on the following hierarchy:

1. The defined default trigger (the only trigger configured)
2. SCCP CdPA GT address
3. SCCP CdPA GT selector
4. SCCP CdPA PC/SSN
5. SCCP CgPA GT address
6. SCCP CgPA GT selector
7. SCCP CgPA PC/SSN

Trigger Terminology

[Table 91](#) describes the types of triggers and the commands you use to specify triggers at various configuration levels.

Table 91 **Trigger Terminology**

Term	Definition
trigger	A trigger represents the SS7 network-layer routing parameters that are used to efficiently identify traffic requiring parsing into the application layers.
primary trigger	The primary trigger represents the network-layer information that is first compared to an incoming packet for possible MLR routing. A primary trigger is specified in cs7 mlr table mode (after the cs7 mlr table command has been specified). The following example shows how to specify a primary trigger. (Note that the CLI prompt changes to indicate that cs7 mlr trigger mode has been enabled.) <pre>Router(config-cs7 mlr)# trigger mtp3 dpc 1-1-1 Router(cfg-cs7-mlr-trigger)#</pre> Primary trigger values must be unique. Possible primary trigger commands are trigger cdpa, trigger cgpa, trigger default, and trigger mtp3. MTP3 may be specified as a primary trigger only.

Table 91 **Trigger Terminology (continued)**

secondary trigger	A secondary trigger is specified in cs7 mlr trigger mode (after the primary trigger has been specified). If one or more secondary triggers are specified, then the primary <i>and</i> one of the secondary trigger values must match for MLR to further process the message. If no secondary triggers are specified, then the primary trigger alone is used for MLR processing. Secondary triggers are matched sequentially in the order in which they are defined. The following example shows how to specify a secondary trigger. Note that configuring a secondary trigger does not enable a new mode. The prompt does not change. <pre>Router(cfg-cs7-mlr-trigger)# cgpa pc 1-1-1 ssn 11 Router(cfg-cs7-mlr-trigger)#</pre> Secondary triggers do not have to be unique. Possible secondary trigger commands are cdpa, cgpa, and default. The primary trigger must be for a called party for the cgpa submode command to be valid. The primary trigger must be for a calling party for the cdpa submode command to be valid.
tertiary trigger	A tertiary trigger is specified in cs7 mlr trigger mode (after the secondary trigger has been specified). If a tertiary trigger is specified, then one of the primary, secondary, <i>and</i> tertiary trigger values must match for MLR to further process the message. If no tertiary triggers are specified, then the primary and secondary triggers are only used for MLR processing. Tertiary triggers are matched sequentially in the order in which they are defined. The following example shows how to specify a tertiary trigger. Note that configuring a tertiary trigger does not enable a new mode. The prompt does not change. <pre>Router(cfg-cs7-mlr-trigger)#cgpa pc 2-2-2 ssn 8</pre> Tertiary triggers need not be unique. Possible tertiary trigger commands are cdpa, cgpa, and default.
subtrigger	A subtrigger is a generic term used to describe a trigger defined within another trigger's submode. A default trigger cannot have subtriggers.
combination trigger	A combination trigger is a composite MLR trigger comprised of more than one trigger. The two possible combination triggers are primary+secondary or primary+secondary+tertiary. When a combination trigger is matched, the trigger action defined on the lowest trigger in the hierarchy is used for MLR processing.

Examples

The following example shows how to specify a trigger to route messages based on the CdPA field of the incoming MSU. The trigger is specified for the table named SMS-TABLE.

```
cs7 mlr table SMS-TABLE
trigger cdpa gt 9991117770 ruleset ruleset1
```


The following example shows how to configure triggers to block messages based on a specified CdPA. The trigger is specified for the table named SMS-BLOCKING.

```
cs7 mlr table SMS-BLOCKING
trigger cdpa gt 9991117770 tt 10 block
```

Related Commands

Command	Description
cgpa	Creates a secondary trigger based on the CgPA, to be used with a primary trigger based on the CdPA.
cs7 mlr table	Specifies the name of the multilayer SMS routing table and enables cs7 mlr table mode.
trigger cgpa (cs7 mlr table)	Specifies a primary routing trigger that is located in the SCCP calling party address field of the incoming MSU.

trigger cgpa (cs7 mlr table)

To specify the routing key, or trigger, for a multilayer SMS routing table and indicate that the routing trigger is located in the SCCP calling party address (CgPA) field of the incoming MSU, use the **trigger cgpa** command in cs7 mlr table mode. To delete the trigger command and disable the specific routing trigger, use the **no** form of this command.

```
trigger cgpa {gt addr-string [gt-addr-type] | pc point-code ssn ssn} [block | continue | ruleset
ruleset-name | result {pc pc [ssn ssn] | asname as-name | gt gta [gt-addr-type] | group
group-name}]
```

```
no trigger cgpa
```

Syntax Description	
gt	Indicates that the CgPA trigger being defined is received with RI=GT.
<i>addr-string</i>	Address string of 1 to 15 hexadecimal characters. The string is input in normal form instead of BCD-String format.
<i>gt-addr-type</i>	Parameters that identify attributes of the global title address being used as a trigger. The parameters are variant-specific, and are identical to those parameters specified on the cs7 gtt selector command. If not specified, the default is the standard E.164 address type for the network variant being used.
	tt <i>tt</i> [gti <i>gti</i>] [np <i>np</i> nai <i>nai</i>]
	tt Identifies the translation type specified within the address.
	<i>tt</i> An integer value from 0 to 255.
	gti Identifies the global title indicator value for the specified address. This value is specified only when the cs7 variant command specifies ITU or China.
	<i>gti</i> Integer value of 2 or 4.
	np Identifies the numbering plan of the specified address. Used only when the <i>gti</i> value is 4.
	<i>np</i> Integer value from 0 to 15.
	nai Identifies the nature of address indicator. Used only when the <i>gti</i> value is 4.
	<i>nai</i> Integer value from 0 to 127.
pc	Matches the trigger if it contains the specified point code. The PC within the SCCP CgPA is inspected first. If the PC is not present, then the OPC is used.
<i>point-code</i>	Point code in variant-specific point code format.
ssn	Matches the trigger if it contains the specified subsystem.
<i>ssn</i>	Subsystem number in decimal. Valid range is 2 to 255.
block	Drops messages matching this trigger. This keyword is ignored if combination triggers are defined within cs7 mlr trigger configuration submode.

continue	Routes messages matching this trigger as received. This behavior is the same as if no primary trigger had been matched. The continue keyword is ignored if combination triggers are defined within cs7 mlr trigger mode.
ruleset	Uses the specified MLR ruleset table if this trigger is matched and not overruled by a secondary trigger ruleset. The ruleset keyword is ignored if combination triggers are defined within cs7 mlr trigger mode.
<i>ruleset-name</i>	Name of a defined CS7 MLR ruleset table. The name is specified as a character string with a maximum of 12 characters.
result	Routes messages based on the trigger alone. If a trigger result is configured, the TCAP/MAP/SMS layers are not parsed. If a message matches a trigger with a result trigger action, then the message is redirected as indicated in the trigger result. Note: Result groups with dest-sme-binding mode are not valid trigger results.
pc	Routes based on point code.
<i>pc</i>	Point code.
ssn	Routes based on PC and subsystem number.
<i>ssn</i>	Subsystem number.
asname	Routes based on AS name.
<i>as-name</i>	AS name.
gt	Routes based on global title.
<i>gta</i>	Global title address.
group	Routes based on result group.
<i>group-name</i>	Result group name.

Defaults

If you configure a default trigger with the **trigger default** command, it is defined as the last trigger in the MLR table. The default trigger is used only if all other triggers are unmatched. If a default trigger is not configured, then packets not matching a trigger are routed according to standard SCCP or MTP3 procedures.

Command Modes

cs7 mlr table

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

The **trigger cgpa** command configures a primary routing key to route or block messages based on the CgPA. (If no primary triggers are specified, the MLR table will not be created.)

If primary CdPA and CgPA triggers are configured, the triggers are not searched sequentially. The first trigger match is used based on the following hierarchy:

1. The defined default trigger (the only trigger configured)

2. SCCP CdPA GT address
3. SCCP CdPA GT selector
4. SCCP CdPA PC/SSN
5. SCCP CgPA GT address
6. SCCP CgPA GT selector
7. SCCP CgPA PC/SSN

Trigger Rules

- Primary trigger values must be unique.
- **cdpa gt** triggers must have a matching GTT GTA or GTT selector entry.

Examples

The following example shows how to specify a trigger to route messages based on the CgPA field of the incoming MSU. The trigger is specified for the table named SMS-TABLE.

```
cs7 mlr table SMS-TABLE
trigger cgpa gt 9991117770 ruleset ruleset1
```

The following example shows how to configure triggers to block messages based on a specified CgPA. The trigger is specified for the table named SMS-BLOCKING.

```
cs7 mlr table SMS-BLOCKING
trigger cgpa gt 9991117770 tt 10 block
```

Related Commands

Command	Description
cgpa	Creates a secondary trigger based on the CgPA, to be used in conjunction with a primary trigger based on the CdPA.
cs7 mlr table	Specifies the name of the multilayer SMS routing table and enables cs7 mlr table mode.
trigger cdpa (cs7 mlr table)	Specifies a primary routing trigger that is located in the SCCP CdPA field of the incoming MSU.

trigger default

To specify a trigger to match all packets received, use the **trigger default** command in cs7 mlr table mode. To delete a specific routing trigger, use the **no** form of this command.

trigger default [**block** | **continue** | **ruleset** *ruleset-name*] **result** { **pc** *pc* [**ssn** *ssn*] | **asname** *as-name* | **gt** *gt* [*gt-addr-type*] | **group** *group-name*]

no trigger default

Syntax	Description
block	Drops messages matching this trigger. The block keyword is ignored if combination triggers are defined within cs7 mlr trigger mode.
continue	Routes messages matching this trigger as received. This behavior is the same as if no primary trigger had been matched. The continue keyword is ignored if combination triggers are defined within cs7 mlr trigger mode.
ruleset	Uses the specified MLR ruleset table if this trigger is matched and not overruled by a secondary trigger ruleset. The ruleset keyword is ignored if combination triggers are defined within cs7 mlr trigger mode.
<i>ruleset-name</i>	Name of a defined CS7 MLR ruleset table. The name is specified as a character string with a maximum of 12 characters.
result	Routes messages based on the trigger alone. If a trigger result is configured, the TCAP/MAP/SMS layers are not parsed. If a message matches a trigger with a result trigger action, then the message is redirected as indicated in the trigger result. Note: Result groups with dest-sme-binding mode are not valid trigger results.
pc	Routes based on point code.
<i>pc</i>	Point code.
ssn	Routes based on PC and subsystem number.
<i>ssn</i>	Subsystem number.
asname	Routes based on AS name.
<i>as-name</i>	AS name.
gt	Routes based on global title.
<i>gt</i>	Global title address.

<i>gt-addr-type</i>	Parameters that identify attributes of the global title address being used as a trigger. The parameters are variant-specific, and are identical to those parameters specified on the cs7 gtt selector command. If not specified, the default is the standard E.164 address type for the network variant being used. tt tt [gti gti] [np np nai nai] tt Identifies the translation type specified within the address. <i>tt</i> An integer value from 0 to 255. gti Identifies the global title indicator value for the specified address. This value is specified only when the CS7 variant is ITU or China. <i>gti</i> Integer value of 2 or 4. np Identifies the numbering plan of the specified address. Specified only when the <i>gti</i> value is 4. <i>np</i> Integer value from 0 to 15. nai Identifies the nature of address indicator. Specified only when the <i>gti</i> value is 4. <i>nai</i> Integer value from 0 to 127.
group	Routes based on result group.
<i>group-name</i>	Result group name.

Defaults

None.

Command Modes

cs7 mlr table

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage GuidelinesThe **trigger default** command enables cs7 mlr trigger mode.**Examples**

The following example shows how to match the trigger to all packets received. The trigger is specified for the table named SMS-TABLE.

```
cs7 mlr table SMS-TABLE
  trigger default ruleset ruleset1
```

Related Commands

Command	Description
cs7 mlr table	Specifies the name of the multilayer SMS routing table and enables cs7 mlr table mode.

trigger mtp3

To specify the routing key, or trigger, for a multilayer SMS routing table and indicate that the trigger is based on an MTP3 routing label field, use the **trigger mtp3** cs7 mlr table mode command. To delete the trigger command and disable the specific routing trigger, use the **no** form of this command.

```
trigger mtp3 {[dpc point-code] [opc point-code] [si indicator]} [block | continue | ruleset
ruleset-name | result {pc pc [ssn ssn] | as-name | gt gta [gt-addr-type] | group group-name}]
```

```
no trigger mtp3
```

Syntax Description		
dpc		Locates the trigger within the MTP3 destination point code field of the routing label.
<i>point-code</i>		The point code in instance-specific point code format.
opc		Locates the trigger within the MTP3 origination point code field of the routing label.
<i>point-code</i>		The point code in instance-specific point code format.
si		Specifies that the trigger will be matched only if the specified service indicator is received in the packet.
<i>indicator</i>		Service indicator. An integer ranging from 3 to 15.
block		Specifies that messages matching this trigger should be dropped. The block keyword is ignored if combination triggers are defined within cs7 mlr trigger configuration submenu.
continue		Specifies that messages matching this trigger should be routed as received. This behavior is the same as if no primary trigger had been matched. The continue keyword is ignored if combination triggers are defined within cs7 mlr trigger mode.
ruleset		Specifies the MLR ruleset table that should be used if this trigger is matched and not overruled by a secondary trigger ruleset. The ruleset keyword is ignored if combination triggers are defined within cs7 mlr trigger mode.
<i>ruleset-name</i>		Name of a defined cs7 mlr ruleset table. The name is specified as a character string with a maximum of 12 characters.
result		Routes messages based on the trigger alone. If a trigger result is configured, the TCAP/MAP/SMS layers are not parsed. If a message matches a trigger with a result trigger action, then the message is redirected as indicated in the trigger result. Note: Result groups with dest-sme-binding mode are not valid trigger results.
pc		Routes based on point code.
<i>pc</i>		Point code.
ssn		Routes based on PC and subsystem number.
<i>ssn</i>		Subsystem number.
asname		Routes based on AS name.
<i>as-name</i>		AS name.
gt		Routes based on global title.

<i>gt-addr-type</i>	Parameters that identify attributes of the global title address being used as a trigger. The parameters are variant-specific, and are identical to those parameters specified on the cs7 gtt selector command. If not specified, the default is the standard E.164 address type for the network variant being used. tt tt [gti gti] [np np nai nai] tt Identifies the translation type specified within the address. <i>tt</i> An integer value from 0 to 255. gti Identifies the global title indicator value for the specified address. This value is specified only when the CS7 variant is ITU or China. <i>gti</i> Integer value of 2 or 4. np Identifies the numbering plan of the specified address. Specified only when the <i>gti</i> value is 4. <i>np</i> Integer value from 0 to 15. nai Identifies the nature of address indicator. Specified only when the <i>gti</i> value is 4. <i>nai</i> Integer value from 0 to 127.
<i>gta</i>	Global title address.
group	Routes based on result group.
<i>group-name</i>	Result group name.

Defaults

None.

Command Modes

cs7 mlr table

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage GuidelinesThe **trigger mtp3** command enables cs7 mlr trigger mode.**Examples**

The following example shows how to specify a trigger to route messages based on the CdPA field of the incoming MSU. The trigger is specified for the table named SMS-TABLE.

```
cs7 mlr table SMS-TABLE
trigger cdpa gt 9991117770 ruleset ruleset1
```

The following example shows how to configure triggers to block messages based on a specified CdPA. The trigger is specified for the table named SMS-BLOCKING.

```
cs7 mlr table SMS-BLOCKING
```

```
trigger cdpa gt 9991117770 tt 10 block
```

Related Commands

Command	Description
cgpa	Creates a secondary trigger based on the CgPA, to be used in conjunction with a primary trigger based on the CdPA.
cs7 mlr table	Specifies the name of the multilayer SMS routing table and enables cs7 mlr table mode.
trigger cgpa (cs7 mlr table)	Specifies a primary routing trigger that is located in the SCCP calling party address field of the incoming MSU.

ttl

To specify the amount of elapsed time in seconds that a cached authentication triplet is stored, use the **ttl** cs7 authent-vlr submode command. To return to the default value of 604800 seconds (7 days), use the **no** form of this command.

ttl *time-to-live*

no ttl *time-to-live*

Syntax Description	<i>time-to-live</i>	Amount of elapsed time in seconds that a cached authentication triplet is stored. Valid values are decimal numbers in the range of 0 to 2147483647.

Defaults	604800 seconds (7 days)

Command Modes	cs7 authent-vlr submode

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples The following example shows how to specify 300000 seconds as the elapsed time that a cached authentication triplet is stored:

```
gsm-authent-vlr
 cache-size 100
 max-return 2
 ttl 300000
```

Related Commands	Command	Description
	cache-size	Specifies the total number of IMSIs for which authentication triplets are cached.
	gsm-authent-vlr	Enables authent-vlr submode, in which you can provision parameters specific to the GSM MAP Process_Obtain_Authentication_Sets_VLR service.
	max-return	Specifies the maximum number of authentication triplets that may be returned to a MAPUA client for a single request.

ttmap

TT mapping rules can be added to existing linksets. To add a rule, use the **ttmap** cs7 linkset submode command. To remove a TT map rule, use the **no** form of this command.

ttmap *existing-tt mapped-tt* [**in** | **out**]

no ttmap *existing-tt mapped-tt* [**in** | **out**]

Syntax Description

<i>existing-tt</i>	Existing translation type. Valid range is 0 to 255.
<i>mapped-tt</i>	Mapped translation type. Valid range is 0 to 255.
in	Performs TT mapping on inbound messages only.
out	Performs TT mapping on outbound messages only.

Defaults

None.

Command Modes

cs7 linkset submode

Command History

Release	Modification
12.2(18)IXE	This command was introduced.

Usage Guidelines

This command is available for all variants. The TT map feature is supported for UDT and XUDT only, not for UDTS or any other message.

Examples

The following example shows how to add a rule that maps all incoming messages that have a TT of 6 to now have a TT of 254:

```
cs7 linkset to_doc
  ttmap 6 254 in
```

Related Commands

Command	Description
show cs7 linkset ttmap	Displays TT mapping rules for the linkset.

ttnmap (cs7 as)

Global title translation type (TT) mapping rules can be added to application servers. To add a rule, use the **ttnmap** cs7 as submode command. To remove a TT mapping rule, use the **no** form of this command.

ttnmap *existing-tt mapped-tt* [**in** | **out**]

no ttnmap *existing-tt mapped-tt* [**in** | **out**]

Syntax Description

<i>existing-tt</i>	Received existing translation type. Valid range is 0 to 255.
<i>mapped-tt</i>	New mapped translation type. Valid range is 0 to 255.
in	Performs TT mapping on inbound messages only.
out	Performs TT mapping on outbound messages only.

Defaults

If neither **in** nor **out** is specified, then TT mapping is performed for both inbound and outbound messages. If the inbound AS cannot be determined from the received message, then TT mapping is not applied.

Command Modes

cs7 as submode

Command History

Release	Modification
12.2(18)IXE	This command was introduced.

Usage Guidelines

Up to 256 input TT mappings may be specified per AS, and up to 256 output TT mappings may be specified per AS.

Inbound TT mapping is applied after ACL and gateway screening, but before MLR and GTT processing. Outbound TT mapping is applied after MLR, GTT, ACL, and gateway screening.

The TT map feature is supported for UDT and XUDT only, not for UDTS or any other message.

Related Commands

Command	Description
show cs7 linkset ttnmap	Displays TT mapping rules for the linkset.

tt-range

To specify a translation type range entry in a CdPA SCCP selector table or CgPA SCCP selector table, use the **tt-range** command in gateway screening table configuration mode.

tt-range *tt-start* [*tt-end*] [**gti** *gti* [**np** *np* **nai** *nai*]] **result** {**action** *action-set-name* | **table** *table-name*}

no tt-range *tt-start* [*tt-end*] [**gti** *gti* [**np** *np* **nai** *nai*]]

Syntax Description		
<i>tt-start</i>		Starting pc in the range.
<i>tt-end</i>		Ending pc in the range.
gti		Identifies the global title indicator for the specified address. This value is specified only when the variant is ITU or China.
<i>gti</i>		Integer value of 2 or 4.
np		Identifies the numbering plan of the specified address. Configured only when <i>gti</i> is 4.
<i>np</i>		Integer in the range 0 to 15.
nai		Identifies the nature of the specified address. Configured only when <i>gti</i> is 4.
<i>nai</i>		Integer in the range 0 to 127.
result		Specifies the next step.
action		Screens by action set by default.
<i>action-set-name</i>		Action set name. Valid names may not exceed 12 alphanumeric characters.
table		Screens by table by default.
<i>table-name</i>		Table name. Valid names may not exceed 12 alphanumeric characters.

Defaults None.

Command Modes Gateway screening table configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines The **tt-range** command is valid for the following table types: CgPA SCCP selector, CdPA SCCP selector. Wildcards (*) are allowed.

The following example shows how to specify a tt-range entry for table SEL1:

```
cs7 instance 0 gws table SEL1 type cgpa-selector action allowed
  tt-range 5 10 gti 2 result table PGTA1
  default result table PGTA1
```

Related Commands

Command	Description
cs7 gws table	Configures a gateway screening table.

tx-queue-depth (cs7 asp)

To configure the maximum transmit queue depth for the association, use the **tx-queue-depth** cs7 asp submode command. To remove the configuration, use the **no** form of this command.

tx-queue-depth *depth*

no tx-queue-depth *depth*

Syntax Description	<i>depth</i>	Number of packets to be queued. The range is 100 to 20000 packets.

Defaults	The default transmit queue depth is the value specified under the local port instance.

Command Modes	cs7 asp submode

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples	The following example shows how to set the transmit queue depth for ASP1 to 2000 packets:

```
cs7 asp ASP1 2904 2905 m3ua
  tx-queue-depth 2000
```

Related Commands	Command	Description
	cs7 asp	Specifies an application server process (ASP) and enables cs7 asp submode.
	show cs7 asp	Displays ASP statistics.

tx-queue-depth (cs7 hs-mtp2 profile)

You can adjust the number of packets that can be queued for transmission. To configure the transmit queue depth, use the **tx-queue-depth** command in cs7 hs-mtp2 profile configuration mode. To return to the default queue depth, use the **no** form of this command.

tx-queue-depth *depth*

no tx-queue-depth *depth*

Syntax Description	<i>depth</i>	Number of packets to be queued. The range is 250 to 50000 packets. The default is 5000 packets.

Defaults	5000 packets

Command Modes	cs7 hs-mtp2 profile configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	The tx-queue-depth command controls the number of packets allowed on the transmit queue. The queue's function is to absorb traffic bursts. When you select the queue depth, you will have to compromise between transmit congestion thresholds, which can drop packets, or transmit delays due to queuing times. Applications that are sensitive to small delays should account for transmit delays due to queuing times. When links are congested, the queue depth controls the number of packets that can be queued before they are discarded. Discarding packets causes application retransmissions.

Examples	The following example shows how to define a profile named HSMTP2. The profile supports high-speed MTP2, specifies the tx-queue-depth command, and applies to all the links in the linkset named TO_NYC.

```
cs7 profile HSMTP2
  hs-mtp2
    tx-queue-depth 2000
  .
  .
  .
cs7 linkset TO_NYC
  profile HSMTP2
```

 tx-queue-depth (cs7 hs-mtp2 profile)**Related Commands**

Command	Description
hs-mtp2	Specifies high-speed MTP2 parameters in a CS7 profile.

tx-queue-depth (cs7 link)

You can adjust the number of packets that can be queued for transmission. To configure the transmit queue depth for a link, use the **tx-queue-depth** command in cs7 link configuration mode. To return to the default queue depth, use the **no** form of this command.

tx-queue-depth [*depth*]

no tx-queue-depth

Syntax Description	<i>depth</i>	Number of packets to be queued. The values for this parameter vary depending on the type of link. For an SCTP link, the range is 10 to 40000 packets with a default of 1000 packets. For an MTP2 link, the range is 25 to 5000 packets with a default of 500 packets. For a high-speed MTP2 link, the range is 250 to 50000 packets with a default of 5000 packets.

Defaults	1000 packets (SCTP link) 500 packets (MTP2 link) 5000 packets (high-speed MTP2 link)

Command Modes	cs7 link configuration

Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>12.2(18)IXA</td><td rowspan="3">This timer was added for high-speed MTP2 links.</td></tr><tr><td>12.4(11)SW</td></tr><tr><td>12.2(33)IRA</td></tr></table>	Release	Modification	12.2(18)IXA	This timer was added for high-speed MTP2 links.	12.4(11)SW	12.2(33)IRA
Release	Modification						
12.2(18)IXA	This timer was added for high-speed MTP2 links.						
12.4(11)SW							
12.2(33)IRA							

Usage Guidelines	The tx-queue-depth command controls the number of packets allowed on the transmit queue. The queue's function is to absorb traffic bursts. When you select the queue depth, you will have to compromise between transmit congestion thresholds, which can drop packets, or transmit delays due to queuing times.

Applications that are sensitive to small delays should account for transmit delays due to queuing times. When links are congested, the queue depth controls the number of packets that can be queued before they are discarded. Discarding packets causes application retransmissions.

Examples	The following example shows how to set the transmit queue depth to 2000 packets:

```
cs7 linkset TO_NYC 10.1.1
link 0 sctp 172.18.44.147 7000 7000
tx-queue-depth 2000
```

Related Commands

Command	Description
mtp2-timer	Specifies MTP2 timer values.
show cs7 m2pa	Displays M2PA statistics.
show cs7 mtp2	Displays MTP2 statistics.

tx-queue-depth (cs7 m2pa profile)

You can adjust the number of packets that can be queued for transmission. To configure the transmit queue depth, use the **tx-queue-depth** command in cs7 m2pa profile configuration mode. To return to the default queue depth, use the **no** form of this command.

tx-queue-depth *queue-depth*

no tx-queue-depth *queue-depth*

Syntax Description	<i>queue-depth</i>	Number of packets to be queued. The values for this parameter vary depending on the type of link. For an SCTP link, the range is 100 to 20000 packets with a default of 1000 packets. For an MTP2 link, the range is 25 to 5000 packets with a default of 500 packets.

Defaults	1000 packets (SCTP link) 500 packets (MTP2 link)

Command Modes	cs7 m2pa profile configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	The tx-queue-depth command controls the number of packets allowed on the transmit queue. The queue's function is to absorb traffic bursts. When you select the queue depth, you will have to compromise between transmit congestion thresholds, which can drop packets, or transmit delays due to queuing times.

Applications that are sensitive to small delays should account for transmit delays due to queuing times. When links are congested, the queue depth controls the number of packets that can be queued before they are discarded. Discarding packets causes application retransmissions.

Examples	The following example shows how to define a profile named m2parfc. The profile supports M2PA RFC, specifies the tx-queue-depth command, and applies to all the links in the linkset named to_nyc.

```
cs7 profile m2parfc
  m2pa
    tx-queue-depth 2000
.
.
.
cs7 linkset to_nyc
  profile m2parfc
```

 tx-queue-depth (cs7 m2pa profile)**Related Commands**

Command	Description
m2pa	Specifies M2PA parameters in a CS7 profile.

tx-queue-depth (cs7 m3ua)

To configure the maximum transmit queue depth for new SCTP associations established with this local port, use the **tx-queue-depth** cs7 m3ua submode command. To return to the default queue depth, use the **no** form of this command.

tx-queue-depth *queue-depth*

no tx-queue-depth *queue-depth*

Syntax Description	queue-depth		Number of packets to be queued. The range is 100 to 20000 packets. The default is 1000 packets.
Defaults	1000 packets		
Command Modes	cs7 m3ua submode		
Command History	Release	Modification	
	12.2(18)IXA	This command was introduced.	
	12.4(11)SW		
	12.2(33)IRA		
Examples	The following example shows how to set the transmit queue depth to 2000 packets: cs7 m3ua 2905 tx-queue-depth 2000		
Related Commands	Command	Description	
	cs7 m3ua	Specifies the local port number for M3UA and enters cs7 m3ua submode.	

tx-queue-depth (cs7 mated-sg)

To configure the maximum transmit queue depth for the association, use the **tx-queue-depth** cs7 mated-sg submode command. To remove the configuration, use the **no** form of this command.

tx-queue-depth *queue-depth*

no tx-queue-depth *queue-depth*

Syntax Description	<i>queue-depth</i> Number of packets to be queued. The range is 100 to 65535 packets. The default is 20000 packets.	
Defaults	20000 packets	
Command Modes	cs7 mated-sg submode	
Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	
Examples	The following example shows how to set the transmit queue depth to 2000 packets: cs7 mated-sg BLUE 5000 tx-queue-depth 2000	
Related Commands	Command	Description
	cs7 mated-sg	Establishes an association to the mated SG and enters cs7 mated-sg submode.

tx-queue-depth (cs7 mtp2 profile)

To configure the MTP2 maximum transmit queue depth in a CS7 MTP2 profile, use the **tx-queue-depth** command in cs7 mtp2 profile configuration mode. To remove the configuration, use the **no** form of this command.

tx-queue-depth *queue-depth*

no tx-queue-depth *queue-depth*

Syntax Description	<i>queue-depth</i>	Number of packets to be queued. The range is 25 to 5000 packets.

Defaults	The default queue depth is the value specified under the local port instance.

Command Modes	cs7 mtp2 profile configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples	The following example shows how to define a profile named timers. The profile supports MTP2, configures the transmit queue depth to 3000 packets, and applies to all the links in the linkset named itpa.

```
cs7 profile timers
 mtp2
  tx-queue-depth 3000

!
cs7 linkset itpa
 profile timers
```

Related Commands	Command	Description
	mtp2	Configures CS7 link profile parameters for MTP2.

tx-queue-depth (cs7 sgmp)

To configure the maximum transmit queue depth for new SCTP associations established with this local port, use the **tx-queue-depth** cs7 sgmp submode command. To return to the default queue depth, use the **no** form of this command.

tx-queue-depth *queue-depth*

no tx-queue-depth *queue-depth*

Syntax Description	<i>queue-depth</i> Number of packets to be queued. The range is 100 to 20000 packets. The default is 20000 packets.	
Defaults	20000 packets	
Command Modes	cs7 sgmp submode	
Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	
Examples	The following example shows how to set the transmit queue depth to 1000 packets: cs7 sgmp 5000 tx-queue-depth 1000	
Related Commands	Command	Description
	cs7 sgmp	Establishes an association to the mated-signaling gateway.

tx-queue-depth (cs7 sua)

To configure the maximum transmit queue depth for new SCTP associations established with this local port, use the **tx-queue-depth** cs7 sua submode command. To return to the default queue depth, use the **no** form of this command.

tx-queue-depth *queue-depth*

no tx-queue-depth *queue-depth*

Syntax Description	<i>queue-depth</i> Number of packets to be queued. The range is 100 to 20000 packets. The default is 1000 packets.	
Defaults	1000 packets	
Command Modes	cs7 sua submode	
Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	
Examples	The following example shows how to set the transmit queue depth to 2000 packets: cs7 sua 15000 tx-queue-depth 2000	
Related Commands	Command	Description
	cs7 sua	Specifies the local port number for SUA and enters cs7 sua submode.

tx-queue-depth (group peer)

You can adjust the number of packets that can be queued for transmission. To configure the transmit queue depth, use the **tx-queue-depth** group peer submode command. To return to the default queue depth, use the **no** form of this command.

tx-queue-depth *queue-depth*

no tx-queue-depth *queue-depth*

Syntax Description	<i>queue-depth</i>	Number of packets to be queued. The values for this argument vary depending on the type of link. For an SCTP link, the range is 100 to 20000 packets with a default of 1000 packets. For an MTP2 link, the range is 25 to 5000 packets with a default of 500 packets.

Defaults	1000 packets (SCTP link) 500 packets (MTP2 link)

Command Modes	Group peer submode

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines	The tx-queue-depth command controls the number of packets allowed on the transmit queue. The queue's function is to absorb traffic bursts. When you select the queue depth, you will have to compromise between transmit congestion thresholds, which can drop packets, or transmit delays due to queuing times.

Applications that are sensitive to small delays should account for transmit delays due to queuing times. When links are congested, the queue depth controls the number of packets that can be queued before they are discarded. Discarding packets causes application retransmissions.

Examples	The following example shows how to set the transmit queue depth to 2000 packets:

```
cs7 group ITP1 3333
 local-ip 1.1.1.1
 peer 4444
 remote-ip 1.1.1.2
 tx-queue-depth 2000
```

Related Commands

Command	Description
peer (group)	Enables ITP to initiate the SCTP association with its peers and enables group peer submode.

ucp (cs7 sms group)

To specify that messages will be routed on a UCP session, use the **ucp** command in cs7 sms group configuration mode. To remove the configuration, use the **no** form of this command.

ucp *session-name* [**weight** *weight*]

no ucp *session-name* [**weight** *weight*]

Syntax Description

<i>session-name</i>	UCP session name.
weight	Specifies the weight applied to the weighted round robin (WRR) algorithm.
<i>weight</i>	Weight value, in the range 0 to 10.

Defaults

None.

Command Modes

cs7 sms group configuration

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Examples

The following example shows how to configure a result group named OFFISLAND and specify that messages will be routed in SMPP sessions:

```
CS7 sms group OFFISLAND smsc protocol ucp
 ucp OFFISLAND1 weight 3
 ucp OFFISLAND2 weight 4
```

Related Commands

Command	Description
cs7 sms group	Configures an SMS result group.

udp-checksum

To turn on the optional calculation of a UDP checksum sent in the PMP stream, use the **udp-checksum** *cs7* *dc*s configuration submode command. To stop the action, use the **no** form of this command.

udp-checksum *udp-checksum*

no udp-checksum *udp-checksum*

Syntax Description

<i>udp-checksum</i>	A 16-bit field used for error checking of the header and data of the UDP transport layer protocol.

Defaults

This command is disabled.

Command Modes

cs7 dcs configuration submode

Command History

Release	Modification
12.4(15)SW3	This command was introduced.
12.2(33)IRC	

Examples

The following example shows how to turn on the UDP checksum for the DCS node named alpha:

```
cs7 dcs alpha
  remote-ip 209.165.201.29 209.165.201.28 3033
  local-ip 1209.165.20127 3033
  ping-interval 5
  timeout-count 3
  udp-checksum
```

Related Commands!

Command	Description
cs7 pmp	Turns probeless monitoring on for all linksets and ASes.
cs7 pmp hold-queue	Sets the integer range of PMP hold queue thresholds.
cs7 dcs-group	Identifies a name to be associated with a DCS group.
cs 7 dcs	Identifies a name to be associated with a DCS node.
show cs7 pmp	Displays errors and information about the PMP.
show cs7 dcs-group	Displays information about the DCS group.
show cs7 dcs	Displays information about the DCS node.

unordered-priority (cs7 m3ua)

To configure the priority of unordered packets, use the **unordered-priority** cs7 m3ua command. To remove the configuration, use the **no** form of this command.

unordered-priority {equal | high}

no unordered-priority

Syntax Description	equal	Unordered packets delivered in the order received.
	high	Unordered packets delivered before any sequenced data.
Defaults	Unordered packets are delivered in the order received.	
Command Modes	cs7 m3ua	
Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	
Examples	The following example shows how to specify that unordered packets are delivered before any sequenced data: cs7 m3ua 2905 unordered-priority high	
Related Commands	Command	Description
	cs7 m3ua	Specifies the local port number for M3UA and enters cs7 m3ua submode.

unordered-priority (cs7 sgmp)

To configure the priority of unordered packets, use the **unordered-priority** cs7 sgmp command. To remove the configuration, use the **no** form of this command.

unordered-priority {equal | high}

no unordered-priority

Syntax Description

equal	Unordered packets delivered in the order received.
high	Unordered packets delivered before any sequenced data.

Defaults

Unordered packets are delivered in the order received.

Command Modes

cs7 sgmp

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Examples

The following example shows how to specify that unordered packets are delivered in the order received:

```
cs7 sgmp 5000
 unordered-priority equal
```

Related Commands

Command	Description
cs7 sgmp	Establishes an association to the mated-signaling gateway and enters cs7 sgmp submode.

unordered-priority (cs7 sua)

To configure the priority of unordered packets, use the **unordered-priority** cs7 sua command. To remove the configuration, use the **no** form of this command.

unordered-priority {equal | high}

no unordered-priority

Syntax Description	equal	Unordered packets delivered in the order received.
	high	Unordered packets delivered before any sequenced data.
Defaults	Unordered packets are delivered in the order received.	
Command Modes	cs7 sua	
Command History	Release	Modification
	12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.
Examples	The following example shows how to specify that unordered packets are delivered before any sequenced data: <pre>cs7 sua 15000 unordered-priority high</pre>	
Related Commands	Command	Description
	cs7 sua	Specifies the local port number for SUA and enters cs7 sua submode.

unrouteable-accounting (cs7 as)

To enable unroutable accounting for xUA ASes, use the **unrouteable-accounting** cs7 as submode command. To disable unroutable accounting, use the **no** form of this command.

unrouteable-accounting

no unrouteable-accounting

Syntax Description	This command has no arguments or keywords.

Defaults	None.

Command Modes	cs7 as submode

Command History

Usage Guidelines	If the command is issued for an M3UA AS, unroutable accounting counts the payload data messages received from M3UA AS. These payload data messages need routing to an inaccessible destination and are classified by an OPC+DPC+SI combination.

If the command is issued for an SUA AS, unroutable accounting counts the CLDT messages received from the SUA AS. These CDLT messages need routing to an inaccessible destination, or the GTT is translated to an inaccessible point code.

Related Commands

Command	Description
clear cs7 accounting	Clears an unroutable database.
cs7 accounting	Enables unroutable accounting on all linksets.
show cs7 accounting	Displays accounting information about unroutable packets.

unrouteable-accounting (cs7 linkset)

To enable unroutable accounting on a linkset, use the **unrouteable-accounting** command in cs7 linkset configuration mode. To remove the configuration, use the **no** form of this command.

unrouteable-accounting

no unrouteable-accounting

Syntax Description This command has no arguments or keywords.

Defaults None.

Command Modes cs7 linkset configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Examples The following example shows how to enable unroutable accounting in linkset1:

```
cs7 linkset linkset1 2.2.2
unrouteable-accounting
```

Related Commands	Command	Description
	clear cs7 accounting	Clears an unroutable database.
	cs7 accounting	Enables unroutable accounting on all linksets.
	show cs7 accounting	Displays accounting information about unroutable packets.

update (cs7 gtt address conversion)

To add, remove, or change a GTT address-conversion entry, use the **update** cs7 gtt address conversion submode command. To delete the entry, use the **no** form of this command.

update [**in-address** *in-address*] [**nai** *nai*] [**np** *np*] [**out-address** *out-address*] [**es** *es-val*] [**remove** *ndigits*]

no update [**in-address** *in-address*] [**nai** *nai*] [**np** *np*] [**out-address** *out-address*] [**es** *es-val*] [**remove** *ndigits*]

Syntax Description		
remove		Specifies the number of digits to remove from the input address before inserting the output address prefix. If not specified, then only the digits specified with the in-address keyword are removed.
<i>ndigits</i>		The number of digits to remove, specified as an integer in the range 0 to 15.
in-address		Specifies the input address prefix that must match for the following modifications to be made. A new default input address may be specified. The default input address is used if no other input addresses within the address conversion table match the input packet. Only one update command within an address table may specify a default input address.
<i>in-address</i>		SCCP address. Valid numbers are 1 to 15 hexadecimal digits in length, or a default address configured as an asterisk (*).
nai		Specifies a new nature of address indicator.
<i>nai</i>		NAI value. Range is 0 to 127.
np		Specifies a new numbering plan.
<i>np</i>		NP value. Range is 0 to 15.
out-address		Specifies the output address.
<i>out-address</i>		SCCP address. Valid numbers are 1 to 15 hexadecimal digits in length.
es		Specifies a specific encoding scheme for the address conversion result.
<i>es-val</i>		Encoding scheme value. Valid range is 0 to 2: 0 = unknown encoding scheme 1 = bcd odd encoding scheme 2 = bcd even encoding scheme

Defaults None.

Command Modes cs7 gtt address conversion submode

Usage Guidelines If the specified number of digits to remove is greater than the number of digits in the input address, then all digits are removed before the new prefix specified by the output address is inserted. If no output address is specified, then the address conversion fails and the MSU is not routed.

Command History

Release	Modification
12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.
12.2(18)IXE	The remove keyword and <i>ndigits</i> argument were added.

Examples

```
cs7 gtt address-conversion CONVERT
```

```
update in-address 23480500 out-address 919821900201 remove 12
```

In this example, an input address of 234805001234567 is first converted

- by removing 12 digits from the address prefix: 234805001234567 -> 567
- then prepending the out-address string: 567 -> 919821900201567

An input address of 2348050034 is converted by

- removing 12 digits from the address prefix: 2348050034 -> NULL
- then prepending the out-address string: NULL -> 919821900201

Related Commands

Command	Description
cs7 gtt address-conversion	Configures a global title address conversion table.

update (cs7 sccp gti conversion)

To add, remove, or change an SCCP GTI conversion table entry, use the **update** cs7 sccp gti conversion submode command. To delete the entry, use the **no** form of this command.

update [**gti-in** *gti-in*] [**tt-in** *tt-in*] [**ssn-in** *ssn-in*] [**es-in** *es-in*] [**np-in** *np-in*] [**nai-in** *nai-in*] [**gti-out** *gti-out*] [**tt-out** *tt-out*] [**ssn-out** *ssn-out*] [**es-out** *es-out*] [**np-out** *np-out*] [**nai-out** *nai-out*] [**addr-conv** *addr-conv*]

no update [**gti-in** *gti-in*] [**tt-in** *tt-in*] [**ssn-in** *ssn-in*] [**es-in** *es-in*] [**np-in** *np-in*] [**nai-in** *nai-in*] [**gti-out** *gti-out*] [**tt-out** *tt-out*] [**ssn-out** *ssn-out*] [**es-out** *es-out*] [**np-out** *np-out*] [**nai-out** *nai-out*] [**addr-conv** *addr-conv*]

Syntax Description

gti-in	Input GTI.
<i>gti-in</i>	Valid values are 2, 4
tt-in	Input TT.
<i>tt-in</i>	Valid range is 0 to 255. All TTs match if not specified.
ssn-in	Input SSN.
<i>ssn-in</i>	Valid range is 0 to 255. All SSNs match if not specified.
es-in	Input ES.
<i>es-in</i>	Allowed if <i>gti-in</i> is 4. Not allowed if <i>gti-in</i> is 2.
np-in	Input NP.
<i>np-in</i>	Allowed if <i>gti-in</i> is 4. Not allowed if <i>gti-in</i> is 2.
nai-in	Input NAI.
<i>nai-in</i>	Allowed if <i>gti-in</i> is 4. Not allowed if <i>gti-in</i> is 2.
gti-out	Valid values are 2, 4.
<i>gti-out</i>	Valid values are 2, 4.
tt-out	Output TT.
<i>tt-out</i>	Valid range is 0 to 255. TT unchanged if not specified.
ssn-out	Output SSN.
<i>ssn-out</i>	Valid range is 0 to 255. SSN unchanged if not specified.
es-out	Output ES. Required if <i>gti-in</i> is 2 and <i>gti-out</i> is 4. Optional if <i>gti-in</i> and <i>gti-out</i> are both 4. Not allowed if <i>gti-out</i> is 2.
<i>es-out</i>	Valid range is 0 to 15. ES is unchanged if not specified. ES is not used if <i>gti-out</i> is 2.
np-out	Output NP. Required if <i>gti-in</i> is 2 and <i>gti-out</i> is 4. Optional if <i>gti-in</i> and <i>gti-out</i> are both 4. Not allowed if <i>gti-out</i> is 2.
<i>np-out</i>	Valid range is 0 to 15. NP is unchanged if not specified. NP is not used if <i>gti-out</i> is 2.

■ **update (cs7 sccp gti conversion)**

nai-out	Output NAI. Required if <i>gti-in</i> is 2 and <i>gti-out</i> is 4. Optional if <i>gti-in</i> and <i>gti-out</i> are both 4. Not allowed if <i>gti-out</i> is 2.
<i>nai-out</i>	Valid range is 0 to 127. NAI is unchanged if not specified. NAI is not used if <i>gti-out</i> is 2.
addr-conv	If specified, this GTI address conversion takes precedence over any GTT address conversion table specified by an instance conversion rule.
<i>addr-conv</i>	Address conversion table name.

Defaults

None.

Command Modes

cs7 sccp gti conversion submode

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.4(11)SW	
12.2(33)IRA	

Usage Guidelines

GTI conversion can be used to update the GTI, TT, SSN, encoding scheme, numbering plan, and nature of address indicator in an SCCP address. You specify sets of input parameters and output parameters. For ANSI, GTI 2 is supported. For ITU, GTI 2 and 4 are supported.

Examples

The following example shows how to convert all MSUs with GTI 2 to GTI 4 and set the encoding scheme to 2, the numbering plan to 1, and the nature of address indicator to 3, but not change the TT and SSN:

```
cs7 sccp gti-conversion gti-conv1
update gti-in 2 gti-out 4 es-out 2 np-out 1 nai-out 3
```

Related Commands

Command	Description
cs7 sccp gti-conversion	Configures a GTI conversion table.
show cs7 sccp gti-conversion	Displays the SCCP GTI conversion table.

update route (route-table)

To update a route, use the **update route** route-table submode command.

update route *point-code* [*mask* | *length*] **linkset** *ls-name* [**priority** *priority-value*] [**qos-class** { *class* | **default** }] [**load_share**]

Syntax Description

<i>point-code</i>	Signaling point code of the destination.
<i>mask</i>	Specifies the significant bits of the point code.
<i>length</i>	Alternate way of specifying the mask. For ANSI, this alternate specification of the default is /24. For ITU, the alternate specification of the default is /14.
linkset	Specifies the linkset.
<i>ls-name</i>	Name of the previously created linkset.
priority	Configures route priority.
<i>priority-value</i>	Priority of the route to the destination. Valid range is 1 to 9 (the smaller the number, the higher the priority). The default is 5. Two routes to the same destination using two different linksets but equal priority form a combined linkset.
qos-class	Specifies the QoS class assigned to the destination.
<i>class</i>	QoS class. Valid range is 1 to 7.
load_share	Enables loadsharing among linksets in combined linkset as per Q.704.

Defaults

The default priority value is 5.

Command Modes

Route-table submode

Command History

Release	Modification
12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.
12.4(15)SW6 12.2(33)IRF	The load_share keyword was introduced.
12.4(15)SW7 12.2(33)IRG	The number of maximum routes with the same priority increased from 2 to 4.

Usage Guidelines

For ITU networks, the mask must be 7.255.7 if the default 3-8-3 bit point code format is used.

For ANSI networks, the mask must be 255.255.255 if the default 8-8-8 bit point code format is used.

You must specify either *mask* or *length*.

A lower number for *priority-value* gives the route a higher priority.

Setting a priority value of 9 is not recommended. This value should be reserved for dynamic routes created when summary routing is enabled. See the “[Summary Routing and ANSI Cluster Routing](#)” chapter for an explanation of summary routing.

A QoS class assignment is based on a destination point code. All routes to a specific DPC will have the same QoS class. When creating multiple routes to the same destination point code, the same QoS class must be specified for the DPC on each **update route** command. If the QoS class value is changed on a route for a DPC, the QoS class for all the routes to that DPC is changed. Omitting a QoS class value for a route to a DPC removes the QoS class from all existing routes to that DPC.

To preserve the priority of an existing route when adding or modifying the QoS class, the priority specified on the existing route must be specified on the modified route. If the priority is omitted, the priority of the modified route changes to the default priority of 5.

The **load_share** keyword enables Q.704 linkset load sharing. The scheme equally divides traffic between the linksets. It then divides the allocated linkset traffic among the links that comprise the linkset.

For example, traffic is first equally distributed over the linkset A and linkset B (50 percent each). It is then divided among the links that make up linkset A or the links that make up linkset B.

ITP performs verification of route availability when a new route for a DPC is added. In the case of a link restart, the status of the route will go to accessible by default in case no TFP is received from any of the adjacent nodes.

Examples

The following two examples show acceptable ways to create a route to destination 1.50.2 using linkset nyc and the default priority:

```
update route 1.50.2 255.255.255 linkset nyc
```

```
update route 1.50.2/24 linkset nyc
```

The following example shows how to create a route to destination 1.50.3 using linkset washington with priority 3:

```
update route 1.50.3 255.255.255 linkset washington priority 3
```

The following example shows how to create a combined linkset:

```
update route 1.50.3 255.255.255 linkset philly priority 3
```

The following two examples show that the lower priority value sets a higher priority for the route. In the examples, LSA is the primary route to 1.1.1 and LSC is the alternate route to 1.1.1.

```
update-route 1.1.1/14 linkset LSA priority 1
```

```
update route 1.1.1/14 linkset LSC priority 9
```

The following example shows how to create a route to destination 1.50.3 using linkset washington with QoS class 2:

```
update-route 1.50.3 255.255.255 linkset washington priority 3 qos-class 2
```

The following examples show how to create routes to destination 1.50.3 with QoS class 3. LSA is the primary route and LSC is the alternate route to 1.50.3.

```
update route 1.50.3 255.255.255 linkset LSA priority 1 qos-class 3
```

```
update route 1.50.3 255.255.255 linkset LSC priority 9 qos-class 3
```



Note

In this example, note that if the **qos-class** keyword is omitted from alternate route LSC, QoS functionality is disabled for destination 1.50.3. If another QoS class is specified on alternate route LSC instead of QoS class 3, that class is assigned to both primary route LSA and alternate route LSC.

In the following example, the second statement modifies an existing route to destination 1.50.3 using linkset washington and priority 3 with QoS class 2:

```
update-route 1.50.3 255.255.255 linkset washington priority 3
update route 1.50.3 255.255.255 linkset washington priority 3 qos-class 2
```

**Note**

In this example, note that if the **priority** keyword is omitted when adding the **qos-class** keyword, the priority of the route changes to the default priority of 5.

In the following example, under the destination 1.1.1, the linksets m2pa_194_00 and m2pa_194_01 have the load share feature enabled:

```
update route 1.1.1/14 linkset m2pa_194_00 priority 1 qos-class 2 load_share
update route 1.1.1/14 linkset m2pa_194_01 priority 1 qos-class 2 load_share
```

Related Commands

Command	Description
cs7 route-table	Specifies a route table for an instance.
show cs7 route	Displays the ITP routing table.

ussd-string (cs7 mlr ruleset rule)

To specify the USSD string used in filtering and routing mobile initiated GSM-MAP messages, use the **ussd-string** command in the cs7 mlr ruleset rule submode. To remove the string, use the **no** form of this command.

ussd-string *string*

no ussd-string

Syntax Description	<i>string</i>	Character string with a maximum length of 20 and not containing * or #.

Defaults	There is no default string.

Command Modes	cs7 mlr ruleset rule submode

Command History	Release	Modification
	12.4(15)SW7	This command was introduced.
	12.2(33)IRG	

Usage Guidelines	Configure the USSD string to be used in filtering and routing mobile-initiated GSM-MAP messages.

Examples	The following example shows how to filter mobile-initiated GSM-MAP messages containing USSD string 123 and route them to DPC 1234:

```
cs7 instance 0 mlr ruleset abc
rule 1 gsm-map mobileUSSD
  ussd-string 123
  result pc 1234
```

Related Commands	Command	Description
	cs7 mlr options	Specifies MLR global options.
	rule (cs7 mlr ruleset)	Specifies the rules for a routing trigger within a multilayer ruleset table and enables cs7 mlr ruleset rule configuration mode.
	show cs7 mlr options	Displays the MLR global options.

variant

To specify which of the SS7 variations the CS7 profile is running, use the **variant** command in cs7 profile configuration mode. To remove the specification from the configuration, use the **no** form of this command.

variant {ansi | china | itu | ttc}

no variant {ansi | china | itu | ttc}

Syntax Description

ansi	American National Standards Institute (ANSI) SS7 protocol variant.
china	CHINA SS7 protocol variant.
itu	International Telecommunications Union (ITU) SS7 protocol variant.
ttc	Telecommunications Technology Committee (Japan) standard interface.

Defaults

None.

Command Modes

cs7 profile configuration

Command History

Release	Modification
12.2(18)IXA 12.4(11)SW 12.2(33)IRA	This command was introduced.

Examples

The following example shows how to specify that the ANSI variant of SS7 [is being used]:

```
cs7 profile SAAL  
  variant ansi
```

Related Commands

Command	Description
cs7 profile	Defines a profile that you can apply to all the links in a linkset.
hsl	Configures CS7 link profile parameters for HSL.
mtp2	Configures CS7 link profile parameters for MTP2.

variant jt1

To enable the Japanese variations of the standard framing formats for T1 controller settings, use the **variant jt1** command in controller configuration mode. To remove the specification from the configuration, use the **no** form of this command.

variant jt1

no variant jt1

Syntax Description This command has no arguments or keywords.

Defaults None.

Command Modes Controller configuration

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.
	12.4(11)SW	
	12.2(33)IRA	

Usage Guidelines This command enables the JT1 interface. The JT1 interface is a 1544-kbit/s Japanese line type specified by the Japanese standards organization, the Telecommunications Technology Committee (TTC). The JT1 interface is similar to T1. The following table show the differences between T1 and JT1.

Function	T1	JT1
Pulse Template	45% allowable undershoot	75% allowable undershoot
Framing Mode	D4 and ESF	ESF only
I/O Impedance	100 ohms	110 ohms
ESF Yellow Alarm	Repeating pattern of 8 ones and 8 zeros	Repeating pattern of 16 ones
ESF CRC	CRC bit sequence is the remainder after multiplying by x6 and then dividing by the generator polynomial, F-bits replaced by 1s.	CRC bit sequence is the remainder divided by the generator polynomial.

Examples The following example shows how to enable the Japanese variations of the standard framing formats for T1 controller settings:

```
controller t1
 variant jt1
```

Related Commands

Command	Description
controller	Specifies the controller and enters controller configuration mode.

wait-timeout

To configure the amount of time an ITP group member waits after bootup to establish communication with its peer, before it assumes it is operating independently, use the **wait-timeout** command in group configuration mode. To reset the peer wait timeout period to its default setting, use the **no** form of this command.

wait-timeout *seconds*

no wait-timeout

Syntax Description	<i>seconds</i> The number of seconds an ITP group member waits to establish communication with a peer. Valid values range from 45 to 300 seconds.							
Defaults	60 seconds							
Command Modes	Group configuration							
Command History	<table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>12.2(18)IXA</td><td rowspan="3">This command was introduced.</td></tr><tr><td>12.4(11)SW</td></tr><tr><td>12.2(33)IRA</td></tr></tbody></table>		Release	Modification	12.2(18)IXA	This command was introduced.	12.4(11)SW	12.2(33)IRA
Release	Modification							
12.2(18)IXA	This command was introduced.							
12.4(11)SW								
12.2(33)IRA								
Usage Guidelines	For most situations the default value of 60 seconds is an adequate amount of time for an ITP group member to establish communication with its peer, assuming the peer is present and initialized, and an operational communication link exists between ITPs. This command only affects the amount of time an ITP group member waits to establish communication with its peer after bootup, before it assumes it is operating independently. The ITP always attempts to establish communication with its peer on a periodic basis when communication has not been established.							
Examples	The following example shows how to set the wait-timeout period to 120 seconds: <pre>cs7 group ITP1 3333 wait-timeout 120</pre>							
Related Commands	<table><thead><tr><th>Command</th><th>Description</th></tr></thead><tbody><tr><td>cs7 group</td><td>Specifies an ITP group.</td></tr></tbody></table>		Command	Description	cs7 group	Specifies an ITP group.		
Command	Description							
cs7 group	Specifies an ITP group.							



ITP Debug Commands

- `debug cs7 gws`
- `debug cs7 gws rate-limit`
- `debug cs7 gws rmt-packet-drop`
- `debug cs7 m2pa`
- `debug cs7 m3ua`
- `debug cs7 mlr`
- `debug cs7 mtp2`
- `debug cs7 mtp3`
- `debug cs7 mtp3 paklog`
- `debug cs7 nso`
- `debug cs7 nso chkpt`
- `debug cs7 offload mtp3`
- `debug cs7 sccp`
- `debug cs7`
- `debug cs7 snmp`
- `debug cs7 sua`
- `debug cs7 tcap`



Note

Enabling debugging during periods of heavy traffic can cause link failure.

Short Message Peer-to-Peer (SMPP) protocol is not supported. Some DSMR functionality is also not supported. It is recommended that commands pertaining to these features are not configured.

debug cs7 gws

To display debug information for the gateway screening feature, use the **debug cs7 gws** command in privileged EXEC mode. To disable the display, use the **no** form of this command.

debug cs7 gws {all | api | error | info | packet} [verbose]

no debug cs7 gws {all | api | error | info | packet}

Syntax Description

all	Enable all Enhanced Gateway Screening debugs.
api	GWS API tracing.
error	GWS error events.
info	GWS informational events.
packet	GWS packet tracing.
verbose	Display detailed packet tracing.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(25)SW4	This command was introduced.

Usage Guidelines

We recommend that use of this and all debug commands be performed with the advice of the Cisco Technical Assistance Center (TAC).

debug cs7 gws rate-limit

To display debug information for the API call and some internal events when processing MSUs at GWS level, use the **debug cs7 gws rate-limit** command in privileged EXEC mode. To disable the display, use the **no** form of this command.

```
debug cs7 gws rate-limit {ingress | egress | both}
```

```
no debug cs7 gws rate-limit
```

Syntax Description

ingress	Specifies inbound traffic.
egress	Specifies outbound traffic.
both	Specifies both inbound and outbound traffic.

Command Default

None.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)IRG	This command was introduced.
12.4(15)SW7	

Usage Guidelines

We recommend that use of this and all debug commands be performed with the advice of the Cisco Technical Assistance Center (TAC).

debug cs7 gws rmt-packet-drop

To display the number of MSUs dropped in a timer window, use the **debug cs7 gws rmt-packet-drop** command in privileged EXEC mode. To disable the display, use the **no** form of this command.

debug cs7 gws rmt-packet-drop {ingress | egress | both}

no debug cs7 gws rmt-packet-drop

Syntax Description

ingress	Specifies inbound traffic.
egress	Specifies outbound traffic.
both	Specifies both inbound and outbound traffic.

Command Default

None.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)IRG	This command was introduced.
12.4(15)SW7	

Usage Guidelines

We recommend that use of this and all debug commands be performed with the advice of the Cisco Technical Assistance Center (TAC).

debug cs7 m2pa

To display debug messages for M2PA, use the **debug cs7 m2pa** EXEC command.

```
debug cs7 m2pa { cong | error | iac | l3api | lsc | packet | poc | retrieval | rxc | peer | sctp | timers
               | txc } linkset slc
```



Note

Enabling debug during high traffic can cause the link to fail.

Syntax Description

cong	Debugs Congestion Control events.
error	Debugs Error events.
iac	Debug Initial Alignment Control events.
l3api	Debugs M2PA Layer 3 API events.
lsc	Debug Link State Control events.
packet	Debugs M2PA Packet tracing.
poc	Debug Processor Outage Control events.
retrieval	Debug Retrieval events.
rxc	Debug Reception Control events.
peer	Debugs M2PA Peer events.
sctp	Debugs M2PA SCTP events.
timers	Debug Timer events.
txc	Debug Transmission Control events.
<i>linkset</i>	Linkset
<i>slc</i>	Signalling link selector value

Defaults

No default behavior or values.

Command History

Release	Modification
12.2(18)IXA	This command was introduced.
12.2(25)SW3	The iac , lsc , poc , retrieval , rxc , timers and txc keywords were added.

debug cs7 m3ua

To display debug messages for M3UA, use the **debug cs7 m3ua** EXEC command.

```
debug cs7 m3ua [all | congestion | error | l3api | mgmt {api | state {as-name ASname | asp-name
ASPname} | pointcode {dpc pointcode}} | packet {short} {asp-name ASPname} | sctp
{asp-name ASPname} | timer {as-name ASname}
```



Note

Enabling debug during high traffic can cause the link to fail.

Syntax Description

all	Enables all debugs.
api	Debugs API events.
as-name	Specify an AS.
<i>ASname</i>	AS name.
asp-name	Specify an ASP
<i>ASPname</i>	AS P name.
congestion	Debugs Congestion Control events
dpc	Specify a point code.
error	Debugs Error events.
l3api	Debugs M3UA Layer 3 API events.
mgmt	Debugs Management events.
packet	Packet tracing
point-code	Point code
<i>point-code</i>	Point code
sctp	SCTP API events.
state	State machine events.
timer	AS timer events.
short	Truncate displayed payload at 32 bytes.

Defaults

No default behavior or values.

Command History

Release	Modification
12.2(18)IXA	This command was introduced.

debug cs7 mlr

To display debug messages for Multi-layer routing, use the **debug cs7 mlr** command in privileged EXEC mode.

debug cs7 mlr table [**all** | **error** | **info** | **packet**] [**verbose** [*paklen*]]

Syntax Description

all	Enables all debugs.
error	Debugs error events.
info	Display informational events.
packet	Displays packet events.
verbose	Display detailed information.
<i>paklen</i>	Number of bytes of TCAP message to display. The default is 0.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)IXA	This command was introduced.

Examples

The following is sample output from the **debug cs7 mlr** command:

```
Router# debug cs7 mlr
*Mar 1 02:08:11.600: CS7 MLR PACKET: Packet 815448A8 received for SCCP MLR processing
*Mar 1 02:08:11.600: CS7 MLR INFO: Primary CdPA GT trigger match on 9991117770
*Mar 1 02:08:11.600: CS7 MLR INFO: mlr_parse_itu_tcap_msg: TC_DLG_BEGIN Tag Decoded
*Mar 1 02:08:11.600: CS7 MLR INFO: mlr_get_tcap_invoke_opCode: Operation Code Decoded
[0x2E]
*Mar 1 02:08:11.604: CS7 MLR INFO: Attempting rule match in ruleset ruleset-5
*Mar 1 02:08:11.604: CS7 MLR INFO: Rule 10 matches input packet
*Mar 1 02:08:11.604: CS7 MLR INFO: Result AS voting-as1 selected
*Mar 1 02:08:11.604: CS7 MLR INFO: MLR SCCP RC=Route to MLR destination for packet
815448A8
*Mar 1 02:08:11.604: CS7 MLR INFO: SCCP route_to_dest RC=0
*Mar 1 02:08:11.604: CS7 MLR INFO: cs7_mlr_process_sccp_data RC=Return, no error
```

The following is sample output from the **debug cs7 mlr** command with the **packet** and **verbose** keywords:

```
Router# debug cs7 mlr error verbose
00:32:06: CS7 MLR ERROR: mlr_get_sms_moForwardSm_parameters: invalid
TP-DA length of 21 digits in SMS-SUBMIT
00:32:06: Error detected in TCAP message (length=92) at offset 71
(0x47):
00:32:06: 0x62524803 0xD200D36B 0x1E281C06 0x07001186
00:32:06: 0x05010101 0xA011600F 0x80020780 0xA1090607
00:32:06: 0x04000001 0x0015026C 0x2BA12902 0x01010201
```

 debug cs7 mlr

```
00:32:06:      0x2E302184 0x06910429 0x00080082 0x06910419
00:32:06:      0x52243804 0x0F118515 0x81810000 0x000A0000
00:32:06:      0x00000BC0 0x000FF054 0x1E251D90
```

Related Commands

Command	Description
cs7 mlr table	Specifies the name of the multi-layer SMS routing table and enables CS7 MLR table mode.

debug cs7 mtp2

To display debug messages for MTP2, use the **debug cs7 mtp2 EXEC** command. The **debug cs7 mtp2** command is not available on the Cisco 7507 or Cisco 7513 platforms.

```
debug cs7 mtp2 {aerm | all | cong | error | iac | l3api | lsc | msu | rcv | suerm | timers | txc} serial
interface
```



Note

Enabling debug during high traffic can cause the link to fail.

Syntax Description

aerm	Debugs Alignment Error Rate Monitor events.
all	Enables all MTP2 debugs.
cong	Debugs Congestion Control events.
error	Debugs Error events.
iac	Debugs Initial Alignment Control events.
l3api	Debugs MTP2 Layer 3 API events.
lsc	Debugs Link State Control events.
msu	Debugs MSU messages. Use during low traffic only.
rcv	Debugs Reception Control events.
suerm	Debugs Signal Unit Error Rate Monitor events.
timers	Debugs timer events.
txc	Debugs Transmission Control events.
serial	Serial interface.
<i>interface</i>	Interface number.

Defaults

No default behavior or values.

Command History

Release	Modification
12.2(18)IXA	This command was introduced.

Usage Guidelines

The **debug cs7 mtp2** command is not available on the Cisco 7507 or Cisco 7513 platforms.

debug cs7 mtp3

To display debug messages for ITP MTP3, use the **debug cs7 mtp3** EXEC command. To disable debug, use the **no** form of this command.

```
debug cs7 mtp3 [destination ss7-access-list-num] [error linkset] [l2api linkset]  
[mgmt {error error} | {event event} | {packet point-code [in | out]}]
```

```
no debug cs7 mtp3 [destination ss7-access-list-num] [error linkset] [l2api linkset]  
[mgmt {error error} | {event event} | {packet point-code [in | out]}]
```

**Note**

Enabling debug during high traffic can cause the link to fail.

Syntax Description

destination	DPC status changes.
<i>ss7-access-list-num</i>	SS7 Access list number. Range is 2700 through 2999.
error	Error events.
<i>linkset</i>	Linkset name.
l2api	MTP3-Layer2 API events.
<i>linkset</i>	Linkset name.
mgmt	MTP3 MGMT Debug options.
error	MTP3 MGMT errors

error

- **all** All management events
- **llsc** Link Set Control
- **lsac** Link Activity Control
- **lsda** Data Link Allocation
- **lsla** Link Activation
- **lslr** Link Restoration
- **rcat** Route Set Congestion Test Control
- **rsrt** Route Set Test Control
- **rtac** Transfer Allowed Control
- **rtcc** Transfer Controlled Control
- **rtpc** Transfer Prohibited Control
- **rtre** Transfer Restricted Control
- **slm** All Link Management errors
- **sltc** Signalling Link Test Control
- **srn** All Route Management errors
- **stm** All Traffic Management errors
- **tcbe** Changeback Control
- **tcoc** Changeover Control
- **tcrc** Controlled Rerouting Control
- **tfrc** Forced Rerouting Control
- **tlac** Link Availability Control
- **tpre** Signaling Point Restart
- **trcc** Signaling Route Congestion Control
- **tsfc** Signaling Traffic Control
- **tsrc** Signaling Routing Control

event

MTP3 MGMT events.

<i>event</i>	• ALL All management errors • LLSC Link Set Control • LSAC Link Activity Control • LSDA Data Link Allocation • LSLA Link Activation • LSLR Link Restoration • RCAT Route Set Congestion Test Control • RSRT Route Set Test Control • RTAC Transfer Allowed Control • RTCC Transfer Controlled Control • RTPC Transfer Prohibited Control • RTRC Transfer Restricted Control • SLM All Link Management errors • SLTC Signalling Link Test Control • SRM All Route Management errors • STM All Traffic Management errors • TCBC Changeback Control • TCOC Changeover Control • TCRC Controlled Rerouting Control • TFRC Forced Rerouting Control • TLAC Link Availability Control • TPRC Signaling Point Restart • TRCC Signaling Route Congestion Control • TSFC Signaling Traffic Control • TSRC Signaling Routing Control
packet	MTP3 MGMT MSUs.
<i>point-code</i>	Point Code.
in	ITP MTP3 MGMT packet level debugging incoming.
out	ITP MTP3 MGMT packet level debugging outgoing.

Defaults

No default behavior or values.

Command History

Release	Modification
12.2(18)IXA	This command was introduced.

debug cs7 mtp3 paklog

To send selected message signaling units (MSU) to an appropriate monitoring tool (chosen by user), use the **debug cs7 mtp3 paklog EXEC** command.

```
debug cs7 mtp3 paklog access-list-number [linkset-name] [incoming] [outgoing]
                        [number-of-packets] [verbose]
```

```
no debug cs7 mtp3 paklog access-list-number [linkset-name] [incoming] [outgoing]
                        [number-of-packets] [verbose]
```



Note

Enabling debug during high traffic can cause the link to fail.

Syntax Description

<i>access-list-number</i>	Integer in the range 2700 to 2999, corresponding to an existing CS7 access list number, used to select packets for logging.
<i>linkset-name</i>	An existing CS7 linkset for which packet debugging is intended. If no linkset is specified packet debugging is implemented on all linksets.
incoming	Perform debugging on incoming MSUs. If neither incoming nor outgoing is specified, debugging is performed on both incoming and outgoing MSUs.
outgoing	Perform debugging on outgoing MSUs. If neither incoming nor outgoing is specified, debugging is performed on both incoming and outgoing MSUs.
<i>number-of-packets</i>	Maximum number of MSUs to copy out via UDP. Valid range is 1 to 1000000 packets. If no number is specified, all MSUs matching the access list will be sent out until the debug is turned off.
verbose	Display information to the console concerning the message being logged. It is recommended that the verbose display be used with low traffic rates only.

Defaults

If no linkset is specified packet debugging is implemented on all linksets.

If neither **incoming** nor **outgoing** is specified, debugging is performed on both incoming and outgoing MSUs.

If no *number-of-packets* is specified, all MSUs matching the access list will be sent out until the debug is turned off.

Verbose display is disabled.

Command History

Release	Modification
12.2(18)IXA	This command was introduced.

Usage Guidelines

You must configure the **cs7 paklog** command before enabling the **debug cs7 mtp3 paklog** command. If you do not, the following error message will be displayed:

```
%Error: paklog debug will not work without configuring 'cs7 paklog'.
```

Examples

In the following example, debugging is turned on for the linkset named `to_chicago` for all MSUs matching access list 2700:

```
debug cs7 mtp3 paklog 2700 to_chicago
```

The following is sample output from the **debug cs7 mtp3 paklog** command with the verbose display:

```
router# debug cs7 mtp3 paklog 2700 to_chicago verbose
```

```
16:10:44: CS7 PAKLOG Data:<135> April 23 14:33
MainITP:00003852,msu=B2001AEE00C0EE0011201112
16:10:44: CS7 PAKLOG DEBUG: sent 110 bytes to 10.4.0.90 on port 5514
16:10:44: CS7 PAKLOG Data:<135> April 23 14:33
MainITP:00003853,msu=B200C0EE001AEE0021201112
16:10:44: CS7 PAKLOG DEBUG: sent 110 bytes to 10.4.0.90 on port 5514
```

The following is sample output from the **show debug** command after the ITP packet logging facility has been configured and **debug cs7 mtp3 paklog** enabled for access list 2700.

Examples for linksets named `to_hurricane` and `to_fastnet`:

```
CS7 MTP3 (to_hurricane):
  MTP3 incoming paklog debugging is on, acl=2700, MSUs=infinite
  MTP3 outgoing paklog debugging is on, acl=2700, MSUs=infinite
```

```
CS7 MTP3 (to_fastnet):
  MTP3 incoming paklog debugging is on, acl=2700, MSUs=infinite
  MTP3 outgoing paklog debugging is on, acl=27
```

Verbose examples for linksets named `to_okracoke` and `to_okracoke2`:

```
CS7 MTP3 (to_okracoke):
  MTP3 verbose incoming paklog debugging is on, acl=2700, MSUs=infinite
  MTP3 verbose outgoing paklog debugging is on, acl=2700, MSUs=infinite
```

```
CS7 MTP3 (to_okracoke2):
  MTP3 verbose incoming paklog debugging is on, acl=2700, MSUs=infinite
  MTP3 verbose outgoing paklog debugging is on, acl=2700, MSUs=infinite
```

Examples with a specific number of MSU:

```
CS7 MTP3 (to_okracoke2):
  MTP3 incoming paklog debugging is on, acl=2701, MSUs=100
  MTP3 outgoing paklog debugging is on, acl=2700, MSUs=100
```

debug cs7 nso

To display all the ITP Non-Stop Operation (NSO) events or errors, use the **debug cs7 nso** command in privileged EXEC mode.

debug cs7 nso {**all** | **client** | **error** | **event** | | **packet** | **state**} [**verbose**]

Syntax Description

all	Display all NSO activity.
client	Display NSO RF client activity.
error	Display NSO errors.
event	Display NSO events.
packet	Display NSO control messages.
state	Display NSO state transitions.
verbose	Generate detailed debug output.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(23)SW	This command was introduced.

Examples

The following example displays all NSO activity in the verbose format:

```
Router# debug cs7 nso error verbose
```

Related Commands

Command	Description
cs7 nso	Enable ITP Non-Stop Operation (NSO).

debug cs7 nso chkpt

To display all the ITP Non-Stop Operation (NSO) checkpointing activity, use the **debug cs7 nso chkpt** command in privileged EXEC mode.

debug cs7 nso chkpt [*instance-number*] {**all** | **client** | **error** | **event** | **packet**} [**verbose**]

Syntax Description

<i>instance-number</i>	Limit debug output to a particular ITP instance.
all	Display all activity related to NSO checkpointing.
client	Display NSO checkpointing facility client activity.
error	Display NSO checkpointing errors.
event	Display NSO checkpointing events.
packet	Display NSO checkpointing messages.
verbose	Generate detailed debug output.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(23)SW	This command was introduced.

Examples

The following example displays all NSO checkpointing activity for instance 2 in the verbose format:

```
Router# debug cs7 nso chkpt 2 error verbose
```

Related Commands

Command	Description
cs7 nso	Enable ITP Non-Stop Operation (NSO).

debug cs7 offload mtp3

To display debug messages for the ITP MTP3 Offload feature, use the **debug cs7 offload mtp3 EXEC** command. To disable debug, use the **no** form of this command.

```
debug cs7 offload mtp3 {error error} | {event event}
```

```
nodebug cs7 offload mtp3
```



Warning

Enabling debug during high traffic can cause the link to fail.

Syntax Description

error	MTP3 offload errors
event	MTP3 offload events.
<i>error/event</i>	Event or Error can be monitored for the following functions: • ALL All RP errors. • DWNLD Configuration and status messages from RP to LC. • GNRL RP general • IPC IPC • LCMSG Control messages from RP to LC • MTP3_MGMT MTP3 MGMT event messages from RP to LC. • RPMSG Control messages from RP to LC. • UPLD Statistics and accounting messages from LC to RP.

Defaults

No default behavior or values.

debug cs7 sccp

To display debug messages for ITP SCCP, use the **debug cs7 sccp** EXEC command. To disable debug, use the **no** form of this command.

```
debug cs7 sccp [{error error} | {event event} | gtt-accounting | map-table | {packet [verbose]
[bytes] [packets]}]
```

```
no debug cs7 sccp
```



Warning

Enabling debug during high traffic can cause the link to fail.

Syntax Description

error	SCCP errors
<i>error</i>	Valid errors include: • ALL All SCCP errors • BCST SCMG - Broadcast • CSCC SCMG - Coordinated state change • GTT Global Title Translation • L3API SCCP-MTP3 API events • LBCS SCMG - Local broadcast • SCLC Connectionless Control • SCMG All Management components • SCOC Connection Control • SCRC Routing Control • SLCC SCMG - Local SCCP & nodal congestion • SPAC SCMG - SP allowed control • SPCC SCMG - SP congested control • SRCC SCMG - Remote SCCP & nodal congestion • SRTC SCMG - SCCP restart control • SSAC SCMG - Subsystem allowed control • SSPC SCMG - SP prohibited control • SSTC SCMG - Subsystem test control • SUA-API • TCAP-API
event	SCCP events.

<i>event</i>	Valid events include: • ALL All SCCP events • BCST SCMG - Broadcast • CSCC SCMG - Coordinated state change • GTT Global Title Translation • L3API SCCP-MTP3 API events • LBCS SCMG - Local broadcast • SCLC Connectionless Control • SCMG All Management components • SCOC Connection Control • SCRC Routing Control • SLCC SCMG - Local SCCP & nodal congestion • SPAC SCMG - SP allowed control • SPCC SCMG - SP congested control • SPPC SCMG - SP prohibited control • SRCC SCMG - Remote SCCP & nodal congestion • SRTC SCMG - SCCP restart control • SSAC SCMG - Subsystem allowed control • SSTC SCMG - Subsystem test control • SUAAPI • TCAPAPI
gtt-accounting	SCCP GTT Linkset Accounting
map-table	SCCP MAP Table Updates
packet	SCCP packet tracing
verbose	Display all bytes in the packet.
<i>bytes</i>	Number of bytes, 1 through 200
<i>packets</i>	Number of packets, 0 through 200. 0 = Unlimited (default).

Defaults

No default behavior or values.

debug cs7

To display debug messages for , use the **debug cs7 EXEC** command.

debug cs7 {all | congestion | error | event | mgmt {api | state} | packet [short] | sctp | timer}



Note

Enabling debug during high traffic can cause the link to fail.

Syntax Description

all	Enable all debugs.
api	Management API events.
congestion	Congestion Control events
error	Error events.
event	Events
mgmt	Management events.
packet	packet tracing to the mated SG.
sctp	SCTP API events for the mated SG.
state	management state machine events.
timers	timer events.

Defaults

No default behavior or values.

Command History

Release	Modification
12.2(18)IXA	This command was introduced.

debug cs7 snmp

To display debug messages for SNMP, use the **debug cs7 snmp** privileged EXEC command.

```
debug cs7 snmp {itp-acl | itp-act itp-gact | itp-grt | itp-gsccp | itp-gsp | itp-gsp2 | itp-rt | itp-sccp  
| itp-sp | itp-sp2 | itp-traps | itp-xua}
```

Syntax Description		
itp-acl		Display debugging information about CISCO-ITP-ACL-MIB: Access Lists for ITP.
itp-act		Display debugging information about CISCO-ITP-ACT-MIB: Accounting for ITP.
itp-gact		Display debugging information about CISCO-ITP-GACT-MIB
itp-grt		Display debugging information about CISCO-ITP-GRT-MIB
itp-gsccp		Display debugging information about CISCO-ITP-GSCCP-MIB
itp-gsp		Display debugging information about CISCO-ITP-GSP-MIB
itp-gsp2		Display debugging information about CISCO-ITP-GSP2-MIB
itp-rt		Display debugging information about CISCO-ITP-RT-MIB: Route Table for ITP.
itp-sccp		Display debugging information about CISCO-ITP-SCCP-MIB: Signaling Connection Control for ITP.
itp-sp		Display debugging information about CISCO-ITP-SP-MIB: Signaling Point for ITP.
itp-sp2		Display debugging information about CISCO-ITP-SP2-MIB.
itp-traps		Display debugging information about ITP traps.
itp-xua		Display debugging information about CISCO-ITP-XUA-MIB

Defaults

No default behavior or values.

debug cs7 sua

To display debug messages for SUA, use the **debug cs7 sua** EXEC command.

debug cs7 sua [**all** | **congestion** | **error** | **mgmt** {**api** | **state** {**as-name** *ASname* | **asp-name** *ASPname*} | **pointcode** {**dpc** *pointcode*}} | **packet** {**short**} {**asp-name** *ASPname*} | **sccp** | **sctp** {**asp-name** *ASPname*} | **timer** {**as-name** *ASname*}



Note

Enabling debug during high traffic can cause the link to fail.

Syntax Description

all	Enables all debugs.
api	API events.
as-name	Specify an AS.
<i>ASname</i>	AS name.
asp-name	Specify an ASP
<i>ASPname</i>	AS P name.
congestion	Debugs Congestion Control events.
dpc	Specify a point code.
error	Debugs Error events.
mgmt	Debugs Management events.
packet	Packet tracing.
pointcode	Point code.
<i>pointcode</i>	Point code.
sccp	SUA SCCP API events.
sctp	SCTP API events.
short	Truncate displayed payload at 32 bytes.
state	State machine events.
timer	AS timer events.

Defaults

No default behavior or values.

Command History

Release	Modification
12.2(18)IXA	This command was introduced.

debug cs7 tcap

To display debug messages for Cisco TCAP, use the **debug cs7 tcap** command in privileged EXEC mode.

debug cs7 tcap [**all** | **api** | **error** | **info** | **packet** [**verbose**] | **state**]

Syntax Description

all	Display all debugs.
api	Display API events.
error	Display error events.
info	Display informational events.
packet	Display packet tracing.
verbose	Display detailed packet tracing.
state	Display state machine tracing.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)IXA7	This command was introduced.

Examples

The following is sample output from the **debug cs7 tcap** command:

```
*Mar 11 18:58:27.177: CS7 TCAP State: New Dialogue state -> IDLE, tid[10]
*Mar 11 18:58:27.177: CS7 TCAP State: New Transaction state -> IDLE, tid[10]
*Mar 11 18:58:27.177: CS7 TCAP State: New operation Invoke state -> IDLE, iid[1] tid[10]
*Mar 11 18:58:27.181: CS7 TCAP State: Invoke state -> OP_SENT,class[1],iid[1],tid[10]
*Mar 11 18:58:27.181: CS7 TCAP State: Dialogue state -> IS, tid[10]
*Mar 11 18:58:27.181: CS7 TCAP State: Transaction state -> IS, tid[10]
*Mar 11 18:58:27.181: CS7 TCAP Pkt: SCCP SEND_DATA called (by MAP user layer)
*Mar 11 18:58:27.181: CS7 TCAP Pkt: data address [0x814BE510],data size [0x3C]
*Mar 11 18:58:27.185: CS7 TCAP Pkt: Calling address:
    ai [92] np [01] es [02] ssn [07] tt [00] noa [04] pc [0.0.0]
    gtd [0x814BE4B9], gt [1939294477|000A92]
    Called address:
    ai [92] np [06] es [01] ssn [06] tt [00] noa [04] pc [0.0.0]
    gtd [0x814BE48D], gt [01020304050607F8]
*Mar 11 18:58:27.185: CS7 TCAP Pkt: SCCP SEND_DATA returned without error
*Mar 11 18:58:27.189: %CS7SCCP-5-SCCPCUNAV: SCCP failed to translate: DPC=1.1.1 is not
available.
LS=NONE OPC=1.6.6 GTI=4 TT=0 NP= 6 NAI= 4 GTA=102030405060708
*Mar 11 18:58:27.189: CS7 TCAP Info: SCCP freeing TCAP data buffer routine called with
data ptr = 814BE510
```

■ `debug cs7 tcap`



ITP System Messages

This document lists and describes Cisco ITP system messages. The system software sends these messages to the console (and, optionally, to a logging server on another system) during operation. Not all system messages indicate problems with your system. Some are purely informational, and others may help diagnose problems with communications lines, internal hardware, or the system software.

Short Message Peer-to-Peer (SMPP) protocol is not supported. Some DSMR functionality is also not supported. It is recommended that commands pertaining to these features are not configured.

This document includes ITP system messages only. For a complete list of all IOS system messages, please refer to the Cisco IOS Software System Messages document at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123sup/123sems/index.htm>

How This Manual Is Organized

The messages are organized according to the particular system facility that produces the messages. The facility sections appear in alphabetical order, and within each facility section, messages are listed alphabetically by mnemonic. The messages are described in the following sections:

- [How to Read System Messages](#)
- [CS7ADDRTBL Messages](#)
- [CS7CDR Messages](#)
- [CS7CHKPT Messages](#)
- [CS7GROUP Messages](#)
- [CS7HSL Messages](#)
- [CS7M2PA Messages](#)
- [CS7MLR Messages](#)
- [CS7MTP2 Messages](#)
- [CS7MTP3 Messages](#)
- [CS7NSO Messages](#)
- [CS7PING Messages](#)
- [CS7RF Messages](#)
- [CS7ROUTE Messages](#)
- [CS7SCCP Messages](#)
- [CS7SMS Messages](#)

- [CS7TCAP Messages](#)
- [CS7XUA Messages](#)
- [DCS7 Messages](#)

How to Read System Messages

System messages begin with a percent sign (%) and are structured as follows:

%FACILITY-SUBFACILITY-SEVERITY-MNEMONIC: Message-text

FACILITY is a code consisting of two or more uppercase letters that indicate the facility to which the message refers. A facility can be a hardware device, a protocol, or a module of the system software.

SEVERITY is a single-digit code from 0 to 7 that reflects the severity of the condition. The lower the number, the more serious the situation.

MNEMONIC is a code that uniquely identifies the error message.

Message-text is a text string describing the condition. This portion of the message sometimes contains detailed information about the event, including terminal port numbers, network addresses, or addresses that correspond to locations in the system memory address space. Because the information in these variable fields changes from message to message, it is represented here by short strings enclosed in square brackets ([]). A decimal number, for example, is represented as [dec].

CS7ADDRTBL Messages

Explanation

Error Message

%CS7ADDRTBL-5-DBCHANGED: Notice: The Address Table may have changed while reading. Operation aborted.

Explanation While attempting to read, copy, or save an address table, another process modified the table.

Recommended Action Repeat the last operation and avoid making configuration changes until complete.

Error Message

%CS7ADDRTBL-3-IFSERR: Internal File System Error:

Explanation An error occurred while trying to load/parse a CS7 Address Table.

Recommended Action This problem is probably due to a corrupt or invalid file format.

Error Message

%CS7ADDRTBL-5-LOADCOMPLETE: NOTICE: Address-Table [chars] loaded from [chars].

Explanation An address-table has finished loading.

Recommended Action No action is required.

Error Message

%CS7ADDRRTBL-5-SLAVETIMEOUT: NOTICE: Address-Table loader timeout waiting on config sync to slave.

Explanation The IOS High Availability sync to the slave did not complete in an expected window

Recommended Action Reboot slave and if problem persists contact Cisco TAC.

Error Message

%CS7ADDRRTBL-5-SYNCCOMPLETE: NOTICE: Address-Table [chars] loaded on slave.

Explanation An address-table has been synchronized on the slave processor.

Recommended Action No action is required.

Error Message

%CS7ADDRRTBL-5-SYNCFAIL: NOTICE: Address-Table [chars] failed on slave.

Explanation An address-table has failed to be synchronized on the slave processor.

Recommended Action See the slave log for failure reason and contact TAC for assistance.

CS7CDR Messages

Error Message

%CS7CDR-5-CDRHASRSRC: Notice: CDR Destination [chars] has changed from no resources available to resources available.

Explanation The CDR destination may have had a disk that is full, but that condition has cleared.

Recommended Action No action is required.

Error Message

%CS7CDR-5-CDRNORSRC: Notice: CDR Destination [chars] has reported no resources available to store records.

Explanation The CDR destination may have a disk that is full.

Recommended Action No action is required.

Error Message

%CS7CDR-5-CDRSERCONGEST: Notice: CDR Service [chars] has reached its congestion threshold.

Explanation The CDR destinations within the service are not processing records fast enough

Recommended Action No action is required.

Error Message

%CS7CDR-5-CDRSEQFULL: Notice: CDR Service [chars] has reached its max queue size.

Explanation The CDR destinations within the service are not processing the records fast enough

Recommended Action No action is required.

Error Message

%CS7CDR-5-CDRSTATCHG: [chars] changed state from [chars] to [chars]

Explanation A CDR Destination changed state

Recommended Action No action is required.

CS7CHKPT Messages

Error Message

%CS7CHKPT-3-INTERR: [chars]

Explanation An internal software error has occurred.

Recommended Action Report this occurrence to Engineering. Use Topic to search for a similar DDTS. If you find none, write a DDTS for this problem.

Error Message

%CS7CHKPT-3-INVALIDINSTANCE: Invalid instance ([int])

Explanation A reference to an undefined variant instance was detected.

Recommended Action Report this occurrence to Engineering. Use Topic to search for a similar DDTS. If you find none, write a DDTS for this problem.

Error Message

%CS7CHKPT-3-MSGERR: [chars]

Explanation A Checkpointing message error has occurred.

Recommended Action Report this occurrence to Engineering. Use Topic to search for a similar DDTS. If you find none, write a DDTS for this problem.

Error Message

%CS7CHKPT-3-NOMEMORY: Insufficient memory for [chars]

Explanation The requested memory allocation failed because of a low memory condition

Recommended Action This problem is probably due to a lack of memory in the router. Either add more memory or reduce other system activity. If this message persists, call your technical support representative for assistance.

Error Message

%CS7CHKPT-5-NORCVBUF: No buffer for received checkpointing message

Explanation A buffer to hold a received Checkpointing message was not available.

Recommended Action Report this occurrence to Engineering. Use Topic to search for a similar DDTs. If you find none, write a DDTs for this problem.

Error Message

%CS7CHKPT-3-SYNCERR: [chars]

Explanation A Checkpointing synchronization error has occurred.

Recommended Action Report this occurrence to Engineering. Use Topic to search for a similar DDTs. If you find none, write a DDTs for this problem.

Error Message

%CS7CHKPT-5-SYNCFailure: ITP sync failure, peer reset

Explanation A failure occurred while synchronizing information to the High Availability peer.

Recommended Action No action required.

CS7GROUP Messages

Error Message

%CS7GROUP-3-DLINKMSG: NULL

Explanation An internal software error in ITP Group message handling has occurred.

Recommended Action Report this occurrence to Engineering. Use Topic to search for a similar DDTs. If you find none, write a DDTs for this problem.

Error Message

%CS7GROUP-3-FSMERR: [chars] event in [chars] state

Explanation An unexpected condition was encountered in the Group finite state machine.

Recommended Action Report this occurrence to Engineering. Use Topic to search for a similar DDTS. If you find none, write a DDTS for this problem.

Error Message

%CS7GROUP-3-INITERR: NULL

Explanation An internal software error in ITP Group initialization has occurred.

Recommended Action Report this occurrence to Engineering. Use Topic to search for a similar DDTS. If you find none, write a DDTS for this problem.

Error Message

%CS7GROUP-3-INTERR: NULL

Explanation An internal software error has occurred.

Recommended Action Report this occurrence to Engineering. Use Topic to search for a similar DDTS. If you find none, write a DDTS for this problem.

Error Message

%CS7GROUP-3-INVALIDINSTANCE: Invalid instance ([int])

Explanation A reference to an undefined variant instance was detected.

Recommended Action Report this occurrence to Engineering. Use Topic to search for a similar DDTS. If you find none, write a DDTS for this problem.

Error Message

%CS7GROUP-3-NEGOERR: Unexpected negotiation condition - state: [chars], peer state: [chars]

Explanation An unexpected condition was encountered in Group role negotiation.

Recommended Action Report this occurrence to Engineering. Use Topic to search for a similar DDTS. If you find none, write a DDTS for this problem.

Error Message

%CS7GROUP-3-NOMEMORY: Insufficient memory for [chars]

Explanation The requested memory allocation failed because of a low memory condition

Recommended Action This problem is probably due to a lack of memory in the router. Either add more memory or reduce other system activity. If this message persists, call your technical support representative for assistance.

Error Message

%CS7GROUP-5-NOTICE: NULL

Explanation Communicating Group information to the user.

Recommended Action No action is required.

CS7HSL Messages

Error Message

%CS7HSL-4-BADSTATE_ERROR: ([chars]): State = [chars], size = [dec]

Explanation This message indicates a SSCF-NNI is in not in a state for receiving packets. The message will display more specific information about the problem location.

Recommended Action Check the endpoint that the router is communicating with for proper configuration and operation.

Error Message

%CS7HSL-3-NOINIT: Could not initialize HSL on the [chars] interface ([chars])

Explanation Software could not initialize the interface for HSL.

Recommended Action This problem is due to an internal software error. If any of these messages recur, call your technical support representative for assistance.

Error Message

%CS7HSL-3-NOSSCFDB: No interface information provided for processing

Explanation Software requires the interface information for continued processing.

Recommended Action This problem is due to an internal software error. If any of these messages recur, call your technical support representative for assistance.

Error Message

%CS7HSL-3-NOSWIDB: No interface information provided for processing

Explanation Software requires the interface information for continued processing.

Recommended Action This problem is due to an internal software error. If any of these messages recur, call your technical support representative for assistance.

Error Message

%CS7HSL-3-NOVARIANT: Must configure CS7 variant before NNI on the interface

Explanation User may not configure NNI on the interface before CS7 variant.

Recommended Action Configure CS7 variant first, then add NNI on the interface.

Error Message

%CS7HSL-4-PKTSIZE_ERROR: ([chars]):State = [chars] size = [dec]

Explanation This message indicates a SSCF-NNI is receiving invalid sized packets. The message will display more specific information about the problem location.

Recommended Action Check the endpoint that the router is communicating with for proper configuration and operation.

Error Message

%CS7HSL-4-PROTOCOL_ERROR: ([chars]): State = [chars], status = [dec]

Explanation This message indicates a SSCF-NNI is receiving malformed packets. The message will display more specific information about the problem location.

Recommended Action Check the endpoint that the router is communicating with for proper configuration and operation.

CS7M2PA Messages

Error Message

%CS7M2PA-3-DESTADDRACT: Destination IP Address [IP_address] active for linkset:slc [chars]:[dec]

Explanation The specified destination IP address can be used by Stream Control transmission Protocol associations.

Recommended Action No action is required.

Error Message

%CS7M2PA-3-DESTADDRINA: Destination IP Address [IP_address] inactive for linkset:slc [chars]:[dec]

Explanation The specified destination IP address cannot be used by Stream Control transmission Protocol associations.

Recommended Action An destination IP address used to support a Stream Control Transmission Protocol association has failed. The association will remain active if other destination IP addresses are available. Determine the reason why this destination address failed and take appropriate action to rectify the failure.

Error Message

%CS7M2PA-5-LISTENFAILURE: Could not post listen for local peer port [int]

Explanation Software failed to post listen for the specified local peer

Recommended Action This can occur due to several reasons. Possibilities are: maximum number of local peers already created, invalid local peer parameters, local peer port is already in use, resources unavailable, etc. Peer links using this local peer will be unavailable. Problem determination should be performed for the above possibilities.

Error Message

%CS7M2PA-3-NEWIPADDR: New IP address ([IP_address]) on [chars] conflicts with cs7 local-peer [dec] local-ip [IP_address] definition.

Explanation The new IP address on the interface conflicts with the local peer configuration and may cause link failure.

Recommended Action Local and remote peer parameters must be re-configured to use the new IP address.

Error Message

%CS7M2PA-3-NOENQUEUE: Could not enqueue event to [chars] event queue.

Explanation An internal software error occurred.

Recommended Action This problem is due to an internal software error. If any of these messages recur, call your technical support representative for assistance.

Error Message

%CS7M2PA-3-NOMEMORY: Insufficient memory for [chars]

Explanation The requested memory allocation failed because of a low memory condition

Recommended Action This problem is probably due to a lack of memory in the router. Either add more memory or reduce other system activity. If this message persists, call your technical support representative for assistance.

Error Message

%CS7M2PA-3-NOPAKBUFFER: Could not get a [chars] packet buffer

Explanation Software failed to obtain a packet buffer from the global buffer pool

Recommended Action This problem is probably due to a lack of memory in the router. Either add more memory or reduce the number of CS7 interfaces. If this message persists, call your technical support representative for assistance.

Error Message

%CS7M2PA-3-NOPROC: Could not create [chars] process

Explanation Insufficient internal resources available to create process.

Recommended Action This problem is due to an internal software error. Check available memory capacity on router. If any of these messages recur, call your technical support representative for assistance.

Error Message

%CS7M2PA-3-NOPTR2PEER: No CS7 M2PA Peer Link information

Explanation Software requires the M2PA link information for continued processing.

Recommended Action This problem is due to an internal software error. If any of these messages recur, call your technical support representative for assistance.

CS7MLR Messages

Error Message

%CS7MLR-3-GTTTRIGGERDISABLED: MLR [chars] GT trigger disabled: GTI=[dec] TT=[dec]
NP=[dec] NAI=[dec] GTA=[chars]

Explanation A primary multi-layer routing global title trigger has been disabled.

Recommended Action This message informs the operator that the specified multi-layer routing trigger is no longer operational. If this was not the expected result of an issued command, contact a technical support representative for assistance.

Error Message

%CS7MLR-3-GTTTRIGGERENABLED: MLR [chars] GT trigger enabled: GTI=[dec] TT=[dec]
NP=[dec] NAI=[dec] GTA=[chars]

Explanation A primary multi-layer routing global title trigger has been enabled.

Recommended Action This message informs the operator that the specified multi-layer routing trigger is operational. If this was not the expected result of an issued command, contact a technical support representative for assistance.

Error Message

%CS7MLR-7-INTERR: Internal Software Error Detected: [chars]

Explanation An internal software error has occurred.

Recommended Action Report this occurrence to Engineering. Use Topic to search for a similar DDTS. If you find none, write a DDTS for this problem.

Error Message

%CS7MLR-3-SSNTRIGGERDISABLED: MLR [chars] PC/SSN trigger disabled: PC=[chars]
SSN=[dec]

Explanation A primary multi-layer routing PC-SSN trigger has been disabled.

Recommended Action This message informs the operator that the specified multi-layer routing trigger is no longer operational. If this was not the expected result of an issued command, contact a technical support representative for assistance.

Error Message

%CS7MLR-3-SSNTRIGGERENABLED: MLR [chars] PC/SSN trigger enabled: PC=[chars]
SSN=[dec]

Explanation A primary multi-layer routing PC-SSN trigger has been enabled.

Recommended Action This message informs the operator that the specified multi-layer routing trigger is operational. If this was not the expected result of an issued command, contact a technical support representative for assistance.

CS7MTP2 Messages

Error Message

%CS7MTP2-3-ENCAPSFAILURE: Interface [chars] could not be configured for MTP2.

Explanation The interface encapsulation command for MTP2 failed.

Recommended Action No action is required.

Error Message

%CS7MTP2-3-INVALIDPORT: Could not initialize MTP2 ([chars] cannot support SS7)

Explanation Software could not initialize the interface for MTP2 because of hardware limitations for SS7 support.

Recommended Action This problem is due to a hardware limitation for SS7 support.

Error Message

%CS7MTP2-3-MAXSS7: Maximum SS7 interfaces ([dec]) already configured on the port adapter.

Explanation Each port adapter supports a limited number of SS7 interfaces. Configuring this interface for MTP2 will exceed the maximum allowed number for the port adapter.

Recommended Action Configure MTP2 on a different port adapter.

Error Message

%CS7MTP2-3-MULTITIMESLOT: [chars] uses [dec] timeslots (multiple timeslots not supported)

Explanation User may not configure MTP2 encap on channelized interfaces that are using multiple timeslots.

Recommended Action Configure channelized interface to use one timeslot only.

Error Message

%CS7MTP2-3-NOINIT: Could not initialize MTP2 on the [chars] interface ([chars])

Explanation Software could not initialize the interface for MTP2.

Recommended Action This problem is due to an internal software error. If any of these messages recur, call your technical support representative for assistance.

Error Message

%CS7MTP2-3-NOMTP2SB: No CS7 MTP2 interface information

Explanation Software requires the MTP2 interface information for continued processing.

Recommended Action This problem is due to an internal software error. If any of these messages recur, call your technical support representative for assistance.

Error Message

%CS7MTP2-3-NOPAKBUFFER: Could not get a [chars] packet buffer for [chars]

Explanation Software failed to obtain a packet buffer from the interface buffer pool.

Recommended Action This problem is probably due to a lack of memory in the router. Either add more memory or reduce the number of CS7 interfaces. If this message persists, call your technical support representative for assistance.

Error Message

%CS7MTP2-3-NOPAKIFINPUT: Packet does not contain input interface information

Explanation Software requires the input interface information for continued processing.

Recommended Action This problem is due to an internal software error. If any of these messages recur, call your technical support representative for assistance.

Error Message

%CS7MTP2-3-NOPOWERON: PowerOn failed for the [chars] interface

Explanation Software failed to powerOn the MTP2 interface

Recommended Action This problem is due to an internal software error. If any of these messages recur, call your technical support representative for assistance.

Error Message

%CS7MTP2-3-NOPTR2CCB: No CS7 MTP2 link information

Explanation Software requires the MTP2 link information for continued processing.

Recommended Action This problem is due to an internal software error. If any of these messages recur, call your technical support representative for assistance.

Error Message

%CS7MTP2-3-NOSS7: SS7 is not supported on the [chars] interface.

Explanation SS7 is not supported on the interface.

Recommended Action No action is required.

Error Message

%CS7MTP2-3-NOSWIDB: No interface information provided for processing

Explanation Software requires the interface information for continued processing.

Recommended Action This problem is due to an internal software error. If any of these messages recur, call your technical support representative for assistance.

Error Message

%CS7MTP2-3-NOVARIANT: Must configure CS7 variant before MTP2 encap on the interface

Explanation User may not configure MTP2 encap on the interface before CS7 variant.

Recommended Action Configure CS7 variant first, then add MTP2 encap on the interface.

Error Message

%CS7MTP2-3-NOXMITQ: Failed to create transmitQ elements for [chars]

Explanation Software failed to create a pool of transmitQ elements for the interface.

Recommended Action This problem is probably due to a lack of memory in the router. Either add more memory or reduce the number of CS7 interfaces. If this message persists, call your technical support representative for assistance.

CS7MTP3 Messages

Error Message

%CS7MTP3-5-ACTDEACTLINK: Link [dec] linkset [chars] [chars] is in progress

Explanation The link activation or deactivation procedure has started.

Recommended Action No action is required.

Error Message

%CS7MTP3-5-ACTDEACTLINKSET: Linkset [chars] [chars] is in progress

Explanation Activation or deactivation of links in the linkset has started.

Recommended Action No action is required.

Error Message

%CS7MTP3-5-ADJRBEGN: Adjacent SP restart beginning for linkset [chars]

Explanation Adjacent SP restart processing has been initiated on behalf of the node adjacent to the specified linkset.

Recommended Action No action is required.

Error Message

%CS7MTP3-5-ADJRCANC: Adjacent SP restart cancelled for linkset [chars]

Explanation Adjacent SP restart was cancelled because there are no active links to the adjacent linkset.

Recommended Action No action is required.

Error Message

%CS7MTP3-5-ADJRDSBL: Adjacent SP restart disabled for linkset [chars]

Explanation Adjacent SP restart processing has been disabled for the node adjacent to the specified linkset.

Recommended Action Adjacent SP restart processing has been disabled by the configuration. If the adjacent node is restart capable, reconfigure the router to enable restart processing for the adjacent node.

Error Message

%CS7MTP3-5-ADJRENDS: Adjacent SP restart ending for linkset [chars]

Explanation Adjacent SP restart processing has completed on behalf of the node adjacent to the specified linkset.

Recommended Action No action is required.

Error Message

%CS7MTP3-5-BADCLUSTERMSG: [chars] received from [chars] with non-zero member part in destination [chars]

Explanation The received cluster management message is badly formatted. It has a non-zero member part.

Recommended Action Verify adherence to ANSI standard on adjacent point.

Error Message

%CS7MTP3-5-BADMSG: [chars] received for route ([chars] [chars]) but cluster route is [chars]

Explanation The received message would cause the cluster route to become more restrictive than the member route.

Recommended Action Verify cluster and member route status on adjacent point are consistent

Error Message

%CS7MTP3-5-BUFPAKDROP: Buffered packets for transmit exceeds maximum ([dec])

Explanation When one MTP3 link goes down, MTP3 buffers the transmit packets for that link to another link; however, MTP3 must limit the total number of buffered packets to prevent using up all of the packet buffer resources. When the number of buffered packets exceeds the maximum limit, MTP3 will drop the packets rather than buffer.

Recommended Action The user may increase the buffered packet threshold using the buffered-packet-threshold config command. However, increasing this threshold may allow MTP3 to use up all packet buffer resources and cause buffer failures for other processes in the router.

Error Message

%CS7MTP3-3-CBDROP: Packets dropped during changeback to [chars] [dec] dropped = [dec] congestion = [dec]

Explanation The software attempted a changeback procedure to the indicated link. Some packets were dropped during the changeback due to congestion.

Recommended Action Increase the congestion threshold for the specified link.

Error Message

%CS7MTP3-3-CBLINKS: Exceeded number of alternate links ([dec]) for changeback to [chars]

Explanation The software attempted a changeback procedure to the indicated linkset. The maximum number of alternate links from which messages will be diverted has been exceeded.

Recommended Action Reduce the number of alternate links defined for the linkset.

Error Message

%CS7MTP3-3-CBLINKSETS: Exceeded number of alternate linksets ([dec]) for changeback to [chars]

Explanation The software attempted a changeback procedure to the indicated linkset. The maximum number of alternate linksets from which messages will be diverted has been exceeded.

Recommended Action Reduce the number of alternate linksets defined for the linkset.

Error Message

%CS7MTP3-5-CLRACCESSVIO: Access-violations accounting database cleared by [chars]

Explanation Access-violations accounting database database has been cleared.

Recommended Action No action is required.

Error Message

%CS7MTP3-5-CLRACCT: MTP3 real-time accounting database cleared by [chars]

Explanation The MTP3 real-time accounting database has been cleared.

Recommended Action No action is required.

Error Message

%CS7MTP3-5-CLRACCTCHKPT: MTP3 checkpointed accounting database cleared by [chars]

Explanation The MTP3 checkpointed accounting database has been cleared.

Recommended Action No action is required.

Error Message

%CS7MTP3-5-CLRALL: All real-time accounting and statistics cleared by [chars]

Explanation All real-time accounting and statistics have been cleared.

Recommended Action No action is required.

Error Message

%CS7MTP3-5-CLRALLCHKPT: All accounting and statistics cleared including all checkpoint databases by [chars]

Explanation All accounting and statistics cleared including all checkpoint databases have been cleared.

Recommended Action No action is required.

Error Message

%CS7MTP3-5-CLRDYNRT: Dynamic routes for [chars] cleared by [chars]

Explanation MTP3 dynamic route entries have been cleared.

Recommended Action No action is required.

Error Message

%CS7MTP3-5-CLREVENTHIS: MTP3 event-history cleared by [chars]. Event history max = [dec]

Explanation MTP3 event-history have been cleared.

Recommended Action No action is required.

Error Message

%CS7MTP3-5-CLRGTT: SCCP GTT real-time accounting database cleared by [chars]

Explanation SCCP GTT real-time accounting database database has been cleared.

Recommended Action No action is required.

Error Message

%CS7MTP3-5-CLRGTTCHKPT: SCCP GTT checkpointed accounting database cleared by [chars]

Explanation SCCP GTT checkpointed accounting database has been cleared.

Recommended Action No action is required.

Error Message

%CS7MTP3-5-CLRSTAT: Link statistics for [chars] [chars] cleared by [chars]

Explanation Link statistics have been cleared.

Recommended Action No action is required.

Error Message

%CS7MTP3-5-CNVTONOALIAS: Unable to convert PC [chars], no alias defined for instance [dec]

Explanation MTP3 is attempting to convert a packet from one instance to another but is unable to convert a point code in the message using the point code conversion table. Since MTP3 cannot convert the point code it will drop the packet.

Recommended Action The user can configure an alias point code for the PC in the specified instance using the **cs7 pc-conversion** command

Error Message

%CS7MTP3-5-DESTSTATUS: Destination [chars] is [chars]

Explanation There was a change in the accessibility status of the destination due to a change in the status of a route to that destination.

Recommended Action The **show cs7 route** command should be used to determine the reason why a destination became inaccessible.

Error Message

%CS7MTP3-6-GROUPROLE: MTP3 Mgmt state is '[chars]'

Explanation The ITP belongs to an ITP Group and has changed MTP3 management state within the group.

Recommended Action No action is required.

Error Message

%CS7MTP3-5-HA_QUIECE: Quiece [chars] links for switchover type [dec]

Explanation MTP3 links are being quieced due to an Route Processor switchover

Recommended Action No action is required.

Error Message

%CS7MTP3-5-HA_UNQUIECE: Unquiece [chars] links for switchover type [dec]

Explanation MTP3 links are being unquieced due to an Route Processor switchover

Recommended Action No action is required.

Error Message

%CS7MTP3-3-IFSERR: Cannot load route table - ifs_copy_file failed to load '[chars]'

Explanation IOS failed to access the specified url for the route table.

Recommended Action Verify the url is correct and accessible

Error Message

%CS7MTP3-3-INHIB: Link [dec] in linkset [chars] [chars] inhibited

Explanation The specified link was either locally or remotely inhibited. Only signalling traffic between the two adjacent nodes will be transported on this link.

Recommended Action No action is required.

Error Message

%CS7MTP3-3-INHIBDENY: Inhibit denied on link [dec] in linkset [chars]

Explanation Either a local or remote inhibit requested was denied. Inhibit requests are denied when there are no alternative links that can carry the traffic.

Recommended Action No action is required.

Error Message

%CS7MTP3-3-INHIBTIMEO: [chars] request timeout on link [dec] in linkset [chars]

Explanation The inhibit or uninhibit request timed out while waiting for an acknowledgement from the remote end.

Recommended Action For inhibit request, increase the T14 timer value and re-issue the **cs7 inhibit** command. For uninhibit request, increase the T12 timer value and re-issue the **cs7 uninhibit** command.

Error Message

%CS7MTP3-5-INNI: Received [chars] message with incorrect NI - OPC = [chars] NI = [dec] on link [chars] [dec]

Explanation Received a message with incorrect network indicator.

Recommended Action This can occur due to several reasons. Possibilities are: the linkset has become congested and a changeover has occurred, causing buffered messages to be transmitted on another link, or the link is not configured correctly. If a changeover has occurred, then no action is required. For all other possibilities, the configuration should be verified and problem determination should take place.

Error Message

%CS7MTP3-5-INOPC: Received [chars] message from incorrect - OPC = [chars] SLC = [dec] message received on ls = [chars] slc = [dec] expected on ls = [chars]

Explanation Received either a MTP3 management message or a signalling link test message with an incorrect OPC. For example, a message was received from OPC 1.1.1. However, the link that received the message was configured in a linkset expecting traffic from OPC 2.2.2. The received OPC was configured as the adjacent point-code for a different linkset in the signalling point

Recommended Action Verify the configuration of the linksets at this node and the originating node.

Error Message

%CS7MTP3-5-INSLC: Received [chars] message with an incorrect SLC value - OPC = [chars] SLC = [dec] message received on ls = [chars] slc = [dec]

Explanation Received either a MTP3 management message or a signalling link test message with an incorrect SLC value. For example, a message was received from SLC value of 5. However, the link that received the message was configured with SLC value 1.

Error Message

%CS7MTP3-7-INTERR: Internal Software Error Detected: [chars]

Explanation An internal software error has occurred.

Recommended Action Report this occurrence to Engineering. Use Topic to search for a similar DDTS. If you find none, write a DDTS for this problem.

Error Message

%CS7MTP3-5-INVH0H1: Received MTP3 message with invalid H0H1: SI: [dec] H0: [dec] H1: [dec] from [chars]

Explanation The ITP received an MTP3 message that is not supported.

Recommended Action No action is required.

Error Message

%CS7MTP3-5-ISOLATED: MTP3 node has been isolated for instance [dec]

Explanation The MTP3 node has been isolated. If the node remains isolated after an automatic attempt to uninhibit inhibited links, a full restart procedure will be performed.

Recommended Action No action is required.

Error Message

%CS7MTP3-3-LINKCONG: Link [dec] in linkset [chars] is in congestion level [dec]

Explanation A link has become congested

Recommended Action No action is required.

Error Message

%CS7MTP3-3-LINKINTERR: Link Internal error - [chars] [chars] [dec] [hex]

Explanation An internal software error occurred.

Recommended Action Copy the message exactly as it appears, and report it your technical support representative.

Error Message

%CS7MTP3-5-LINKNOCONG: Link [dec] in linkset [chars] has cleared congestion

Explanation A link has abated congested

Recommended Action No action is required.

Error Message

%CS7MTP3-3-LINKNOTUP: Link [dec] in linkset [chars] failed. Reason=[chars]

Explanation A link in a linkset is no longer active. Link restoration/activation procedures will be initiated.

Recommended Action No action is required. Link should return to active state once changeover is complete. If the serial interface does not automatically recover, issue the **clear interface** command for the serial link. If that does not help, perform physical line diagnostics.

Error Message

%CS7MTP3-3-LINKSETREMOTE: Linkset [chars] received remote processor [chars] indication

Explanation A remote processor outage or remote processor recovered indication was received on one of the links in the linkset.

Recommended Action No action is required.

Error Message

%CS7MTP3-3-LINKSETSTATE: Linkset [chars] is [chars]

Explanation If the linkset is unavailable, it indicates that there are no active links in the linkset. This may be a transient condition if the links are attempting recovery. If the linkset is available, it indicates that there is at least one link in the active state.

Recommended Action If the linkset is unavailable, check the status of the links in the linkset. Also look up the reason code provided in the link inactive message and take appropriate action to rectify the deactivation.

Error Message

%CS7MTP3-6-LINKSUPDOWN: [chars]

Explanation All links on the specified FlexWAN have been activated or deactivated. This event can be triggered by two means. Either the user issued a test CLI, or the CS7 software automatically shut/started the links. To determine if this event was invoked by the CS7 software, look for a CS7 messages preceding this one, which will provide the reason for the action. If no message is found, it implies that a user issued the test cs7 CLI command to shut/start the links. If the links were shut, the state of the affected links will be displayed as sys-shut when the **show cs7 linkset** command is issued.

Recommended Action No action is required.

Error Message

%CS7MTP3-3-LINKTESTFAIL: Link test failed on link [dec] linkset [chars]
Reason=[chars]

Explanation Signaling link test has failed on the specified link. Link restoration/activation procedures will be initiated.

Recommended Action This can occur due to several reasons. Possibilities are: mismatch in point code definitions on either STP, quality of transmission line, memory corruption in either STP (local or remote), etc. Problem determination should be performed for the above possibilities. Link testing can be disabled in the link configuration sub-mode.

Error Message

%CS7MTP3-5-LINKUPDOWN: Link [dec] in linkset [chars] is [chars]

Explanation The link is either available, unavailable or down.

Recommended Action No action is required.

Error Message

%CS7MTP3-7-LSACINTERR: Internal Software Error Detected: [chars] LS [chars] [dec]
[chars] [dec] [chars] [chars] [dec]

Explanation An internal software error has occurred.

Recommended Action Report this occurrence to Engineering. Use Topic to search for a similar DDTS. If you find none, write a DDTS for this problem.

Error Message

%CS7MTP3-5-MAXDYN: Maximum ([dec]) dynamic route table entries exceeded

Explanation The system could not create a dynamic route table entry, or x-list member for ANSI, because the total number is at the maximum allowed.

Recommended Action No action is required.

Error Message

%CS7MTP3-4-NOBSNT: Timeout waiting for BSNT on link [dec] in linkset [chars]

Explanation A response to the BSNT request was not received from MTP2 during changeover.

Recommended Action This problem is due to an internal software error. If any of these messages recur, call your technical support representative for assistance.

Error Message

%CS7MTP3-3-NOBUF: No event buffers ([chars])

Explanation The software did not have enough available memory to perform a required action.

Recommended Action If condition persists, it may be necessary to increase memory configuration.

Error Message

%CS7MTP3-2-NOCLS: An internal software error occurred.

Explanation An internal software error occurred.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Research and attempt to resolve the error using the Output Interpreter <https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl>. Also perform a search of the Bug Toolkit <http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl>. If you still require assistance, open a case with the Technical Assistance Center via the Internet http://www.cisco.com/cgi-bin/front.x/case_tools/caseOpen.pl, or contact your Cisco technical support representative and provide the representative with the gathered information.

Error Message

%CS7MTP3-3-NOINSTANCE: No CS7 MTP3 instance information

Explanation Software requires the MTP3 instance information to perform this operation.

Recommended Action This problem is due to an internal software error. If any of these messages recur, call your technical support representative for assistance.

Error Message

%CS7MTP3-3-NOLINK: No CS7 MTP3 link information

Explanation Software requires the MTP3 link information to perform this operation.

Recommended Action This problem is due to an internal software error. If any of these messages recur, call your technical support representative for assistance.

Error Message

%CS7MTP3-3-NOLINKSET: An internal software error occurred.

Explanation An internal software error occurred.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Research and attempt to resolve the error using the Output Interpreter <https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl>. Also perform a search of the Bug Toolkit <http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl>. If you still require assistance, open a case with the Technical Assistance Center via the Internet http://www.cisco.com/cgi-bin/front.x/case_tools/caseOpen.pl, or contact your Cisco technical support representative and provide the representative with the gathered information.

Error Message

%CS7MTP3-3-NOMEM: No memory is available

Explanation The software did not have enough available memory to perform a required action.

Recommended Action Reduce other system activity to ease memory demands. If condition persists, it may be necessary to increase memory configuration.

Error Message

%CS7MTP3-5-NONADJSIG: Received [chars] message from non adjacent node OPC = [chars]

Explanation Received either a MTP3 management message or a signalling link test message from a non adjacent node.

Recommended Action This can occur due to several reasons. Possibilities are : the linkset has become congested and a changeover has occurred, causing buffered messages to be transmitted on another link, or the link is not configured correctly. If a changeover has occurred, then no action is required. For all other possibilities, the configuration should be verified and problem determination should take place.

Error Message

%CS7MTP3-3-NOPAK: No packet parameter provided

Explanation Software requires a packet parameter to perform this operation.

Recommended Action This problem is due to an internal software error. If any of these messages recur, call your technical support representative for assistance.

Error Message

%CS7MTP3-4-NORETRIEVE: Timeout waiting for message to be retrieved on link [dec] in linkset [chars]

Explanation A response to the retrieve request was not received from MTP2 during changeover.

Recommended Action This problem is due to an internal software error. If any of these messages recur, call your technical support representative for assistance.

Error Message

%CS7MTP3-3-NOROUTETABLE: No route table

Explanation No mtp3 route table could be loaded due to an internal error.

Recommended Action Verify provisioning of the route table. A load command with a valid url must be present

Error Message

%CS7MTP3-7-NOTFR: Restricted destination [chars] changed to available

Explanation The system is not configured to allow restricted destinations. The specified restricted destination is being changed to available.

Recommended Action Report this occurrence to Engineering. Use Topic to search for a similar DDTS. If you find none, write a DDTS for this problem.

Error Message

%CS7MTP3-6-NSOINPROG: CS7 NSO in progress for instance [dec]

Explanation Non Stop Operation has performed a failover to the Standby Route Processor. Link recovery is in progress for this instance.

Recommended Action No action is required.

Error Message

%CS7MTP3-6-NSOLINK: CS7 NSO Recived link status from slot [dec] for instance [dec]
[chars] [dec]

Explanation The link status for the indicated link required to perform Non Stop Operation has been received. When the link status is receive for all links in the instance, Non stop operation will proceed.

Recommended Action No action is required.

Error Message

%CS7MTP3-6-NSOPROCEED: CS7 NSO Proceeding for instance [dec]

Explanation Non Stop Operation has performed a failover to the Standby Route Processor. The Standby Route Processor is now ready to proceed with normal link management operations for links within this instance.

Recommended Action No action is required.

Error Message

%CS7MTP3-6-NSORESsync: CS7 NSO Resync request received from FlexWAN in slot [dec]

Explanation Non Stop operation is in process. The FlexWAN in slot [dec] is ready to be resynchronized with the Route Processor.

Recommended Action No action is required.

Error Message

%CS7MTP3-6-NSOSTANDBY: CS7 NSO is in STANDBY for instance [dec]

Explanation Non Stop Operation will be attempted for this instance in the event of a Primary Route Processor failure

Recommended Action No action is required.

Error Message

%CS7MTP3-6-NSOTIMEOUT: CS7 NSO Timeout for instance [dec]

Explanation Non Stop Operation has performed a failover to the Standby Route Processor. The Standby Route Processor has timed out while attempting to perform non-stop operation on one or more links in the instance. The affected links will be restarted. The Standby Route Processor is ready to begin normal link management operations for links within this instance.

Recommended Action No action is required.

Error Message

%CS7MTP3-5-PAKLOGCOMP: CS7 Paklog facility for linkset [chars] has completed.

Explanation The maximum amount of paklog messages for the linkset has been reached.

Recommended Action No action is required.

Error Message

%CS7MTP3-5-QOSPAKDROP: Packets dropped due to QoS class [dec] link unavailable

Explanation MTP3 is attempting to forward packets that have been marked for a specific QoS class. When the outbound linkset does not have any links available that support the marked QoS class, MTP3 tries to forward the packets over the default class (class 0) links. If QoS class 0 links are not available, MTP3 will drop the packets.

Recommended Action The **show cs7 accounting access-violations** command can be used to determine the origin and destination point codes of the dropped packets. A link can be unavailable for a QoS class for several reasons. Possibilities are: link or linkset is shut down, link failure, QoS class not assign to link. For all other possibilities, the configuration should be verified and problem determination should take place.

Error Message

%CS7MTP3-5-REMCONG: Destination [chars] is in congestion status [dec]

Explanation Remote congestion status for this destination changed due to received TFC or due to routeset congestion test procedure.

Recommended Action Investigate destination network element for cause of local link congestion.

Error Message

%CS7MTP3-4-RETRIEVE: Message retrieved after timeout on link [dec] in linkset [chars]

Explanation A retrieved message was received from MTP2 after the timer expired.

Recommended Action This problem is due to an internal software error. If any of these messages recur, call your technical support representative for assistance.

Error Message

%CS7MTP3-5-ROUTETABLELOADED: Route table '[chars]' has been loaded from '[chars]'

Explanation Route table has been successful loaded

Recommended Action No action is required.

Error Message

%CS7MTP3-5-RSRTBEGN: MTP3 full restart beginning for instance [dec]

Explanation MTP3 full restart processing has been initiated.

Recommended Action No action is required.

Error Message

%CS7MTP3-5-RSRTCONT: MTP3 restart continuing for Instance [dec]

Explanation MTP3 restart has detected a sufficient number of available links to continue with the restart.

Recommended Action No action is required.

Error Message

%CS7MTP3-5-RSRTENDS: MTP3 full restart completed for instance [dec]

Explanation MTP3 full restart processing has completed.

Recommended Action No action is required.

Error Message

%CS7MTP3-5-RSRTFRST: MTP3 full restart is disabled for instance [dec]

Explanation The MTP3 fast restart option has been configured. This option bypasses the normal MTP3 full restart processing.

Recommended Action Reconfigure the router to disable the fast restart option and restart the router.

Error Message

%CS7MTP3-5-RSRTNOACT: Expected links in linkset [chars] are not active instance [dec]

Explanation The expected number of links in the linkset did not become available during the link activation phase of the MTP3 restart procedure.

Recommended Action Check that the links that are expected to become available during MTP3 restart are able to become available at layer 2. Links that are not expected to become available should be administratively shutdown.

Error Message

%CS7MTP3-5-RSRTNOTRA: No TRA received from the adjacent node on linkset [chars]
instance [dec]

Explanation The ITP expected to receive a TRA message from the adjacent node.

Recommended Action Check that the adjacent node is restart capable. If the adjacent node is not restart capable, reconfigure the ITP to disable adjacent restart for the concerned linkset.

Error Message

%CS7MTP3-5-RSRTSEND: MTP3 restart has entered the send status phase for instance
[dec]

Explanation MTP3 restart has entered the send status phase. TFP and TFR signals are sent to adjacent nodes during the send status phase.

Recommended Action No action is required.

Error Message

%CS7MTP3-5-RSRTT18: MTP3 restart T18 Expired instance [dec]

Explanation A sufficient number of TRAs were not available to proceed with a normal MTP3 restart.

Recommended Action No action is required.

Error Message

%CS7MTP3-5-RSRTT22: MTP3 restart T22 Expired instance [dec]

Explanation A sufficient number of links were not available to proceed with a normal MTP3 restart.

Recommended Action No action is required.

Error Message

%CS7MTP3-5-RSRTT23: MTP3 restart T23 Expired instance [dec]

Explanation MTP3 restart did not receive an expected TRA from every adjacent node

Recommended Action No action is required.

Error Message

%CS7MTP3-5-RSRTTIMO: MTP3 restart terminating before send status completed for
instance [dec]

Explanation MTP3 restart timeout out while in the send status phase.

Recommended Action Verify that the MTP3 timers T22, T23, and T24 have been configured to appropriate values. Increase the timer values as required.

Error Message

%CS7MTP3-5-RSRTXTRA: MTP3 restart expected TRAs have been received for instance [dec]

Explanation MTP3 restart has received a TRA for every active linkset and is continuing with the restart.

Recommended Action No action is required.

Recommended Action

Error Message

%CS7MTP3-6-SRTFAILTMR: CS7 Signaling Route Test (SRT) FAILED (timer expiration) to: [chars] from: [chars] sls: [dec]

Explanation TTC Signaling Route Test was performed and failed

Recommended Action No action is required.

Error Message

%CS7MTP3-6-SRTPASS: CS7 Signaling Route Test (SRT) PASSED to: [chars] from: [chars] sls: [dec]

Explanation TTC Signaling Route Test was performed and succeeded

Recommended Action No action is required.

Error Message

%CS7MTP3-6-SRTRESP: CS7 Signaling Route Test (SRT) request received, response sent to: [chars] from: [chars] sls: [dec]

Explanation TTC Signaling Route Test request was received and an SRTA acknowledgement was sent in response

Recommended Action No action is required.

Error Message

%CS7MTP3-5-TFRINVALID: Received TFR from [chars], TFR option is off

Explanation The use of TFR messages is a National Option and this node is configured to not use TFRs.

Recommended Action If TFRs should be used in this network, the option can be turned on with the command **cs7 national-options TFR**. If TFRs should not be used, the adjacent node may be misconfigured.

Error Message

%CS7MTP3-5-UNEXPECTRA: An unexpected TRA was received on linkset [chars]

Explanation A TRA message was received on the linkset but the linkset is not configured to perform an adjacent SP restart.

Recommended Action Verify that the adjacent node is restart capable. If the adjacent node is restart capable, reconfigure the router to enable restart processing for the adjacent node. If the adjacent node is not restart capable, then investigate why it is sending a TRA message on the linkset.

Error Message

%CS7MTP3-5-UNEXPECTRW: An unexpected TRW was received on linkset [chars]

Explanation A TRW message was received on the linkset but the linkset is not configured to perform an adjacent SP restart.

Recommended Action Verify that the adjacent node is restart capable. If the adjacent node is restart capable, reconfigure the router to enable restart processing for the adjacent node. If the adjacent node is not restart capable, then investigate why it is sending a TRWE message on the linkset.

Error Message

%CS7MTP3-3-UNINHBNOTP: Uninhibit is not possible on link [dec] in linkset [chars]

Explanation Uninhibit is not possible on the link since the remote SP is not accessible. This could be due the fact that the link has failed.

Recommended Action Restart the failed link.

Error Message

%CS7MTP3-5-UNINHIB: Link [dec] in linkset [chars] [chars] uninhibited

Explanation The specified link was either locally or remotely uninhibited. Normal traffic will now be transported on this link.

Recommended Action No action is required.

Error Message

%CS7MTP3-5-UNOPC: Received [chars] message from undefined - OPC = [chars] SLC = [dec] message received on ls = [chars] slc = [dec]

Explanation Received either a MTP3 management message or a signalling link test message with an undefined OPC. For example, a message was received from OPC 1.1.1. However, the link that received the message was configured in a linkset expecting traffic from OPC 2.2.2. The received OPC has not been defined as the adjacent point-code for any other linkset configured for this signalling point.

Recommended Action Verify the configuration of the linksets at this node and the originating node.

Error Message

%CS7MTP3-5-UNSIO: Received [chars] message with unsupported SIO: [dec] on link [chars] [dec]

Explanation Received a message with unsupported service indicator octet.

Recommended Action No action is required.

Error Message

%CS7MTP3-5-UNSLC: Received [chars] message with an undefined SLC value - OPC = [chars] SLC = [dec] message received on ls = [chars] slc = [dec]

Explanation Received either a MTP3 management message or a signalling link test message with an unknown SLC value. For example, a message was received from SLC value of 5. However, the link that received the message was configured with SLC value 1. The linkset on which the packet was received does not have a link configured with the received SLC value.

Recommended Action

CS7NSO Messages

Error Message

%CS7NSO-5-CONFIGINOPER: ITP NSO is going inoperative due to a configuration change. Reset of standby is required.

Explanation ITP NSO is now inoperative because it has been disabled in the configuration. This causes a reset of the Standby unit.

Recommended Action No action is required.

Error Message

%CS7NSO-5-CONFIGOPER: ITP NSO is going operative due to a configuration change

Explanation ITP NSO is now operative because it has been enabled in the configuration.

Recommended Action No action is required.

Error Message

%CS7NSO-3-INITERR: [chars]

Explanation An internal software error in ITP NSO initialization has occurred.

Recommended Action Report this occurrence to Engineering. Use Topic to search for a similar DDTS. If you find none, write a DDTS for this problem.

Error Message

%CS7NSO-3-INTERR: [chars]

Explanation An internal software error in ITP NSO has occurred.

Recommended Action Report this occurrence to Engineering. Use Topic to search for a similar DDTS. If you find none, write a DDTS for this problem.

Error Message

%CS7NSO-3-IPCERROR: [chars] [chars]

Explanation An error has occurred establishing an interprocess communication channel between the active system and the standby system.

Recommended Action Report this occurrence to Engineering. Use Topic to search for a similar DDTS. If you find none, write a DDTS for this problem.

Error Message

%CS7NSO-3-MSGERR: [chars]

Explanation An internal software error in ITP NSO message handling has occurred.

Recommended Action Report this occurrence to Engineering. Use Topic to search for a similar DDTS. If you find none, write a DDTS for this problem.

Error Message

%CS7NSO-3-NOEVENTQLEM: No NSO event queue elements

Explanation An element for queueing an internal NSO event was not available.

Recommended Action Report this occurrence to Engineering. Use Topic to search for a similar DDTS. If you find none, write a DDTS for this problem.

Error Message

%CS7NSO-3-NOMEMORY: Insufficient memory for [chars]

Explanation The requested memory allocation failed because of a low memory condition

Recommended Action This problem is probably due to a lack of memory in the router. Either add more memory or reduce other system activity. If this message persists, call your technical support representative for assistance.

Error Message

%CS7NSO-3-NOMSGQLEM: No NSO message queue elements for received message

Explanation An element for queueing a received NSO message was not available.

Recommended Action Report this occurrence to Engineering. Use Topic to search for a similar DDTs. If you find none, write a DDTs for this problem.

CS7PING Messages

Error Message

%CS7PING-3-CONTEXT: Q.755 Test: [chars] context

Explanation Internal software error

Recommended Action If problem persists call your Cisco technical support representative and provide the representative with the gathered information.

Error Message

%CS7PING-6-DUP: Test Q.755 [chars]: duplicate test request ignored

Explanation An attempt was made to start a second traffic test between signalling points. Only a single MTP traffic way be started between a pair of signalling points.

Recommended Action Wait till existing test has completed or issue command to cancel current test prior to stating new test

Error Message

%CS7PING-3-FAIL: Q.755 Test [chars]: cannot create [chars]

Explanation Software could not allocate resources required to run requested traffic test.

Recommended Action Retry request.

Error Message

%CS7PING-3-FSM: Test Q.755 [chars]: fsm error ([chars]/[chars]/[dec])

Explanation An internal software error occurred.

Recommended Action Stop the running traffic test with 'ping cs7 stop x.x.x'

Error Message

%CS7PING-3-INTERN: Test Q.755 [chars]: internal error ([chars]/[chars])

Explanation An internal software error occurred.

Recommended Action Stop the running traffic test with 'ping cs7 stop x.x.x' command

Error Message

%CS7PING-3-NOPAK: Test Q.755 [chars]: no packet buffer ([chars]/[chars])

Explanation Software could not find a packet buffer to send a message.

Recommended Action Stop the running traffic test with 'ping cs7 stop x.x.x'.

Error Message

%CS7PING-6-NORoute Processor: [chars]: No response from target node.

Explanation The node timed out while waiting for a response from the target node.

Recommended Action Ensure that the target node is reachable.

Error Message

%CS7PING-6-RTT: Test Q.755 [chars]: MTP Traffic test rtt [dec]/[dec]/[dec]

Explanation The MTP Traffic test to the specified point code has completed.

Recommended Action No action is required.

Error Message

%CS7PING-3-SEND: Test Q.755 [chars]: failed to send [chars] message

Explanation Software could not allocate resources required to run requested traffic test.

Recommended Action Retry request.

Error Message

%CS7PING-4-SEQ: Test Q.755 [chars]: received sequence [dec], expected [dec]

Explanation Traffic test verification received an out of sequence packet.

Recommended Action Verify network topology and configuration.

Error Message

%CS7PING-6-STAT: Test Q.755 [chars]: MTP Traffic test [dec]% successful ([dec]/[dec])

Explanation The MTP Traffic test to the specified signalling point has completed.

Recommended Action No action is required.

Error Message

%CS7PING-6-TERM: Test Q.755 [chars]: MTP Traffic test terminated.

Explanation Q.755 traffic test terminated.

Recommended Action No action is required.

Error Message

%CS7PING-6-TURN: Q.755 Test [chars]: MTP Traffic test requested

Explanation A remote signalling point requested a MTP traffic test

Recommended Action No action is required.

CS7RF Messages

Recommended Action**Error Message**

%CS7RF-3-BADCLIENT: Unknown RF client [int]

Explanation An RF message was received from an unknown RF client.

Recommended Action Report this occurrence to Engineering. Use Topic to search for a similar DDTS. If you find none, write a DDTS for this problem.

Error Message

%CS7RF-3-INTERR: NULL

Explanation An internal software error in ITP NSO has occurred.

Recommended Action Report this occurrence to Engineering. Use Topic to search for a similar DDTS. If you find none, write a DDTS for this problem.

Error Message

%CS7RF-3-MSGERR: NULL

Explanation An internal software error in ITP RF message handling has occurred.

Recommended Action Report this occurrence to Engineering. Use Topic to search for a similar DDTS. If you find none, write a DDTS for this problem.

Error Message

%CS7RF-3-NOMEMORY: Insufficient memory for [chars]

Explanation The requested memory allocation failed because of a low memory condition

Recommended Action This problem is probably due to a lack of memory in the router. Either add more memory or reduce other system activity. If this message persists, call your technical support representative for assistance.

CS7ROUTE Messages

Error Message

%CS7ROUTE-3-BADLS: Error in route table file, line [dec], byte [dec]: no linkset with index [dec]

Explanation Error in route table

Recommended Action Correct the error in the route table file

Error Message

%CS7ROUTE-3-DUPLS: Error in route table file, line [dec], byte [dec]: linkset number defined twice

Explanation Syntax error in route table

Recommended Action Correct the syntax error in the route table file

Error Message

%CS7ROUTE-3-INFO: Error in route table file, line [dec], byte [dec]: expected info element

Explanation Syntax error in route table

Recommended Action Correct the syntax error in the route table file

Error Message

%CS7ROUTE-3-INFOLS: Error in route table file, line [dec], byte [dec]: expected linkset index

Explanation Syntax error in route table

Recommended Action Correct the syntax error in the route table file

Error Message

%CS7ROUTE-3-INSERT: Error loading route table file, line [dec]: cannot insert route [chars]/[dec]

Explanation Internal error inserting node into rtree

Recommended Action Report this occurrence to Engineering. Use Topic to search for a similar DDTs. If you find none, write a DDTs for this problem.

Error Message

%CS7ROUTE-3-INSINFO: Error loading route table file, line [dec]: cannot activate route [chars]/[dec] linkset [chars] priority [dec]

Explanation Error in route table

Recommended Action Correct the error in the route table file

Error Message

%CS7ROUTE-3-LSIND: Error in route table file, line [dec], byte [dec]: linkset index too high

Explanation Attempt to load more than 1024 linkset definitions

Recommended Action ITP configuration is too big

Error Message

%CS7ROUTE-3-LSNUM: Error in route table file, line [dec], byte [dec]: expected linkset number

Explanation Syntax error in route table

Recommended Action Correct the syntax error in the route table file

Error Message

%CS7ROUTE-3-MASK: Error in route table file, line [dec], byte [dec]: invalid mask length [dec]

Explanation Syntax error in route table

Recommended Action Correct the syntax error in the route table file

Error Message

%CS7ROUTE-3-NOLS: Error in route table file, line [dec], byte [dec]: linkset [chars] does not exist

Explanation Syntax error in route table

Recommended Action Correct the syntax error in the route table file

Error Message

%CS7ROUTE-3-NOMASK: Error in route table file, line [dec], byte [dec]: expected mask

Explanation Syntax error in route table

Recommended Action Correct the syntax error in the route table file

Error Message

%CS7ROUTE-3-NOPRIO: Error in route table file, line [dec], byte [dec]: expected priority

Explanation Syntax error in route table

Recommended Action Correct the syntax error in the route table file

Error Message

%CS7ROUTE-3-NOQOS: Error in route table file, line [dec], byte [dec]: expected QoS value

Explanation Syntax error in route table

Recommended Action Correct the syntax error in the route table file

Error Message

%CS7ROUTE-3-PC: Error in route table file, line [dec], byte [dec]: linkset [chars] does not exist

Explanation Syntax error in route table

Recommended Action Correct the syntax error in the route table file

Error Message

%CS7ROUTE-3-PRIO: Error in route table file, line [dec], byte [dec]: invalid priority [dec]

Explanation Syntax error in route table

Recommended Action Correct the syntax error in the route table file

Error Message

%CS7ROUTE-3-QOS: Error in route table file, line [dec], byte [dec]: invalid QoS value [hex]

Explanation Syntax error in route table

Recommended Action Correct the syntax error in the route table file

Error Message

%CS7ROUTE-3-RECORD: Error in route table file, line [dec]: expected L/R record

Explanation Syntax error in route table

Recommended Action Correct the syntax error in the route table file.

CS7SCCP Messages

Error Message

%CS7SCCP-5-BADGT: SCCP MGMT received message with invalid routing indicator.
LS=[chars] DPC=[chars] OPC=[chars] GTI=[dec] RI=[dec]

Explanation SCCP MGMT received a message that was not supported.

Recommended Action No action is required.

Error Message

%CS7SCCP-5-CLRGTTMEAS: Global GTT measurements were cleared by [chars]

Explanation The SCCP global GTT measurements were cleared.

Recommended Action No action is required.

Error Message

%CS7SCCP-5-GTTIFSPARSE: GTT file parse error: [chars]

Explanation A syntax or semantic error occurred while trying to read in the GTT config

Recommended Action No action is required.

Error Message

%CS7SCCP-5-GTTIFPARSEWARN: NOTICE: GTT file parse warning: [chars]

Explanation A syntax or semantic error occurred while trying to read in the GTT config

Recommended Action No action is required.

Error Message

%CS7SCCP-5-GTTREPFALL: GTT Replace of file:[chars] failed. Previous database retained.

Explanation The file specified in the error failed to be bulk loaded to the ITP. Probably the result of a bad or corrupt file.

Recommended Action Re-issue the **cs7 gtt replace-db** command with a valid file free of errors.

Error Message

%CS7SCCP-5-GTTTBL_LOAD_BEGIN: GTT load of [chars] begins.

Explanation The load process of reading a GTT table into main memory has begun.

Recommended Action No action is required.

Error Message

%CS7SCCP-5-GTTTBL_LOAD_END: GTT load of [chars] has completed

Explanation The load process of reading a GTT table into main memory has finished.

Recommended Action No action is required.

Error Message

%CS7SCCP-5-GTTTBL_SAVE_BEGIN: GTT save to [chars] has begun

Explanation The save process of a GTT table has begun.

Recommended Action No action is required.

Error Message

%CS7SCCP-5-GTTTBL_SAVE_END: GTT save to [chars] has completed

Explanation The save process of a GTT table has completed.

Recommended Action No action is required.

Error Message

%CS7SCCP-5-HOPCNT: SCCP received message with hop counter expired.
LS=[chars] MSG_TYPE=[chars] OPC=[chars] GTI=[dec] TT=[dec] NP=[chars] NAI=[chars]
GTA=[chars]

Explanation SCCP received a message with an expired hop counter.

Recommended Action No action is required.

Error Message

%CS7SCCP-3-IFSEERR: Cannot load gtt configuration - ifs_copy_file failed to load
'[chars]'

Explanation IOS failed to access the specified url for the gtt configuration.

Recommended Action Verify the URL is correct and accessible.

Error Message

%CS7SCCP-7-INTERR: Internal Software Error Detected: [chars]

Explanation An internal software error has occurred.

Recommended Action Report this occurrence to Engineering. Use Topic to search for a similar DDTS. If you find none, write a DDTS for this problem.

Error Message

%CS7SCCP-5-INV_GTI: SCCP received message with invalid Global Title Indicator.
LS=[chars] DPC=[chars] OPC=[chars] GTI=[dec] RI=[dec]

Explanation SCCP received message with an invalid or not supported Global Title Indicator.

Recommended Action Notify originator of message to correct the invalid or unsupported message.

Error Message

%CS7SCCP-5-INVMSGTYPE: SCCP received message for GTT of an invalid type.
LS=[chars] DPC=[chars] OPC=[chars] Type=[dec] Class=[chars]

Explanation SCCP received a message for GTT that was not supported.

Recommended Action No action is required.

Error Message

%CS7SCCP-5-MTP3FAIL: MTP3 was unable to route the message, PC=[chars] SSN=[dec].
LS=[chars] OPC=[chars] GTI=[dec] TT=[dec] NP=[chars] NAI=[chars] GTA=[chars]

Explanation MTP3 failed to route the message due to user misconfiguration or software error

Recommended Action No action is required.

Error Message

%CS7SCCP-5-NIMISMATCH: SCCP received msu with wrong network ind. in Called Party.
LS=[chars] OPC=[chars] GTI=[dec] TT=[dec] NP=[chars] NAI=[chars] GTA=[chars]
NI=[dec]

Explanation SCCP received a message which contain a unsupported network indicator.

Recommended Action Notify originator of message to send supported network indicator in SCCP Called Party.

Error Message

%CS7SCCP-5-NOAPPGRPMEM: SCCP translated message to app-group with no available members.

LS=[chars] OPC=[chars] GTI=[dec] TT=[dec] NP=[chars] NAI=[chars] GTA=[chars]
SSN=[chars] AppGrp=[chars]

Explanation SCCP received a message that translated to a application group with no available members.

Recommended Action No action is required.

Error Message

%CS7SCCP-5-NOCLDSSN: SCCP received message with no called party SSN present.

LS=[chars] MSG_TYPE=[chars] OPC=[chars] GTI=[dec] TT=[dec] NP=[chars] NAI=[chars]
GTA=[chars]

Explanation SCCP received a message that did not contain a SSN where it was required.

Recommended Action Verify that the source of the MSU is sending properly formatted messages.

Error Message

%CS7SCCP-5-NOSELECT: SCCP received message for which no selector is defined.

LS=[chars] MSG_TYPE=[chars] OPC=[chars] GTI=[dec] TT=[dec] NP=[chars] NAI=[chars]
GTA=[chars]

Explanation No matching selector entry was found in the CS7 GTT Selector table for the given translation.

Recommended Action Use the **cs7 gtt selector** command to add the referenced selector to the database.

Error Message

%CS7SCCP-5-NOTRANS: SCCP received message with no translation for GTA.

LS=[chars] MSG_TYPE=[chars] OPC=[chars] GTI=[dec] TT=[dec] NP=[chars] NAI=[chars]
GTA=[chars]

Explanation No matching GTA entry was found in the CS7 GTT GTA table for the given translation.

Recommended Action Use the **cs7 gtt gta** command to add the referenced GTA into to the table under the appropriate selector.

Error Message

%CS7SCCP-5-REASSUNSUPP: SCCP received message requiring reassembly.

LS=[chars] OPC=[chars] DPC=[chars] GTI=[dec] TT=[dec] NP=[chars] NAI=[chars]
GTA=[chars] RI=[dec] SSN=[chars]

Explanation SCCP received a message that requires reassembly, which is not supported.

Recommended Action No action is required.

Error Message

%CS7SCCP-5-SCCCPRPTTERM: NOTICE: report terminated due to DB change

Explanation The last show command for SCCP/GTT related data was prematurely terminated because a config change occurred during the reports execution

Recommended Action Re-issue the SCCP/GTT show command that was terminated.

Error Message

%CS7SCCP-5-SCCPAVL: SCCP at [chars] is available.

Explanation A SSA (subsystem available) message was received for SCCP. GTT translations destined for the SP will be processed

Recommended Action No action is required.

Error Message

%CS7SCCP-5-SCCPCONVFAIL: SCCP failed conversion to alternate instance.
LS=[chars] MSG_TYPE=[chars] OPC=[chars] GTI=[dec] TT=[dec] NP=[chars] NAI=[chars]
GTA=[chars]

Explanation SCCP received a message which was GT translated to an alternate instance. During the instance conversion a failure occurred.

Recommended Action Check the configuration of alias point-codes for the desired conversion.

Error Message

%CS7SCCP-5-SCCPGNRL: Translated DPC unavailable LS=[chars] MSG_TYPE=[chars]
OPC=[chars] GTI=[dec] TT=[dec] NP=[chars] NAI=[chars] GTA=[chars] SSN=[chars]

Explanation An error has occurred at the SCCP layer.

Recommended Action Refer to the message details for more information about the error.

Error Message

%CS7SCCP-5-SCCPGTTDBCHANGED: SCCP GTT database changed during read

Explanation A read of cs7:gtt-tables/gtt_default was aborted because the GTT database changed during the read.

Recommended Action Retry the read or save that was aborted. Do not make make GTT changes while the read or save is in progress.

Error Message

%CS7SCCP-5-SCCPGTTREPSYNCFAIL: GTT config sync to slave failed

Explanation A failure has occurred while trying to copy the GTT running config to the slave processor.

Recommended Action Reset the slave processor and verify the GTT config is copied over after reset.

Error Message

%CS7SCCP-5-SCCPGTTSYNC_BEGIN: GTT config sync to slave has begun. GTT config commands are currently disabled.

Explanation An information message indicating that the GTT tables have begun the sync process to the slave RP. During this process no GTT config commands can be executed.

Recommended Action No action is required.

Error Message

%CS7SCCP-5-SCCPGTTSYNC_END: GTT config sync to slave has completed. GTT config commands are enabled.

Explanation An information message indicating that the GTT tables have been copied to the slave RP successfully.

Recommended Action No action is required.

Error Message

%CS7SCCP-5-SCCPNOMAP: SSCP failed to translate, no MAP entry.
CDPA PC=[chars] SSN=[dec] LS=[chars] OPC=[chars] GTI=[dec] TT=[dec] NP=[chars]
NAI=[chars] GTA=[chars]

Explanation No matching GTT MAP entry was found for the CdPA PC/SSN.

Recommended Action Configure the PC/SSN in the GTT MAP table.

Error Message

%CS7SCCP-5-SCCPPCCONG: SSCP failed to translate: DPC=[chars] is congested.
LS=[chars] OPC=[chars] GTI=[dec] TT=[dec] NP=[chars] NAI=[chars] GTA=[chars]

Explanation Translation resulted in new PC, but the PC is congested.

Recommended Action Check traffic load and distribution to given MAP.

Error Message

%CS7SCCP-5-SCCPUNAV: SSCP failed to translate: DPC=[chars] is not available.
LS=[chars] OPC=[chars] GTI=[dec] TT=[dec] NP=[chars] NAI=[chars] GTA=[chars]

Explanation Translation resulted in new PC, but the PC is not available.

Recommended Action Ensure MTP3 has available route to the PC.

Error Message

%CS7SCCP-5-SCCPSSCONG: SSN is congested for the translated node, CDPA PC=[chars]
SSN=[dec].
LS=[chars] OPC=[chars] GTI=[dec] TT=[dec] NP=[chars] NAI=[chars] GTA=[chars]

Explanation Translation resulted in new PC/SSN, but the SSN is congested.

Recommended Action Check traffic load and distribution to given MAP.

Error Message

%CS7SCCP-5-SCCPSSUNAV: SSN is not available for the translated node, CDPA
PC=[chars] SSN=[dec].
LS=[chars] OPC=[chars] GTI=[dec] TT=[dec] NP=[chars] NAI=[chars] GTA=[chars]

Explanation Translation resulted in new PC/SSN, but the SSN is unavailable.

Recommended Action Check the MAP's subsystem status.

Error Message

%CS7SCCP-5-SCCPUNAV: SSCP is not available on CDPA PC=[chars] SSN=[dec].
LS=[chars] OPC=[chars] GTI=[dec] TT=[dec] NP=[chars] NAI=[chars] GTA=[chars]

Explanation Translation resulted in new PC/SSN, but a UPU has been received for the MAP.

Recommended Action Check the MAP's subsystem status.

Error Message

%CS7SCCP-5-SSA: Subsystem [dec] at [chars] is available.

Explanation A subsystem available message was received for the specified SS.

Recommended Action No action is required.

Error Message

%CS7SCCP-5-SSP: Subsystem [dec] at [chars] is not available.

Explanation A subsystem prohibited message was received for the specified SS.

Recommended Action No action is required.

Error Message

%CS7SCCP-5-UNEQUIPSS: SCCP received message for invalid or unequipped SSN.
 LS=[chars] OPC=[chars] DPC=[chars] GTI=[dec] TT=[dec] NP=[chars] NAI=[chars]
 GTA=[chars] RI=[dec] SSN=[chars]

Explanation SCCP received a message that was not supported.

Recommended Action No action is required.

Error Message

%CS7SCCP-5-UNQUALIFIED: SCCP received message which caused an unqualified error.
 LS=[chars] MSG_TYPE=[chars] OPC=[chars] GTI=[dec] TT=[dec] NP=[chars] NAI=[chars]
 GTA=[chars]

Explanation SCCP received a message which produced an unqualified internal software error.

Recommended Action Contact Cisco Technical Assistance Center.

Error Message

%CS7SCCP-5-UPU: SCCP at [chars] is unavailable.

Explanation An UPU (user part unavailable) message was received for the specified SP. GTT translations destined for the SP will fail.

Recommended Action No action is required.

Error Message

%CS7SCCP-5-UPU_NOT_EQP: No SCCP at [chars].

Explanation An UPU (user part unavailable) message with cause code of <<missing text>>

Recommended Action No action is required.

Error Message

%Error: command is not applied to xUA DPC

Explanation The command is not applicable to xUA DPC.

Recommended Action Apply the command to SS7/M2PA DPC.

Error Message

%Error: BPC and BSSN must both be specified for dominant or shared multiplicity

Explanation A backup point code and subsystem is not specified when mode is set as dominant or shared.

Recommended Action A backup point code and subsystem must be specified if mode (multiplicity) is dominant or shared.

Error Message

%Error: PC/SSN is being used as a backup.

Explanation Cannot delete an entry for which a backup entry already exists.

Recommended Action A PC/SSN entry cannot be deleted if it is referenced by an entry in the GTA table.

Error Message

%Error: SSN specified is referenced by gta, sua, mapua, pc-conversion or mlr

Explanation Cannot delete a referenced entry.

Recommended Action A PC/SSN entry cannot be deleted if it is referenced by an entry in the GTA table.

Error Message

%Error: Primary and backup point codes cannot be equal.

Explanation The primary and backup point codes are set to be identical.

Recommended Action Set the primary and backup point codes to not be identical.

CS7SMS Messages

Error Message

%CS7SMS-7-INTERR: Internal Software Error Detected: [chars]

Explanation An internal software error has occurred.

Recommended Action Report this occurrence to Engineering. Use Topic to search for a similar DDTS. If you find none, write a DDTS for this problem.

Error Message

%CS7SMS-3-MSCPROXYADDRFAIL: SMS GSM MAP msc-proxy-addr lookup failed. MSC PC [chars] is not defined in msc-proxy-addr table.

Explanation A SMS GSM MAP MSC proxy address lookup has failed.

Recommended Action This message informs the operator that the specified calling address MSC PC was not found in the SMS GSM MAP msc-proxy-addr table. Therefore, the MO-ForwardSM could not be built. Define this MSC PC in the msc-proxy-addr table to resolve this issue.

Error Message

%CS7SMS-3-SESSACTIVE: SMS [chars] session active, [chars] [IP_address]:[dec]

Explanation An SMS SMPP or UCP session has become active.

Recommended Action This message informs the operator that the specified SMPP or UCP session is now operational. No operator action is required.

Error Message

%CS7SMS-3-SESSBINDFAIL: SMS [chars] session failed, [chars] [IP_address]:[dec], reason:[chars]

Explanation An SMS SMPP or UCP session activation attempt has failed.

Recommended Action This message informs the operator that the specified SMPP or UCP session could not be activated. Modify the local or remote configuration to resolve the connectivity issue.

Error Message

%CS7SMS-3-SESSCONNECTFAIL: SMS connection attempt failed, ip=[IP_address] port=[dec], reason:[chars]

Explanation An SMS SMPP or UCP session connection attempt has failed.

Recommended Action This message informs the operator that the specified SMPP or UCP session could not be activated. Modify the local or remote configuration to resolve the connectivity issue.

Error Message

%CS7SMS-3-SESSINACTIVE: SMS [chars] session inactive, [chars] [IP_address]:[dec]

Explanation An SMS SMPP or UCP session has become inactive.

Recommended Action This message informs the operator that the specified SMPP or UCP session is no longer operational. If this event was not expected, check the remote application and network for connectivity issues.

CS7TCAP Messages

Error Message

%CS7TCAP-5-CLRTCAP: TCAP stats cleared by [chars]

Explanation TCAP stats cleared.

Recommended Action No action is required.

CS7XUA Messages

Error Message

CS7XUA-3- IPADDRFAIL: IP Address Failed: IP Address [chars] Association [hex]
[chars] [chars]

Explanation : IP Address has failed.

Recommended Action No action is required.

Error Message

CS7XUA-3-ASSOCFAIL: Association [hex] for [chars] [chars] has failed, reason:
[chars]

Explanation Association has failed for given reason.

Recommended Action No action is required.

Error Message

CS7XUA-3-ASSOCTERMINATE: Association [hex] for [chars][chars] has terminated

Explanation Association has been terminated by the remote end.

Recommended Action No action is required.

Error Message

%CS7XUA-5-ASPSTATE: ASP [chars] is [chars] in AS [chars]

Explanation An ASP entered or exited active state in an AS.

Recommended Action No action is required.

Error Message

%CS7XUA-5-ASROUTESTATUS: Route [chars] in AS route [chars] is [chars]

Explanation An AS Route changed status.

Recommended Action No action is required.

Error Message

%CS7XUA-5-ASSTATE: AS [chars] is [chars]

Explanation An AS entered or exited active state.

Recommended Action No action is required.

Error Message

%CS7XUA-5-CLRASEVENT: AS event tables for [chars] cleared by [chars]

Explanation AS event tables cleared.

Recommended Action No action is required.

Error Message

%CS7XUA-5-CLRASPEVENT: ASP event tables for [chars] cleared by [chars]

Explanation ASP event tables cleared.

Recommended Action No action is required.

Error Message

%CS7XUA-5-CLRASPCSTAT: ASP statistic tables for [chars] cleared by [chars]

Explanation ASP statistic tables cleared.

Recommended Action No action is required.

Error Message

%CS7XUA-5-CLRASRTEVENT: AS route events for [chars] cleared by [chars]

Explanation AS route events cleared.

Recommended Action No action is required.

Error Message

%CS7XUA-5-CLRASRTSTAT: AS route statistic tables for [chars] cleared by [chars]

Explanation AS route statistic tables cleared.

Recommended Action No action is required.

Error Message

%CS7XUA-5-CLRASSTAT: AS statistic tables for [chars] cleared by [chars]

Explanation AS statistic tables cleared.

Recommended Action No action is required.

Error Message

%CS7XUA-5-CLRPCEVENTS: Point code events cleared by [chars]

Explanation Point code events cleared.

Recommended Action No action is required.

Error Message

%CS7XUA-5-CLRPCSTATS: Point code statistics cleared by [chars]

Explanation Point code statistics cleared.

Recommended Action No action is required.

Error Message

%CS7XUA-5-CLRSGMATESTAT: SG mate statistics cleared by [chars]

Explanation SG mate statistics cleared.

Recommended Action No action is required.

Error Message

%CS7XUA-3-ENQUEUEFAIL: Could not enqueue event to [chars] event queue.

Explanation An internal software error occurred.

Recommended Action This problem is due to an internal software error. If any of these messages recur, call your technical support representative for assistance.

Error Message

%CS7XUA-3-LISTFAIL: List [chars] operation failed for [chars]

Explanation A list operation failed, probably due to memory corruption

Recommended Action This problem is due to an internal software error. If this message persists, call your technical support representative for assistance.

Error Message

%CS7XUA-3-NOMEMORY: Insufficient memory for [chars]

Explanation The requested memory allocation failed because of a low memory condition

Recommended Action This problem is probably due to a lack of memory in the router. Either add more memory or reduce other system activity. If this message persists, call your technical support representative for assistance.

Error Message

%CS7XUA-3-NOPAKBUFFER: Could not get a [chars] packet buffer

Explanation Software failed to obtain a packet buffer from the global buffer pool

Recommended Action This problem is probably due to a lack of memory in the router. Either add more memory or reduce the number of CS7 interfaces. If this message persists, call your technical support representative for assistance.

Error Message

%CS7XUA-3-NOPROC: Could not create [chars] process

Explanation Insufficient internal resources available to create process.

Recommended Action This problem is due to an internal software error. Check available memory capacity on router. If any of these messages recur, call your technical support representative for assistance.

Error Message

%CS7XUA-3-NOTIMPLEMENTED: [chars] not implemented

Explanation The requested function is not implemented

Recommended Action This function is intended for a future release. Call your technical support representative for assistance.

Error Message

%CS7XUA-3-PROTOCOLERROR: [chars] error message with error code [chars] for ASP [chars]

Explanation A protocol error message was sent or received

Recommended Action This problem is due to an internal software error or an incompatibility with an M3UA or SUA peer. If this message persists, call your technical support representative for assistance.

Error Message

%CS7XUA-3-RTREEFAIL: Radix tree [chars] operation failed for [chars]

Explanation A radix tree operation failed, probably due to memory corruption

Recommended Action This problem is due to an internal software error. If this message persists, call your technical support representative for assistance.

Error Message

%CS7XUA-5-SCTPCONGESTABATE: [chars]([chars]) Level [dec] -> Level [dec]

Explanation An ASP or SG Mate has transitioned to a lower level of congestion.

Recommended Action No action is required.

Error Message

%CS7XUA-5-SCTPCONGESTONSET: [chars]([chars]) Level [dec] -> Level [dec]

Explanation An ASP or SG Mate has transitioned to a higher level of congestion.

Recommended Action No action is required.

Error Message

%CS7XUA-3-VARIABLEWRAP: [chars] wrapped

Explanation The value of a variable exceeded its maximum size

Recommended Action This problem is due to an internal software error. If this message persists, call your technical support representative for assistance.

Error Message

%CS7XUA-3-WAVLFAIL: AVL [chars] operation failed for [chars] [chars]

Explanation An AVL tree operation failed, probably due to memory corruption

Recommended Action This problem is due to an internal software error. If this message persists, call your technical support representative for assistance.

Error Message

%CS7XUA-5-XUAPCSSNSTATUS: XUA PC [chars] SSN [dec] is [chars]

Explanation An XUA PC/SSN combination changed status.

Recommended Action No action is required.

Error Message

%CS7XUA-5-XUAPCSTATUS: XUA PC [chars] is [chars]

Explanation An XUA PC or changed status.

Recommended Action No action is required.

DCS7 Messages

Error Message

%DCS7-3-DATAINCON: [chars] RC=[dec]. Configuration information is inconsistent with Route Processor on FlexWAN slot [dec]

Explanation Route Processor was unable to send configuration or status information update to the specified FlexWAN, due to an internal software error.

Recommended Action No action is required. The ITP will automatically perform error recovery and re-start the links on the FlexWAN. Issue CS7 show commands on the Route Processor to determine the current status.

Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message

%DCS7-3-DCS7BADXDRIPC: Invalid IPC/XDR. IPC len/XDRs len [dec]/[dec]. IPC at [hex]

Explanation An internal software error occurred.

Recommended Action Copy the message exactly as it appears, and report it your technical support representative.

Error Message

%DCS7-3-DCS7BADXDRTYPE: Invalid XDR type. Type [dec]. XDR at [hex]

Explanation An internal software error occurred.

Recommended Action Copy the message exactly as it appears, and report it your technical support representative.

Error Message

%DCS7-3-DCS7DISABLE: Fatal error, slot [dec]: [chars] RC=[dec]

Explanation An internal software error has occurred because of an IPC problem between the LC and the RP.

Recommended Action No action is required. The ITP will automatically perform error recovery and re-start the links on the FlexWAN. Issue CS7 show commands on the Route Processor to determine the current status.

Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message

%DCS7-3-DCS7IPCERR: IPC error: [chars] [dec] [hex]

Explanation CS7 encountered an error with the IPC component for the specified slot. This may cause the configuration and status on the FlexWAN to be inconsistent with the Route Processor. This is an internal software error.

Recommended Action No action is required. The ITP will automatically perform error recovery and re-start the links on the FlexWAN. Issue CS7 show commands on the Route Processor to determine the current status.

Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message

%DCS7-4-DCS7MSG: Invalid message received. Type [dec], field [chars], value [hex], length [dec]

Explanation An internal software error occurred.

Recommended Action Copy the message exactly as it appears, and report it to your technical support representative.

Error Message

%DCS7-2-DCS7_OVERLENGTH_XDR: Overlength DCS7 XDR message - len [dec] > [dec] from [chars]

Explanation An internal software error occurred preventing the sending of an DCS7 XDR message.

Recommended Action Copy the message exactly as it appears, and report it to your technical support representative.

Error Message

%DCS7-1-DCS7PERMMDIS: MTP3 offload has been permanently disabled on FlexWAN [dec]

Explanation CS7 has exhausted all error recovery procedures on the specified FlexWAN. All MTP3 links on the FlexWAN have been shut down.

Recommended Action Investigate the cause of errors and correct them if possible. To re-enable the links and MTP3 offload on the FlexWAN, issue the **cs7 offload mtp3 slot restart** command. Inform your support representative of this occurrence.

Error Message

%DCS7-4-DCS7RATE: [chars] rate limit status [dec]

Explanation An internal software error occurred.

Recommended Action Copy the message exactly as it appears, and report it to your technical support representative.

Error Message

%DCS7-1-DCS7RELDFlexWAN: CS7 is reloading microcode on FlexWAN in slot [dec].
Reason: [chars]

Explanation If the reason is fatal errors, it means CS7 has exhausted all error recovery procedures on the specified FlexWAN. The IOS image will be reloaded on the FlexWAN by simulating an OIR remove and insert.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Research and attempt to resolve the error using the Output Interpreter <https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl>. Also perform a search of the Bug Toolkit <http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl>. If you still require assistance, open a case with the Technical Assistance Center via the Internet http://www.cisco.com/cgi-bin/front.x/case_tools/caseOpen.pl, or contact your Cisco technical support representative and provide the representative with the gathered information.

Error Message

%DCS7-4-DCS7RESTART: Restarting MTP3 offload on FlexWAN [dec] due to fatal error

Explanation MTP3 offload has been restarted on the FlexWAN due to a fatal error reported in an earlier error message. All links on the FlexWAN will be shut and re-started after the CS7 configuration has been downloaded to the FlexWAN.

Recommended Action Issue CS7 show commands on the Route Processor to determine the current status. Inform your support representative of this occurrence.

Error Message

%DCS7-3-DCS7SEQ: Out of sequence. State [dec] Rcvd [dec]

Explanation The line card has received an out-of-sequence IPC from the RP.

Recommended Action Copy the message exactly as it appears, and report it to your technical support representative.

Error Message

%DCS7-1-DCS7SYNC: MTP3 offload configuration is incorrect on FlexWAN in slot [dec]

Explanation CS7 has detected a loss of MTP3 configuration or status update message on the specified FlexWAN. This indicates that the MTP3 data on the FlexWAN (for example, route, link, linkset) is inconsistent with the master copy on the Route Processor.

Recommended Action No action is required. The ITP will automatically perform error recovery and re-start the links on the FlexWAN. Issue CS7 show commands on the Route Processor to determine the current status.

Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message

%DCS7-3-DCS7XDRLEN: Invalid XDR length. Type [dec][chars]. XDR/buffer len [dec]/[dec]

Explanation An internal software error occurred.

Recommended Action Copy the message exactly as it appears, and report it your technical support representative.

Error Message

%DCS7-5-INFO: [chars] [dec] [hex] [hex]

Explanation This is an informational message. If it occurs frequently, it can indicate a problem.

Recommended Action Monitor the system resources and status. If the message appears frequently, copy the message exactly as it appears, and report it your technical support representative.

Error Message

%DCS7-5-INFOG: [chars] [dec] [hex] [hex]

Explanation This is an informational message. If it occurs frequently, it can indicate a problem.

Recommended Action Monitor the system resources and status. If the message appears frequently, copy the message exactly as it appears, and report it your technical support representative.

Error Message

%DCS7-3-INTERR: Internal error - [chars] [dec] [hex]

Explanation An internal software error occurred.

Recommended Action No action is required. The ITP will automatically perform error recovery and re-start the links on the FlexWAN. Issue CS7 show commands on the Route Processor to determine the current status.

Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message

%DCS7-3-INTERRF: Internal error - [chars] [dec] [hex]

Explanation An internal software error occurred.

Recommended Action No action is required. The ITP will automatically perform error recovery and re-start the links on the FlexWAN. Issue CS7 show commands on the Route Processor to determine the current status. Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message

%DCS7-3-INTERRG: Internal error - [chars] [dec] [hex]

Explanation An internal software error occurred.

Recommended Action No action is required. The ITP will automatically perform error recovery and re-start the links on the FlexWAN. Issue CS7 show commands on the Route Processor to determine the current status. Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message

%DCS7-3-INTERRM: Internal error - [chars] [dec] [hex]

Explanation An internal software error occurred.

Recommended Action No action is required. The ITP will automatically perform error recovery and re-start the links on the FlexWAN. Issue CS7 show commands on the Route Processor to determine the current status. Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message

%DCS7-3-INVALIDSTATE: Internal state error [chars] Slot [dec] Flags [hex]

Explanation An internal software error occurred. Linecard is in incorrect state

Recommended Action Copy the message exactly as it appears, and report it to your technical support representative.

Error Message

%DCS7-2-LCINITFAIL: Linecard could not initialize DCS7 forwarding

Explanation Initialization of the line card for distributed CS7 failed. This is most likely due to insufficient memory on the line card.

Recommended Action Reduce other system activity to ease memory demands. If conditions warrant, upgrade to a larger memory configuration.

Error Message

%DCS7-5-MTP3OFFLDBEG: MTP3 offload activation on FlexWAN slot [dec] is in progress

Explanation MTP3 offload has been enabled on the FlexWAN.

Recommended Action No action is required.

Error Message

%DCS7-6-MTP3OFFLDRESP: MTP3 offload has been [chars] on FlexWAN slot [dec].
[chars]

Explanation MTP3 offload has been enabled on the FlexWAN.

Recommended Action No action is required.

Error Message

%DCS7-2-NODEST: An internal software error occurred.

Explanation An internal software error occurred.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Research and attempt to resolve the error using the Output Interpreter <https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl>. Also perform a search of the Bug Toolkit <http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl>. If you still require assistance, open a case with the Technical Assistance Center via the Internet http://www.cisco.com/cgi-bin/front.x/case_tools/caseOpen.pl, or contact your Cisco technical support representative and provide the representative with the gathered information.

Error Message

%DCS7-2-NOHWIDB: An internal software error occurred.

Explanation An internal software error occurred.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Research and attempt to resolve the error using the Output Interpreter <https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl>. Also perform a search of the Bug Toolkit <http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl>. If you still require assistance, open a case with the Technical Assistance Center via the Internet http://www.cisco.com/cgi-bin/front.x/case_tools/caseOpen.pl, or contact your Cisco technical support representative and provide the representative with the gathered information.

Error Message

%DCS7-3-NOMEM: Malloc Failure. [chars]

Explanation A memory shortage has caused an internal software error.

Recommended Action Copy the message exactly as it appears, and report it to your technical support representative.

Error Message

%DCS7-2-NOROUTE: An internal software error occurred.

Explanation An internal software error occurred.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Research and attempt to resolve the error using the Output Interpreter <https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl>. Also perform a search of the Bug Toolkit <http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl>. If you still require assistance, open a case with the Technical Assistance Center via the Internet http://www.cisco.com/cgi-bin/front.x/case_tools/caseOpen.pl, or contact your Cisco technical support representative and provide the representative with the gathered information.

Error Message

%DCS7-2-NOROUTETABLE: An internal software error occurred.

Explanation An internal software error occurred.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Research and attempt to resolve the error using the Output Interpreter <https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl>. Also perform a search of the Bug Toolkit <http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl>. If you still require assistance, open a case with the Technical Assistance Center via the Internet http://www.cisco.com/cgi-bin/front.x/case_tools/caseOpen.pl, or contact your Cisco technical support representative and provide the representative with the gathered information.

Error Message

%DCS7-3-OFFLDNOACK: [chars] MTP3 offload command acknowledgement not received from FlexWAN [dec]

Explanation An enable/disable MTP3 offload command was not acknowledged by the specified FlexWAN. The system will resend the command. The FlexWAN offload operation may not be operating as expected.

Recommended Action Issue CS7 show commands to determine the status. If condition is unacceptable, issue the **cs7 offload mtp3 slot restart** command. Inform your support representative of this occurrence

Error Message

%DCS7-3-OOSEQ: Sequence error encountered on Slot [dec] - FlexWAN Expected [dec], received [dec]

Explanation The CS7 software on the FlexWAN encountered loss of message(s) from the Route Processor. This indicates the configuration and status on the FlexWAN may be out of sync with that on the Route Processor. The configuration will be reloaded on the FlexWAN.

Recommended Action No action is required. The ITP will automatically perform error recovery and re-start the links on the FlexWAN. Issue CS7 show commands on the Route Processor to determine the current status. Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message

%DCS7-3-Route ProcessorIPCERR: IPC error. [chars] RC = [hex]

Explanation CS7 encountered an error with the IPC component on the Route Processor. This will prevent exchange of configuration and status information between the Route Processor and the FlexWAN. This is an internal software error.

Recommended Action No action is required. The ITP will automatically perform error recovery and re-start the links on the FlexWAN. Issue CS7 show commands on the Route Processor to determine the current status. Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message

%DCS7-5-SLMOFFLDALL: SLM offload [chars] on all FlexWAN's is in progress

Explanation SLM offload has been enabled or disabled on all the FlexWAN's.

Recommended Action No action is required.

Error Message

%DCS7-1-SLMOFFLDFlexWAN: SLM offload has been [chars] on FlexWAN slot [dec]. [chars]

Explanation SLM offload has been enabled or disabled on the FlexWAN.

Recommended Action No action is required.

Error Message

%DCS7-3-FlexWANERR: [chars]. FlexWAN in slot [dec]

Explanation CS7 encountered an abnormal error related to the specified FlexWAN. This will prevent exchange of configuration and status information between the Route Processor and the FlexWAN. This is an internal software error.

Recommended Action No action is required. The ITP will automatically perform error recovery and re-start the links on the FlexWAN. Issue CS7 show commands on the Route Processor to determine the current status. Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message

%DCS7-2-XDRINIT: Error initializing DCS7 xdr chunks

Explanation Initialization of the DCS7 xdr chunks could not be accomplished because of a low memory condition.

Recommended Action Reduce other system activity to ease memory demands. If conditions warrant, upgrade to a larger memory configuration.

