



IP Transfer Point on the Cisco 7600 Platform

IOS Release 12.2(18)IXD
April 19, 2007

EDCS-589347

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 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.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0612R)

IP Transfer Point

Copyright © 2007, Cisco Systems, Inc.

All rights reserved.



CONTENTS

About this Book	29
Audience	29
Documentation Organization	30
Documentation Conventions	31
Obtaining Documentation	33
Cisco.com	33
Product Documentation DVD	33
Ordering Documentation	33
Documentation Feedback	33
Cisco Product Security Overview	34
Reporting Security Problems in Cisco Products	34
Obtaining Technical Assistance	35
Cisco Technical Support & Documentation Website	35
Submitting a Service Request	36
Definitions of Service Request Severity	36
Obtaining Additional Publications and Information	36
Using Cisco IOS Software	39
Understanding Command Modes	39
Getting Help	40
Example: How to Find Command Options	41
Using the no and default Forms of Commands	43
Filtering Output from the show and more Commands	44
Finding Additional Feature Support Information	44
Overview of ITP	45
SS7oIP Technology Overview	45
Introduction to SS7oIP	45
Stream Control Transmission Protocol (RFC2960)	45
Sigtran M2PA - SS7 MTP2-User Peer-to-Peer Adaptation Layer	46
Sigtran M3UA - SS7 MTP3-User Adaptation Layer	46

Sigtran SUA - SS7 SCCP-User Adaptation Layer	47
Benefits	48

Planning to Configure ITP	49
Supported Platforms	49
Restrictions	49
Supported Standards, MIBs, and RFCs	49
Standards	49
MIBs	50

ITP Non-Disruptive Upgrade on the Cisco 7600 Platform 53

Contents	53
Prerequisites for Non-Disruptive Upgrade	53
Information About Non-Disruptive Upgrade	54
Performing a Non-Disruptive Upgrade	54
Preparing for Non-Disruptive Upgrade	54
SUMMARY STEPS	55
DETAILED STEPS	55
What to Do Next	56
Resetting the Standby Supervisor	57
SUMMARY STEPS	57
DETAILED STEPS	57
What to Do Next	57
Switching the Standby Supervisor to Active Role	58
SUMMARY STEPS	58
DETAILED STEPS	58
What to Do Next	58
Upgrading the Software Image on FlexWAN Line Cards	59
SUMMARY STEPS	59
DETAILED STEPS	59
What to Do Next	59
Upgrading the Software Image on the Standby Supervisor	59
SUMMARY STEPS	59
DETAILED STEPS	60

61

Configuring ITP Basic Functionality 63

Contents	65
Configuring Redundancy and Stateful Switchover (SSO)	65
SUMMARY STEPS	65
DETAILED STEPS	66
Copying an Image onto an RSP	67

SUMMARY STEPS	67
DETAILED STEPS	67
Configuring RPR+	69
SUMMARY STEPS	69
DETAILED STEPS	69
SUMMARY STEPS	70
DETAILED STEPS	71
Setting the Config-Register Boot Variable	71
SUMMARY STEPS	71
DETAILED STEPS	72
Enabling Secure Shell	73
SUMMARY STEPS	73
Specifying the SS7 Variant, National Option, and Network Indicator	75
SUMMARY STEPS	75
Specifying the Point Code	76
Specifying the Point Code Representation	76
Specifying the Primary Local Point Code	77
Specifying a Secondary Point Code	78
Specifying the Capability Point Code	78
Specifying the Interface and Encapsulation	79
A Note About Clocking on the SS7 Port Adapter and SS7 Q.703 High Speed Port Adapter	79
Configuring a Serial Interface and SS7 High-Speed MTP2 Encapsulation (Q.703 Annex A) on the SS7 Q.703 High Speed Port Adapter	80
Configuring a Serial Interface and MTP2 Encapsulation on the SS7 Port Adapter	81
Configuring SS7 over ATM High Speed Links (HSL)	83
Enabling an ATM Interface	84
Enabling an OC3 ATM Interface	84
Configuring a Permanent Virtual Circuit (PVC)	85
Configuring BITS Network Clocking	85
Configuring SS7 ATM High Speed Links with BITS Network Clocking	86
Configuring the Clock Source for the Cisco 2811 Router	90
Configuring the Clock-Source	90
SUMMARY STEPS	90
DETAILED STEPS	90
Examples	92
Configuring Local Peers	92
Configuring Linksets	93
Configuring Multiple Linksets to Adjacent Nodes	94
Specifying the Cisco ITP Route Table	95
Specifying the Default Route Table	95
Loading the Route Table Contents	95
Adding Routes to the Route Table	96
Saving the Route Table	96

Assigning Links to Linksets	96
Traditional SS7 Links	97
High-Speed Signaling Links	97
SS7 Over IP Links (Peers)	97
Shutting Down and Restarting Linksets and Links	98
Configuration Example of RPR+	99
Configuration Example of ITP Basic Functionality	101

Multiple Instances and Instance Translation 111

Contents	111
Information About Multiple Instances and Instance Translation	112
Understanding Virtual Linksets	112
How to Configure Multiple Instances	113
How to Configure Instance Translation	114
Configuring Point Code Conversion	114
Configuring Global Title Conversion	115
Overview of Global Title Conversion	115
Creating a GTI Conversion Table	116
Creating a Subsystem Mapping Table	116
Creating a GTA Prefix Conversion Table	117
Assigning a Conversion Table to an Instance	117
Configuring Instance Conversion After Global Title Translation	118
Verifying the Multiple Instances Configuration	119
Configuration Example for Multiple Instance	119
Configuration Examples for Instance Translation	120

Global Title Translation 123

Contents	123
Overview of GTT Components	124
GTT Selectors	124
GTT Global Title Address Entries	125
GTT Application Groups	126
GTT Mated Application Entries	127
Storing and Loading GTT Configuration Data	127
Loading a GTT Table from a Remote File Server or Flash (No existing GTT Data)	128
Loading a GTT Table from a Remote File Server or Flash (Existing GTT Data)	129
Bulk Loading/Replacing GTT Database	129
Syntax and Format Rules for Creating a GTT Database Download File	129
Command Identifiers in a GTT Database Download File	130
Parameter Values in GTT Database Download Files	130

Examples of Entries in a GTT Database Download File	132
Displaying Current GTT Configuration	135
Configuring GTT: 6 Scenarios	136
Configuring Intermediate GTT To Route MSUs to a Single Point Code	136
Provisioning the ITP	137
Configuring the ITP GTT Database	137
Configuring Intermediate GTT To Load Balance MSUs Across Two Or More Point Codes	139
Provisioning the ITP	139
Configuring the ITP GTT Database	140
Configuring Final GTT To Route MSUs to a Solitary Point Code	142
Provisioning the ITP	142
Configuring the ITP GTT Database	142
Configuring Final GTT To Route MSUs to a Primary and Backup Point Code and SSN (Dominant Mode)	145
Provisioning the ITP	145
Configuring the ITP GTT Database	146
Configuring Final GTT To Load Balance MSUs Across a Group of Point Codes and Subsystems	148
Provisioning the ITP	148
Configuring the ITP GTT	149
Configuring Final GTT to an SUA AS with a Backup Point Code (Dominant Mode)	151
Provisioning the ITP	151
Configuring the ITP GTT	152
Configuring Global Title Address Conversion	154
Verifying Global Title Translations	155
GTT Measurements	155
SCCP Accounting	156
Subsystem Status	156
Logging GTT Errors with the ITP Logging Facility	157
GTT Error Log	158
Configuration Example for GTT	160
M3UA and SUA SS7 Over IP Signaling Gateways	171
Contents	171
Information About M3UA and SUA ITP Signaling Gateways	172
M3UA	172
SUA	173
SGMP and Mated SGs	174
C-Link Backup Routing of M3UA/SUA Traffic	175
C-link Route Availability	176
AS Point Code Availability	176
ASP Bindings	176
Application Server (AS)	176

Application Server Process (ASP)	176
Point Code Assignment and Management	176
AS Load-sharing Support	177
AS Fail-over support	178
SCCP Traffic Processing for M3UA	178
ITP SG Quality Of Service (QoS)	179
How to Configure Signaling Gateways	179
Performing Basic ITP Configuration	179
Enabling and Disabling M3UA or SUA on the ITP SG	180
Enabling M3UA	180
Disabling M3UA	180
Enabling SUA	180
Disabling SUA	181
Defining an SG Mated Pair	181
Disabling M3UA	181
Enabling SUA and SUA SCTP Offload	181
Defining an Application Server Process (ASP)	182
Defining Application Servers (AS) and Routing Keys	184
Enabling M3UA Extended User Part Unavailable (UPU) Operation	185
ITP Signaling Gateway Configuration Examples	185
M3UA Configuration Example	186
SUA Configuration Example	186
ITP Signaling Gateway: ASPs with Unique Point Codes Configuration Example	187
ITP SG Mated-SG Configuration Example	188
ITP SG GTT Configuration Example	190
ITP SG QoS Configuration Examples	191
Example 1	191
Example 2	191
Example 3	192
Example 4	192
Gateway Screening (GWS)	195
Contents	196
Information About GWS	196
GWS Tables	196
GWS Table Matching Order for Incoming Packets	207
How GWS Works with Access Lists	207
How to Configure GWS	210
Configuring Basic GWS with Access Lists	210
SUMMARY STEPS	210
DETAILED STEPS	211

What to Do Next	211
Configuring Enhanced GWS	212
212	
SUMMARY STEPS	212
DETAILED STEPS	212
Defining GWS Action Sets	212
SUMMARY STEPS	212
DETAILED STEPS	212
What to Do Next	214
Defining GWS Tables	214
SUMMARY STEPS	214
DETAILED STEPS	215
What to Do Next	216
Defining Entries in GWS Tables	216
What to Do Next	218
Defining Gateway Linkset Tables	219
SUMMARY STEPS	219
DETAILED STEPS	220
What to Do Next	221
Defining an AS Table for GWS	221
SUMMARY STEPS	221
DETAILED STEPS	222
What to Do Next	223
Monitoring GWS	223
Message Logging	223
SUMMARY STEPS	224
DETAILED STEPS	224
SUMMARY STEPS	224
DETAILED STEPS	225
Verifying GWS Configuration	226
SUMMARY STEPS	226
DETAILED STEPS	226
Configuration Examples for GWS	227
GWS Scenario: Linkset with Allowed DPC	227
GWS Scenario: XUA AS with Allowed DPC	228
GWS Scenario with CgPA, CdPA	229
Additional References	230
Standards	230
MLR Routing and Screening	231
Contents	232
Information About MLR Routing and Screening	232
Trigger Search Order	233

Destination Selection	233
How to Configure MLR-Based Routing	234
Define MLR Global Options	234
SUMMARY STEPS	234
DETAILED STEPS	235
Define the MLR Group	235
SUMMARY STEPS	236
DETAILED STEPS	236
Defining the MLR Modify-Profile	238
SUMMARY STEPS	239
DETAILED STEPS	239
Creating and Managing Address Tables	242
Creating and Loading an Address Table File Using the CLI	242
SUMMARY STEPS	242
DETAILED STEPS	242
Creating and Loading a Stored Address Table File	245
SUMMARY STEPS	247
DETAILED STEPS	247
Replacing an Address Table File	248
SUMMARY STEPS	248
DETAILED STEPS	249
Examples	249
Define One or More Multi-layer SMS Rulesets	250
SUMMARY STEPS	254
DETAILED STEPS	255
Define the MLR Triggers	266
Define the MLR Triggers with GWS	266
Information About MLR Triggers with GWS	266
Migration of Existing MLR Trigger Configuration	266
Disabling of MLR Triggers	266
MLR and GWS Table Matching Order for Incoming Packets	267
Precedence Followed for Link Set or AS	267
Precedence Followed for a Local Application	267
How MLR Using GWS Works with Access Lists	267
Define MLR Triggers with Proprietary Method	267
SUMMARY STEPS	268
DETAILED STEPS	268
How to Configure MLR-Based Screening	269
Blocking Based on SCCP cdPa and cgPa	270
Define GTT Entries for cdPa and cgPa digits to Screen	270
SUMMARY STEPS	270
DETAILED STEPS	270
Define MLR table and Blocking Based on SCCP cdPa or cgPa	271
Define MLR Table and Blocking on Combination of SCCP cdPa and cgPa	272

Blocking Based on cgPa, cdPa, and SMS MAP Operation Code	272
Blocking Based on cgPa, cdPa and SMS MO/MT Routing Parameters	272
Verifying and Monitoring Multi Layer SMS Routing	274
Configuration Examples of Multi-layer SMS Routing	276
Configuration Example for Multi-Layer Routing: ITP Receives All SMS-MO Traffic in GT-Routed Network	277
Configuration Example for Multi-Layer Routing: Legacy SMSC Retains Point Code in PC-Routed Network	279
Configuration Example for Multi-Layer Routing: MLR Distribution to MTP3-Based SMSCs	282
Examples of Configuring Routing based on Operation types	283
Example of Routing with B-Address Binding	284
Configuration Example of Address Modification	285
MTP3 Offload	287
Contents	287
Restrictions for MTP3 Offload	287
Information About MTP3 Offload	288
How to Configure MTP3 Offload	288
Verifying MTP3 Offload	288
	288
ITP Non-Stop Operation (NSO)	289
Contents	289
Restrictions for ITP NSO	290
Information About ITP NSO	290
How to Configure ITP NSO	290
Configuring M2PA Offload	290
M2PA Offload	290
SUMMARY STEPS	290
DETAILED STEPS	291
What to Do Next	291
Configuring xUA SCTP Offload	291
xUA SCTP Offload	291
SUMMARY STEPS	291
DETAILED STEPS	292
What to Do Next	292
Configuring Stateful Switchover Redundancy Mode	292
SUMMARY STEPS	292
DETAILED STEPS	293
What to Do Next	293
Enabling ITP NSO	293
SUMMARY STEPS	293

	DETAILED STEPS	294
	What to Do Next	294
Monitoring NSO		294
	SUMMARY STEPS	294
	DETAILED STEPS	294
Configuration Example for ITP NSO		294
ITP QoS		297
Contents		297
Information About ITP QoS		297
	ITP QoS Components	298
	ITP QoS Functionality	298
How to Configure ITP QoS		299
	Specifying Packet Classification	300
	Specifying Input Linkset Classification	300
	Specifying Access List Classification	301
	Specifying Service Indicator Classification	302
	Specifying SCCP Packet Classification	303
	Specifying Destination Point Code Classification	305
	Specifying a QoS classification for an ASP	306
	Specifying QoS Routing Over M2PA Links	307
Verifying ITP QoS		307
QoS Configuration Example		308
	Example 1	322
	Example 2	322
	Example 3	322
	Example 4	323
Load Sharing		325
Contents		325
How to Configure MTP3 Load Sharing		325
	How to Configure MTP3 Enhanced Load Sharing For ITU	326
	SUMMARY STEPS	326
Information About SCCP Load Sharing		327
How to Configure SCCP Load Sharing		328
	How to Configure SCCP Load Sharing to Ignore Class and Sequencing	331
	SUMMARY STEPS	331
	DETAILED STEPS	331
	Example	331
Summary Routing and ANSI Cluster Routing		333
Contents		333
Information About Summary Routing and ANSI Cluster Routing		333

How Point Codes Are Used in Summary Routing	334
Assigning Point Codes	334
Specifying Summary Destinations	335
Summary Routes and the Routing Table	335
How to Configure Summary Routes	336
How to Configure ANSI Cluster Routing	338
Verifying, Monitoring, and Tuning the ITP	341
Verifying ITP	341
Monitoring ITP	352
Configuring ITP for Event Logging to an External Server	352
Enabling Simple Network Management Protocol	353
Monitoring the Cisco ITP	354
Monitoring CPU/Memory	355
Monitoring Linksets and Links	356
Monitoring MTP2 Links/Interfaces	357
Monitoring M2PA Links/Interfaces	362
Monitoring GTT Measurements	366
Monitoring M3UA or SUA	366
Monitoring M3UA	367
Monitoring SUA	367
Monitoring Point Code Status	367
Monitoring AS, ASP, Mated-SG	368
Monitoring AS	368
Monitoring ASP	369
Monitoring SGMP and Mated SG Pairs	371
Monitoring AS Route Table	372
Monitoring Routes	373
Monitoring Gateway Screening Violations	374
Monitoring System Messages	374
Monitoring Accounting	375
Summary of Commands to Monitor Cisco ITP	375
Tuning ITP	377
Tuning HSL Parameters	377
Create a Profile to Support HSL	377
Specify HSL Parameters on a Link	379
Tuning MTP3 Timers	380
Tuning MTP2 Parameters	380
Understanding the MTP2 Parameters	380
Specifying MTP2 Parameters in a CS7 Profile	382
Specifying MTP2 Parameters Individually	383

Tuning SCTP Parameters	384
How SCTP Parameters Work	384
Tuning SCTP Parameters for M2PA	387
Tuning SCTP Parameters for M3UA, SGMP, and SUA	388
Tuning SCTP Parameters for an ASP	389
Tuning AS Options	389
Tuning SCTP Parameters for a Mated SG	390
Tuning SCTP Parameters for Satellite Channels	391
Overview of SCTP and Satellite Channels	391
Tuning SCTP on Satellite Channels	392
Verifying SCTP Parameters on Satellite Channels	394

ITP Command Set: A - D 395

access-group	400
access-list	401
accounting	404
active-asps-target	405
addr (cs7 mlr address-table)	406
adjacent-sp-restart	408
allow-multi-message-dialogue	409
asname (cs7 gtt application group)	410
asname (cs7 mlr result)	412
asp	414
assoc-retransmit (cs7 asp)	416
assoc-retransmit (cs7 link)	417
assoc-retransmit (cs7 m2pa profile)	418
assoc-retransmit (cs7 m3ua)	419
assoc-retransmit (cs7 mated-sg)	420
assoc-retransmit (cs7 sgmp)	421
assoc-retransmit (cs7 sua)	422
atm nni	423
block	424
broadcast	425
bundling (cs7 asp)	427
bundling (CS7 Link)	428
bundling (cs7 m2pa profile)	430
bundling (cs7 m3ua)	432
bundling (cs7 mated-sg)	433

bundling (cs7 profile) 434
 bundling (cs7 sgmp) 436
 bundling (cs7 sua) 437
 burst-recovery-timeout 438
 cdpa (cs7 mlr table trigger) 439
 cgpa (cs7 mlr modify-profile) 442
 cgpa (cs7 mlr table trigger) 444
 clear cs7 accounting 447
 clear cs7 all 448
 clear cs7 as 449
 clear cs7 asp 450
 clear cs7 dynamic-route 451
 clear cs7 gtt-meas 452
 clear cs7 mated-sg statistics 453
 clear cs7 mtp3 event-history 454
 clear cs7 pointcode event-history 455
 clear cs7 statistics 456
 clear cs7 tcap statistics 458
 clock source (controller) 459
 clock source (interface) 461
 cs7 accounting 463
 cs7 address-table replace 464
 cs7 as 465
 cs7 asp 467
 cs7 capability-pc 469
 cs7 cli 471
 cs7 description 472
 cs7 display-name 473
 cs7 distribute-sccp-sequenced 474
 cs7 distribute-sccp-unsequenced 475
 cs7 fast-restart 476
 cs7 gtt address-conversion 477
 cs7 gtt application-group 478
 cs7 gtt concern-pclist 479
 cs7 gtt load 481

cs7 gtt map 482
 cs7 gtt map sp 485
 cs7 gtt map ss 486
 cs7 gtt replace-db 488
 cs7 gtt selector 489
 cs7 gws action-set 491
 cs7 gws as 493
 cs7 gws linkset 494
 cs7 gws table 495
 cs7 host 497
 cs7 inhibit 499
 cs7 instance pc-conversion 500
 cs7 instance pc-conversion default 501
 cs7 linkset 503
 cs7 local-peer 505
 cs7 local-sccp-addr-ind 507
 cs7 log 509
 cs7 log checkpoint 511
 cs7 m3ua 512
 cs7 m3ua extended-upu 514
 cs7 mated-sg 515
 cs7 max-dynamic-routes 517
 cs7 mlr address-table 518
 cs7 mlr modify-profile 519
 cs7 mlr options 520
 cs7 mlr result 521
 cs7 mlr ruleset 524
 cs7 mlr table 526
 cs7 msu-rates notification-interval 528
 cs7 msu-rates sample-interval 529
 cs7 msu-rates threshold-default 530
 cs7 msu-rates threshold-proc 532
 cs7 mtp3 event-history 534
 cs7 mtp3 timer 536
 cs7 mtp3 tuning 541

cs7 multi-instance 543
cs7 national-options 544
cs7 network-indicator 546
cs7 network-name 547
cs7 nso 548
cs7 paklog 549
cs7 point-code 551
cs7 point-code delimiter 552
cs7 point-code format 553
cs7 profile 555
cs7 prompt enhanced 557
cs7 qos class 558
cs7 remote-congestion-msgs 559
cs7 route-mgmt-sls 560
cs7 route-table 562
cs7 save address-table 563
cs7 save gtt-table 564
cs7 save log 565
cs7 save route-table 567
cs7 sccp gti-conversion 568
cs7 sccp instance-conversion 569
cs7 sccp ssn-conversion 571
cs7 secondary-pc 572
cs7 sg-event-history 573
cs7 sgmp 574
cs7 sls-shift 576
cs7 snmp dest-max-window 577
cs7 snmp mgmt-max-window 578
cs7 sua 579
cs7 sua-allow-xudt-request 581
cs7 summary-routing-exception 582
cs7 tcap tid-timer 583
cs7 tcap variant 584
cs7 tfc-pacing-ratio 585
cs7 uninhibit 586

- cs7 upgrade analysis 587
- cs7 upgrade module 590
- cs7 util-abate 591
- cs7 util-plan-capacity 592
- cs7 util-sample-interval 593
- cs7 util-threshold 594
- cs7 variant 595
- cs7 xua-as-based-congestion 597
- cs7 xua-ssnm-filtering 598
- cs7 xua-tfc-allowed 599
- cumulative-sack (CS7 ASP) 600
- cumulative-sack (CS7 Link) 601
- cumulative-sack (cs7 m2pa profile) 602
- cumulative-sack (CS7 M3UA) 603
- cumulative-sack (cs7 mated-sg) 604
- cumulative-sack (CS7 SGMP) 605
- cumulative-sack (cs7 sua) 606
- default 607
- default result 609
- description (cs7 link) 610
- description (cs7 linkset) 611
- dest-port (cs7 mlr ruleset rule) 612
- dest-sme (cs7 mlr ruleset rule) 613
- dest-sme-table (cs7 mlr ruleset rule) 616
- dest-smisc (cs7 mlr ruleset rule) 618
- display-name (cs7 link) 620
- display-name (cs7 linkset) 621

ITP Command Set: E - R 623

- encapsulation hs-mtp2 628
- encapsulation mtp2 629
- false-congestion 630
- fast-cwnd-rate (cs7 asp) 631
- fast-cwnd-rate (cs7 link) 632
- fast-cwnd-rate (cs7 m2pa profile) 633
- fast-cwnd-rate (cs7 m3ua) 635

[fast-cwnd-rate \(cs7 mated-sg\)](#) **636**
[fast-cwnd-rate \(cs7 sgmp\)](#) **637**
[fast-cwnd-rate \(cs7 sua\)](#) **638**
[gt \(cs7 mlr result\)](#) **639**
[gta app-grp](#) **641**
[gta asname](#) **642**
[gta pcssn](#) **644**
[gta -prefix](#) **646**
[gta qos-class](#) **648**
[gta-start](#) **650**
[gtt-accounting](#) **651**
[hold-transport \(cs7 link\)](#) **652**
[hold-transport \(cs7 m2pa profile\)](#) **653**
[hs-mtp2](#) **654**
[hs-mtp2-timer \(cs7 link\)](#) **655**
[hsl](#) **657**
[idle-cwnd-rate \(cs7 asp\)](#) **658**
[idle-cwnd-rate \(cs7 link\)](#) **659**
[idle-cwnd-rate \(cs7 mated-sg\)](#) **660**
[idle-cwnd-rate \(cs7 m2pa profile\)](#) **661**
[idle-cwnd-rate \(cs7 m3ua\)](#) **663**
[idle-cwnd-rate \(cs7 sgmp\)](#) **664**
[idle-cwnd-rate \(cs7 sua\)](#) **665**
[inbound \(config-gws-as\)](#) **666**
[inbound \(config-gws-ls\)](#) **668**
[init-cwnd-size \(cs7 asp\)](#) **670**
[init-cwnd-size \(cs7 link\)](#) **671**
[init-cwnd-size \(cs7 m2pa profile\)](#) **672**
[init-cwnd-size \(cs7 m3ua\)](#) **674**
[init-cwnd-size \(cs7 mated-sg\)](#) **675**
[init-cwnd-size \(cs7 sgmp\)](#) **676**
[init-cwnd-size \(cs7 sua\)](#) **677**
[init-ip-dscp](#) **678**
[init-ip-precedence](#) **679**
[init-retransmit \(cs7 link\)](#) **680**

[init-retransmit \(cs7 m2pa profile\)](#) **681**
[init-retransmit \(cs7 m3ua\)](#) **682**
[init-retransmit \(cs7 sgmp\)](#) **683**
[init-retransmit \(CS7 SUA\)](#) **684**
[init-timeout \(CS7 Link\)](#) **685**
[init-timeout \(cs7 m2pa profile\)](#) **686**
[init-timeout \(CS7 M3UA\)](#) **687**
[init-timeout \(CS7 SGMP\)](#) **688**
[init-timeout \(CS7 SUA\)](#) **689**
[insert-dpc-in-cdpa](#) **690**
[ip-dscp \(cs7 m2pa profile\)](#) **692**
[ip-precedence \(CS7 Link\)](#) **693**
[ip-precedence \(cs7 m2pa profile\)](#) **694**
[isup-msg-type](#) **695**
[keepalive \(CS7 ASP\)](#) **697**
[keepalive \(CS7 Link\)](#) **698**
[keepalive \(cs7 m2pa profile\)](#) **699**
[keepalive \(CS7 M3UA\)](#) **700**
[keepalive \(CS7 Mated-SG\)](#) **701**
[keepalive \(CS7 SGMP\)](#) **702**
[keepalive \(CS7 SUA\)](#) **703**
[linestate debounce](#) **704**
[link \(CS7 linkset\)](#) **705**
[link-test](#) **708**
[link-timer](#) **709**
[load \(cs7 route table\)](#) **712**
[local-ip \(CS7 local peer\)](#) **714**
[local-ip \(CS7 M3UA\)](#) **715**
[local-ip \(CS7 SGMP\)](#) **716**
[local-ip \(CS7 SUA\)](#) **717**
[m2pa](#) **718**
[match access-group](#) **720**
[match any \(CS7 ASP\)](#) **721**
[match any \(CS7 Linkset\)](#) **722**
[match si \(cs7 asp\)\)](#) **723**

[match si \(cs7 linkset\)](#) **724**
[match-unknown-ton-np \(cs7 mlr ruleset rule\)](#) **725**
[max-inbound-streams \(CS7 M3UA\)](#) **728**
[max-inbound-streams \(CS7 SGMP\)](#) **729**
[max-inbound-streams \(CS7 SUA\)](#) **730**
[modify-failure \(cs7 mlr option\)](#) **731**
[modify-profile \(cs7 mlr ruleset rule\)](#) **732**
[mtp2](#) **733**
[mtp2-timer](#) **734**
[mtp2-timer ttc enable](#) **736**
[multi-message-dialogue \(cs7 mlr ruleset rule\)](#) **737**
[multiplicity](#) **739**
[nai](#) **740**
[network-appearance](#) **741**
[new-name](#) **742**
[np](#) **743**
[orig-imsi \(cs7 mlr ruleset rule\)](#) **744**
[orig-imsi-table \(cs7 mlr ruleset rule\)](#) **745**
[orig-sme \(cs7 mlr ruleset rule\)](#) **747**
[orig-sme-table \(cs7 mlr ruleset rule\)](#) **750**
[orig-smsc \(cs7 mlr ruleset rule\)](#) **752**
[orig-smsc \(cs7 mlr modify-profile\)](#) **754**
[outbound \(config-gws-as\)](#) **756**
[outbound \(config-gws-ls\)](#) **758**
[path-retransmit \(CS7 ASP\)](#) **760**
[path-retransmit \(CS7 Link\)](#) **761**
[path-retransmit \(cs7 m2pa profile\)](#) **762**
[path-retransmit \(CS7 M3UA\)](#) **763**
[path-retransmit \(CS7 Mated-SG\)](#) **764**
[path-retransmit \(CS7 SGMP\)](#) **765**
[path-retransmit \(CS7 SUA\)](#) **766**
[pc \(cs7 gtt application group\)](#) **767**
[pc \(cs7 mlr result\)](#) **768**
[pc-range](#) **770**
[pc-range ssn](#) **771**

peer-timer (cs7 link) 772
 peer-timer (cs7 m2pa profile) 774
 pid (cs7 mlr ruleset rule) 776
 ping cs7 777
 plan-capacity-rcvd 779
 plan-capacity-send 780
 post-gtt-address-conversion 781
 pre-gtt-address-conversion 782
 preserve-opc (cs7 mlr ruleset) 783
 preserve-opc (cs7 mlr options) 784
 preventive-txp 785
 qos-access-group 786
 qos-class (CS7 AS) 787
 qos-class (CS7 ASP) 788
 qos-class (CS7 gtt selector) 789
 qos-class (CS7 link) 790
 qos-class (cs7 m2pa profile) 791
 qos-class (CS7 Mated-SG) 792
 qos-ip-dscp 793
 qos-ip-precedence 794
 receive-window (CS7 local peer) 795
 receive-window (CS7 M3UA) 797
 receive-window (CS7 SGMP) 798
 receive-window (CS7 SUA) 799
 recovery-timeout 800
 remote-ip (CS7 ASP) 801
 remote-ip (CS7 Mated-SG) 802
 remove route (route table) 803
 result (cs7 mlr ruleset rule) 804
 retransmit-cwnd-rate (CS7 ASP) 806
 retransmit-cwnd-rate (CS7 Link) 808
 retransmit-cwnd-rate (cs7 m2pa profile) 810
 retransmit-cwnd-rate (CS7 M3UA) 812
 retransmit-cwnd-rate (CS7 Mated-SG) 814
 retransmit-cwnd-rate (CS7 SGMP) 816

retransmit-cwnd-rate (CS7 SUA) **818**
 retransmit-timeout (CS7 ASP) **820**
 retransmit-timeout (CS7 Link) **822**
 retransmit-timeout (cs7 m2pa profile) **824**
 retransmit-timeout (CS7 M3UA) **826**
 retransmit-timeout (CS7 Mated-SG) **828**
 retransmit-timeout (CS7 SGMP) **830**
 retransmit-timeout (CS7 SUA) **832**
 rotate-sls **834**
 routing-key (CS7 AS) **835**
 rule (cs7 mlr ruleset) **839**

ITP Command Set: S - Z 847

sccp-msg **851**
 set **853**
 show cs7 **855**
 show cs7 access-lists **857**
 show cs7 accounting **858**
 show cs7 as **861**
 show cs7 asp **864**
 show cs7 gtt address-conversion **869**
 show cs7 gtt application-group **870**
 show cs7 gtt concern-pclist **871**
 show cs7 gtt config **872**
 show cs7 gtt consistency **874**
 show cs7 gtt gta **876**
 show cs7 gtt map **878**
 show cs7 gtt measurements **880**
 show cs7 gtt selector **883**
 show cs7 gws action-set **884**
 show cs7 gws as **886**
 show cs7 gws linkset **888**
 show cs7 gws table **890**
 show cs7 linkset **893**
 show cs7 log **899**
 show cs7 m2pa **901**

[show cs7 m3ua](#) **909**
[show cs7 mated-sg](#) **911**
[show cs7 mlr address-table](#) **913**
[show cs7 mlr dest-sme-binding](#) **914**
[show cs7 mlr modify-profile](#) **915**
[show cs7 mlr result](#) **916**
[show cs7 mlr ruleset](#) **917**
[show cs7 mlr statistics](#) **920**
[show cs7 mlr table](#) **927**
[show cs7 mtp2](#) **930**
[show cs7 mtp3 error](#) **938**
[show cs7 mtp3 event-history](#) **942**
[show cs7 mtp3 timers](#) **943**
[show cs7 nso](#) **944**
[show cs7 offload mtp3](#) **946**
[show cs7 pc-conversion](#) **948**
[show cs7 ping](#) **949**
[show cs7 point-codes](#) **950**
[show cs7 qos](#) **952**
[show cs7 route](#) **954**
[show cs7 sccp gti-conversion](#) **959**
[show cs7 sccp instance-conversion](#) **961**
[show cs7 sccp ssn-conversion](#) **962**
[show cs7 sctp address-table](#) **963**
[show cs7 sctp port-map](#) **964**
[show cs7 sgmp](#) **965**
[show cs7 sua](#) **966**
[show cs7 tcap](#) **968**
[show cs7 version](#) **969**
[show cs7 virtual linkset](#) **970**
[show hosts](#) **973**
[show ip sctp](#) **975**
[show redundancy states](#) **982**
[show sscf-nni](#) **984**
[show sscop](#) **986**

[show tech-support](#) **989**
[shutdown \(cs7 as\)](#) **991**
[shutdown \(cs7 asp\)](#) **992**
[shutdown \(cs7 link\)](#) **993**
[shutdown \(cs7 linkset\)](#) **994**
[shutdown \(cs7 m3ua\)](#) **996**
[shutdown \(cs7 mated-sg\)](#) **997**
[shutdown \(cs7 sgmp\)](#) **998**
[shutdown \(cs7 sua\)](#) **999**
[si](#) **1000**
[sls-shift](#) **1003**
[snmp-server enable traps bits-clock](#) **1004**
[snmp-server enable traps cs7](#) **1005**
[snmp-server enable traps sctp](#) **1008**
[sscf-nni](#) **1009**
[sscop](#) **1011**
[teleservice](#) **1013**
[threshold-receive](#) **1014**
[threshold-send](#) **1015**
[timer \(cs7 hs-mtp2 profile\)](#) **1016**
[timer \(cs7 linkset\)](#) **1018**
[timer \(cs7 profile\)](#) **1021**
[traffic-mode](#) **1023**
[trigger cdpa \(cs7 mlr table\)](#) **1025**
[trigger cgpa \(cs7 mlr table\)](#) **1030**
[trigger default](#) **1033**
[trigger mtp3](#) **1035**
[ttmap](#) **1037**
[tt-range](#) **1038**
[tx-queue-depth \(cs7 asp\)](#) **1040**
[tx-queue-depth \(cs7 hs-mtp2 profile\)](#) **1041**
[tx-queue-depth \(cs7 link\)](#) **1042**
[tx-queue-depth \(cs7 m2pa profile\)](#) **1044**
[tx-queue-depth \(cs7 m3ua\)](#) **1046**
[tx-queue-depth \(cs7 mated-sg\)](#) **1047**

tx-queue-depth (cs7 profile)	1048
tx-queue-depth (cs7 sgmp)	1049
tx-queue-depth (cs7 sua)	1050
unordered-priority (cs7 m3ua)	1051
unordered-priority (cs7 sgmp)	1052
unordered-priority (cs7 sua)	1053
unrouteable-accounting	1054
update (cs7 gtt address conversion)	1055
update (cs7 sccp gti conversion)	1056
update route (route-table)	1058
variant	1060
variant jt1	1061

ITP Debug Commands 1063

debug cs7 gws	1064
debug cs7 m2pa	1065
debug cs7 m3ua	1066
debug cs7 mlr	1067
debug cs7 mtp2	1069
debug cs7 mtp3	1070
debug cs7 mtp3 paklog	1073
debug cs7 nso	1075
debug cs7 nso chkpt	1076
debug cs7 offload mtp3	1077
debug cs7 sccp	1078
debug cs7 sgmp	1080
debug cs7 snmp	1081
debug cs7 sua	1082
debug cs7 tcap	1083

ITP System Messages 1085

How This Manual Is Organized	1085
How to Read System Messages	1086
CS7ADDRTBL Messages	1086
CS7CDR Messages	1087
CS7CHKPT Messages	1088
CS7GROUP Messages	1089

CS7HSL Messages	1091
CS7M2PA Messages	1092
CS7MAPUA Messages	1094
CS7MLR Messages	1096
CS7MONITOR Messages	1097
CS7MTP2 Messages	1099
CS7MTP3 Messages	1101
CS7NSO Messages	1119
CS7PING Messages	1121
CS7RF Messages	1123
CS7ROUTE Messages	1124
CS7SCCP Messages	1127
CS7SMS Messages	1134
CS7TCAP Messages	1136
CS7XUA Messages	1136
DCS7 Messages	1140





About this Book

This preface describes the audience, organization, and conventions of *IP Transfer Point on the Cisco 7600 Platform*. 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 29](#)
- [Documentation Organization, page 30](#)
- [Documentation Conventions, page 31](#)
- [Obtaining Documentation, page 33](#)
- [Documentation Feedback, page 33](#)
- [Cisco Product Security Overview, page 34](#)
- [Obtaining Technical Assistance, page 35](#)
- [Obtaining Additional Publications and Information, page 36](#)

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 (ITP) on the Cisco 7600 Platform</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.
Non-Disruptive Upgrade on the Cisco 7600 Platform	Describes the ITP IOS software upgrade procedure on the Cisco 7600 platform.
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.
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.
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

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only — security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered non-emergencies.

- For Non-emergencies — psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>



Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

<http://www.cisco.com/go/guide>

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:
<http://www.cisco.com/go/marketplace/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:
<http://www.cisco.com/packet>
- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:
<http://www.cisco.com/go/iqmagazine>
or view the digital edition at this URL:
<http://ciscoiq.texterity.com/ciscoiq/sample/>
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:
<http://www.cisco.com/ipj>
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
<http://www.cisco.com/discuss/networking>
- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.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 39](#)
- [Getting Help, page 40](#)
- [Using the no and default Forms of Commands, page 43](#)
- [Filtering Output from the show and more Commands, page 44](#)
- [Finding Additional Feature Support Information, page 44](#)

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
<pre>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)#</pre>	<p>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.</p>
<pre>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</pre>	<p>Enter the command that you want to configure for the interface. This example uses the ip command.</p> <p>Enter ? to display what you must enter next on the command line. This example shows only some of the available interface IP configuration commands.</p>

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

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 dependant 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.

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

- [SS7oIP Technology Overview, page 45](#)
- [Benefits, page 48](#)

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>.

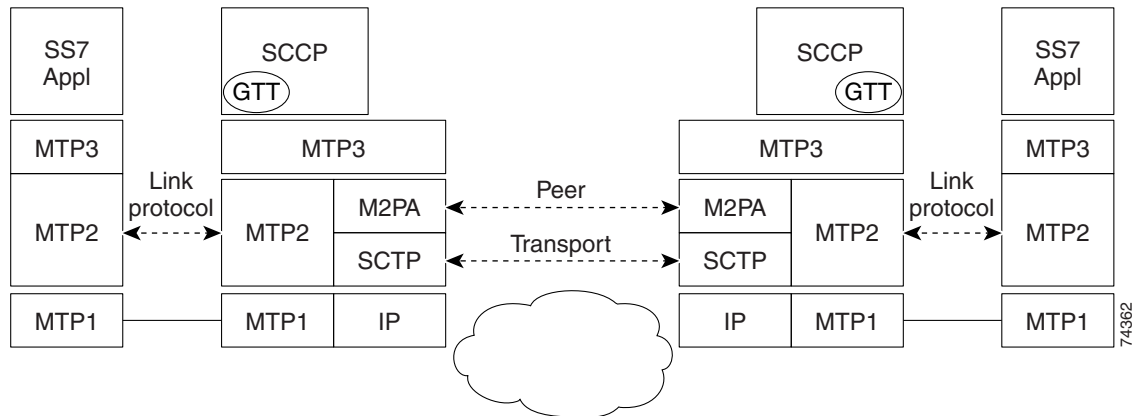
Stream Control Transmission Protocol (RFC2960)

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*

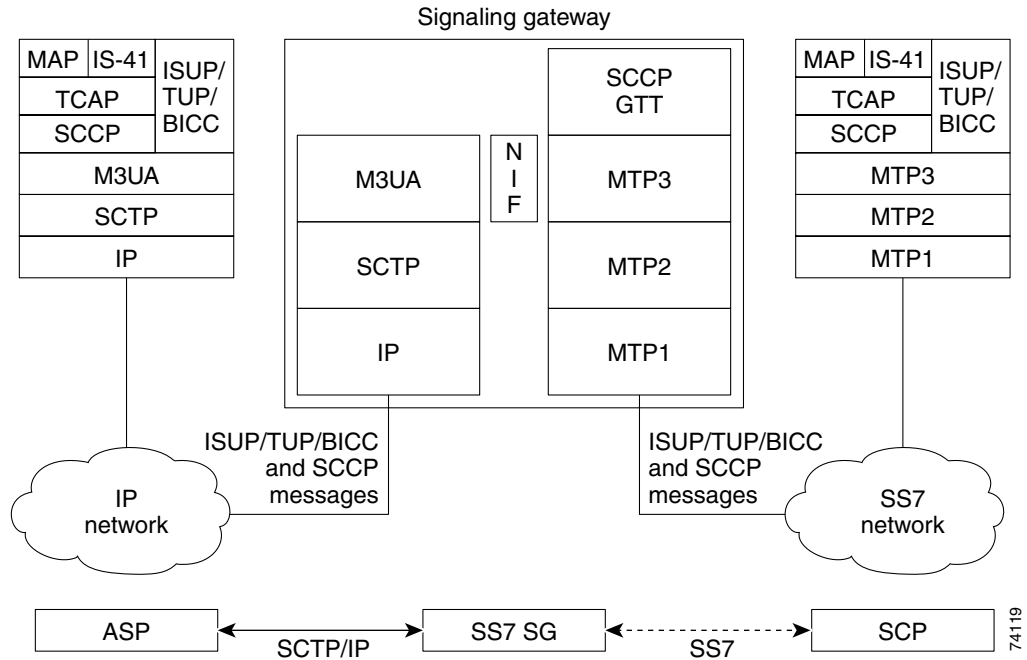


M2PA offers a protocol high availability similar to an STP. The MTP3 implementation layer in an M2PA SG is unaware of whether a link is time-division multiplexing (TDM) or IP and run equally well over either. This preserves congestion, Layer 2 failure detection, changeover, change-back, load balancing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

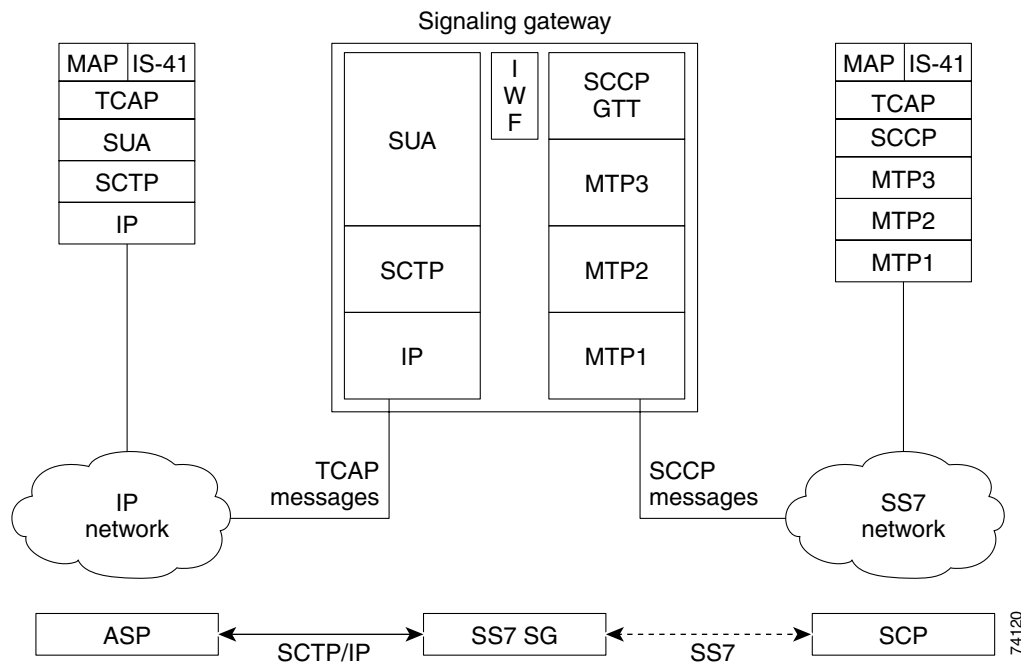
Figure 2 M3UA Signaling Gateway Protocol Stacks

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 7606 Router
- Cisco 7609 Router
- Cisco 7613 Router
- FlexWAN Module for the Cisco 7600 Series Router
- Cisco 7600 Series Supervisor Engine 720

Restrictions

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

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

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

Supported Standards, MIBs, and RFCs

Standards

- ANSI 1996
- ITU white 1996
- M2PA-User Peer-to-Peer Adaptation Layer [draft-ietf-sigtran-m2pa-02.txt, March 2, 2001]
- 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-DSMR-MIB.my

MIB for information about Distributed Short Message Routing for Short Message Service Center.

NOTIFICATIONS

- ciscoItpDsmrTableLoad

- CISCO-ITP-DSMR-SMPP.my

MIB for information about Distributed Short Message Routing for Short Message Service Center message delivered using SMPP.

NOTIFICATIONS

- ciscoItpDsmrSmppSessionState

- CISCO-ITP-DSMR-UCP-MIB.my

MIB for information about Distributed Short Message Routing for Short Message Service Center message delivered using UCP.

NOTIFICATIONS

- ciscoItpDsmrUcpSessionState

- 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

- ciscoGscppGttErrors
- ciscoGscppGttLoadTable
- ciscoGscppGttMapStateChange

- 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-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)
- Stream Control Transmission Protocol (RFC 2960)



ITP Non-Disruptive Upgrade on the Cisco 7600 Platform

Feature History for Non-Disruptive Upgrade

Release	Modification
12.2(18)IXA	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

- [Prerequisites for Non-Disruptive Upgrade, page 53](#)
- [Information About Non-Disruptive Upgrade, page 54](#)
- [Performing a Non-Disruptive Upgrade, page 54](#)
- [, page 61](#)

Prerequisites for Non-Disruptive Upgrade

- Stateful Switchover (SSO) must be configured.
- Non-Stop Operation (NSO) must be configured

- The network configuration must provide link/linkset redundancy; linksets span multiple FlexWAN modules.

Information About Non-Disruptive Upgrade

The Non-Disruptive Upgrade feature enables you to upgrade the software image on a Supervisor 720 and a FlexWAN.

Performing a Non-Disruptive Upgrade



Note

Before the first upgrade switchover users must make sure that the new image is first on the standby and the old image is first on the current active.



Note

The CS7 configuration will be locked out once the Standby Supervisor is reset with the new image.

To perform a Non-Disruptive Upgrade you perform the tasks described in the following sections:

- [Preparing for Non-Disruptive Upgrade, page 54](#)
- [Resetting the Standby Supervisor, page 57](#)
- [Switching the Standby Supervisor to Active Role, page 58](#)
- [Upgrading the Software Image on FlexWAN Line Cards, page 59](#)
- [Upgrading the Software Image on the Standby Supervisor, page 59](#)

Preparing for Non-Disruptive Upgrade

The steps in this task prepare for the Non-Disruptive Upgrade procedure.

We recommend that before performing the upgrade procedure, you use the **copy running-config startup-config** command to save the running configuration as the startup configuration.

We also recommend that you run the **cs7 upgrade analysis** command. This command displays the available links configured in each FlexWAN slot and reports either the destinations that might become inaccessible due to loss of all links in a linkset if the FlexWAN is upgraded or the expected utilization of remaining links on other FlexWANs due to diversion of traffic to those links, and displays a summary of the upgrade process. Sample output is shown in the command reference chapter entry for the **cs7 upgrade analysis** command.



Note

You can use the **show cs7** command or **show cs7 version** command at any time during the NDU process to see the status of the upgrade.



Note

For the purposes of this task, OLD image refers to the pre-upgrade image and NEW image refers to the upgrade image.

SUMMARY STEPS

1. **enable**
2. **copy running-config startup-config**
3. **cs7 upgrade analysis**
4. **mkdir slavedisk0:archive**
5. **rename slavedisk0:image slavedisk0:archive/image**
6. **copy tftp:newimage slavedisk0:newimage**
7. **verify /md5 slavedisk0:newimage [checksum]**
8. **boot system disk0:**
9. **show boot | include BOOT**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: ITP> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	copy running-config startup-config Example: ITP# copy running-config startup-config	Saves the running configuration as the startup configuration.
Step 3	cs7 upgrade analysis Example: ITP# cs7 upgrade analysis	Shows the current software version on Supervisors and all FlexWANs and provides an analysis of each of the FlexWAN slots. Sample output is provided in the command reference entry for the cs7 upgrade analysis command.
Step 4	mkdir slavedisk0:archive Example: ITP# mkdir slavedisk0:archive	Creates a subdirectory named archive on slavedisk0.
Step 5	rename slavedisk0:image slavedisk0:archive/image Example: ITP# rename slavedisk0:s72033-itpk9v-mz.122-18.IXA slavedisk0:archive/s72033-itpk9v-mz.122-18.IXA	Moves existing image from slavedisk0: to the slavedisk0:archive subdirectory. Repeat this step as necessary to move all images from slavedisk0 to the subdirectory.
Step 6	copy tftp:newimage slavedisk0:newimage Example: ITP# copy tftp:s72033-itpk9v-mz.122-18.IXB slavedisk0:s72033-itpk9v-mz.122-18.IXB	Copies the new image onto the disk.

	Command or Action	Purpose
Step 7	<pre>verify /md5 slavedisk0:newimage [checksum]</pre> <p>Example:</p> <pre>ITP# verify /md5 slavedisk0:s72033-itpk9v-mz.122-18.IXB 740ba4eb52bcf8ffae9909938f36a955Done! Verified (slavedisk0:s72033-itpk9v-mz.122-18.IXB) = 740ba4eb52bcf8ffae9909938f36a955</pre>	<p>Verifies the image on the Standby Supervisor.</p> <p>Note: In the example, the verify command includes an optional checksum. If you include the md5 checksum in the command, the output will indicate either verification or error. If you do not include the md5 checksum the command will simply return the computed checksum which you would have to manually check against the sum published with the image.</p>
Step 8	<pre>boot system disk0:</pre> <p>Example:</p> <pre>ITP# boot system disk0:</pre>	<p>Sets the location to boot from.</p> <p>Note: Remove any other boot statements. This should be the only boot statement in the running config.</p> <p>The boot system disk0: command will boot the first valid image file on disk0: from the list of files as seen in the output of dir disk0:. Make sure that the first image on disk0: is the old image and the first image on slavedisk0: is the new image.</p>
Step 9	<pre>show boot include BOOT</pre> <p>Example:</p> <pre>Router# show boot include BOOT Verify that one location is listed and that standby variable matches the primary. Example: BOOT variable = disk0:,12; and Standby BOOT variable = disk0:,12;</pre>	<p>Displays output to verify that the boot variable is set to disk0:.</p>

What to Do Next

Reset the Standby Supervisor.

Resetting the Standby Supervisor

This task resets the standby Supervisor (SUP2 in our scenario) and boots the new software that you loaded onto the standby Supervisor in the previous task. The standby Supervisor progresses to the “STANDBY HOT” state. After resetting the Standby Supervisor, you can verify the redundancy status.

SUMMARY STEPS

1. **hw-module module *standby-sup-slot* reset**
2. **show redundancy states**
3. **show cs7 nso state**

DETAILED STEPS

	Command or Action	Purpose
Step 1	hw-module module <i>standby-sup-slot</i> reset Example: ITP# hw-module module 6 reset	Resets the specified Supervisor module. In the example, the specified Supervisor module is the standby Supervisor (SUP2) in slot 6.
Step 2	show redundancy states Example: ITP# show redundancy states	Displays redundancy state information. Sample output is provided in the command reference entry for the show redundancy states command.
Step 3	show cs7 nso state Example: ITP# show cs7 nso state	Displays Non-stop operation (NSO) state information. Sample output is provided in the command reference entry for the show cs7 nso state command.

What to Do Next

Switch the Standby Supervisor to ACTIVE Role

Switching the Standby Supervisor to Active Role

This task switches the role of “ACTIVE” to the Supervisor that you reset in the previous task (SUP2, which is running the new software). The previously Active Supervisor (SUP1, which is running the old software) is now in the STANDBY COLD role. After forcing the switchover, you can verify the redundancy status.

SUMMARY STEPS

1. `redundancy force-switchover`
2. `show redundancy states`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>redundancy force-switchover</code>	Switches the role of “ACTIVE” to the Supervisor to the current Standby Supervisor (SUP2).
	Example: <code>ITP# redundancy force-switchover</code>	Wait for the message “Standby supervisor is up. Line cards can be upgraded now.”
Step 2	<code>show redundancy states</code>	Displays redundancy state information.
	Example: <code>ITP# show redundancy states</code>	

What to Do Next

Upgrade the software image on the FlexWAN line cards.

Upgrading the Software Image on FlexWAN Line Cards

In this step, the newly ACTIVE Supervisor (SUP2 in our scenario) upgrades a specified FlexWAN line card. This step can be performed only after the message “Standby supervisor is up. Line cards can be upgraded now” is returned from the redundancy force-switchover command that you performed in the previous task.

SUMMARY STEPS

1. **cs7 upgrade module**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>cs7 upgrade module slotnumber</code> Example: <code>ITP# cs7 upgrade module 1</code>	<p>Upgrades the software on a linecard. Repeat this step for all FlexWANs.</p> <p>This step can be performed only after the message “Standby supervisor is up. Line cards can be upgraded now” is returned from the redundancy force-switchover command that you performed in the previous task.</p>

What to Do Next

Upgrade the software image on the standby Supervisor.

Upgrading the Software Image on the Standby Supervisor

In this final step you upgrade the software image on the Standby Supervisor (SUP1 in our scenario) to the new image. The Standby Supervisor has been in the STANDBY COLD state to allow for a quick revert/reset. You will now copy the new software image to the filesystem of the new Standby Supervisor and reset the module to bring the system back to SSO mode and a STANDBY HOT state with both Supervisors now running the new software image.

SUMMARY STEPS

1. **mkdir slavedisk0:archive**
2. **rename slavedisk0:image slavedisk0:archive/image**
3. **copy disk0:newimage slavedisk0:newimage**
4. **hw-module module standby-sup-slot reset ¹**
5. **show redundancy states**
6. **show cs7 nso state**

1. This command is documented in detail in the Cisco 7600 Series Cisco IOS Command Reference, 12.2 SX.

DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>mkdir slavedisk0:archive</pre> <p>Example: ITP# mkdir slavedisk0:archive</p>	Creates a subdirectory named archive on slavedisk0.
Step 2	<pre>rename slavedisk0:image slavedisk0:archive/image</pre> <p>Example: ITP# rename slavedisk0:s72033-itpk9v-mz.122-18.IXA slavedisk0:archive/s72033-itpk9v-mz.122-18.IXA</p>	<p>Moves existing image from slavedisk0 to the slavedisk0:archive subdirectory.</p> <p>Repeat this step as necessary to move all images from slavedisk0 to the subdirectory.</p>
Step 3	<pre>copy disk0:newimage slavedisk0:newimage</pre> <p>Example: ITP# copy disk0:NEW slavedisk0:NEW</p>	Copies the new Supervisor image onto the Standby Supervisor.
Step 4	<pre>hw-module module standby-sup-slot reset</pre> <p>Example: ITP# hw-module module 5 reset</p>	<p>Resets the Standby Supervisor.</p> <p>In the example, the Standby Supervisor is in slot 5.</p>
Step 5	<pre>show redundancy states</pre> <p>Example: ITP# show redundancy states</p>	<p>Displays redundancy state information.</p> <p>Sample output is provided in the command reference entry for the show redundancy states command.</p>
Step 6	<pre>show cs7 nso state</pre> <p>Example: ITP# show cs7 nso state</p>	<p>Displays Non-stop operation (NSO) state information.</p> <p>Sample output is provided in the command reference entry for the show cs7 nso state command.</p>



Configuring ITP Basic Functionality



Note

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



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 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 URL:

<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/software/122sx/swcg/index.htm>

http://www.cisco.com/en/US/products/sw/iosswrel/tsd_products_support_category_home.html

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/index.htm>

For information about configuring interfaces, beyond the specific ITP configuration instructions that are included in this document, refer to the Cisco IOS 12.2 Interface Configuration Guide at the following URL:

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

Feature History for Basic Configuration

Release	Modification
12.2(25)SW6	<ul style="list-style-type: none">The Secure Shell (SSH) feature is supported on the ITP in the Cisco 7500 (image rsp-itpk91v-mz), Cisco 7301 (image c7301-itpk91-mz), and Cisco 7200 (image c7200-itpk91-mz) platforms.The JT1 interface, the Japanese variation of the standard framing formats for T1 controller settings, is supported on the ITP. The JT1 interface is a 1544 kbit/s line type specified by the Japanese standards organization, TTC.

12.2(25)SW8	The linestate debounce command was added to suppress rapid linestate transitions that may occur due to brief interruptions of the framing on an E1 controller.
12.4(11)SW	Feature introduced with support for multiple HSL PVCs per physical ATM interface.
12.2(18)IXA	The Secure Shell (SSH) feature is supported on the ITP in the Cisco 7600 platforms (s72033-itpk9v-mz).
12.2(18)IXA	The JT1 interface, the Japanese variation of the standard framing formats for T1 controller settings, is supported on the ITP. The JT1 interface is a 1544 kbit/s line type specified by the Japanese standards organization, TTC.
12.2(18)IXB	The linestate debounce command was added to suppress rapid linestate transitions that may occur due to brief interruptions of the framing on an E1 controller.
12.2(18)IXC	Added support for multiple HSL PVCs per physical ATM interface.
12.2(18)IXD	Added enhanced load sharing to improve load distribution among available links.

Contents

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

- [Configuring Redundancy and Stateful Switchover \(SSO\), page 65](#)
- [Configuring RPR+ \(Cisco 7500 Series Only\), page 66](#)
- [Enabling Secure Shell, page 73](#)
- [Specifying the SS7 Variant, National Option, and Network Indicator, page 75](#)
- [Specifying the Point Code, page 76](#)
- [Specifying the Point Code, page 76](#)
- [Specifying the Interface and Encapsulation, page 79](#)
- [Configuring Local Peers, page 92](#)
- [Configuring Linksets, page 93](#)
- [Configuring Multiple Linksets to Adjacent Nodes, page 94](#)
- [Specifying the Cisco ITP Route Table, page 95](#)
- [Assigning Links to Linksets, page 96](#)
- [Shutting Down and Restarting Linksets and Links, page 98](#)
- [Configuration Example of RPR+, page 99](#)
- [Configuration Example of ITP Basic Functionality, page 101](#)

Configuring Redundancy and Stateful Switchover (SSO)

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `redundancy`
4. `mode sso`
5. `end`
6. `show redundancy states`

DETAILED STEPS

	Command	Purpose
Step 1	<code>enable</code>	Enables higher privilege levels, such as privileged EXEC mode.
	Example: <code>ITP> enable</code>	Enter your password if prompted.
Step 2	<code>configure {terminal memory network}</code>	Enters global configuration mode.
	Example: <code>ITP# configure terminal</code>	
Step 3	<code>redundancy</code>	Enters redundancy mode.
	<code>ITP(config)# redundancy</code>	
Step 4	<code>mode sso</code>	Sets the redundancy mode to SSO
	Example: <code>ITP(config-red)# mode sso</code>	
Step 5	<code>end</code>	Exits configuration mode.
	Example: <code>ITP(config-r)# end</code>	
Step 6	<code>show redundancy states</code>	Displays the operating redundancy state.
	Example: <code>ITP# end</code>	

Configuring RPR+ (Cisco 7500 Series Only)

The Route Processor Redundancy Plus (RPR+) feature is an enhancement of the RPR feature on Cisco 7500 series routers. RPR+ reduces the amount of unplanned downtime of a Cisco 7500 series router by enabling a faster switchover time to the standby Route Switch Processor (RSP). RPR+ keeps the Virtual Interface Processors (VIPs) from being reset and reloaded when a switchover occurs between the active and standby RSPs. Because VIPs are not reset and microcode is not reloaded on the VIPs, and the time needed to parse the configuration is eliminated, switchover time is reduced to 10 to 30 seconds.

Feature	Switchover Time	Notes
High System Availability (HSA)	8 to 10 minutes	System default.
RPR	4 to 5 minutes	VIPs and legacy interface processors supported.
RPR+	10 to 30 seconds	VIPs supported.

- RPR+ requires a Cisco 7500 series router loaded with two RSP8s.

- RPR+ operates only in a system with VIPs as the line cards. Systems with legacy Interface Processors default to RPR.
- In RPR+ mode, configuration changes done through SNMP may not be automatically configured on the standby RP after a switchover occurs.
- RPR+ does not work on routers configured with MPLS.

See the following sections for the configuration tasks required to run RPR+:

- [Copying an Image onto an RSP, page 67](#) (required)
- [Configuring RPR+, page 69](#) (required)
- [Setting the Config-Register Boot Variable, page 71](#) (optional)

Copying an Image onto an RSP

Use TFTP to copy a high availability Cisco IOS image onto the active and standby RSPs.



Note

Secure Shell (SSH) feature is supported on the ITP in the Cisco 7500 platform with image `rsp-itpk91v-mz`.

SUMMARY STEPS

1. `enable`
2. `copy tftp slotslot-number:`
3. `copy tftp slaveslotslot-number:`

DETAILED STEPS

	Command	Purpose
Step 1	<code>enable</code>	Enables higher privilege levels, such as privileged EXEC mode.
	Example: <code>ITP> enable</code>	Enter your password if prompted.

Step 2	<pre>copy tftp slotslot-number:</pre> <p>Example:</p> <pre>ITP# copy tftp slot0:</pre> <p>Address or name of remote host []? <i>ip-address</i></p> <p>Name of file to copy []? <i>imagename</i><Return> writing filename!!</p> <p>Destination file name? [<i>imagename1</i>] <Return> Accessing file 'imagename' on ip-address.. found !</p> <p>Loading imagename from ip-address (via Ethernet1/0/0): !</p>	<p>Uses TFTP to copy a high availability Cisco IOS image onto the Flash memory card of the active RSP.¹</p> <ul style="list-style-type: none"> slotslot-number—Specifies the Flash memory card of the active RSP. <p>The router prompts you for the IP address of the TFTP server.</p> <ul style="list-style-type: none"> ip-address—Specifies the IP address of the TFTP server that contains the new image. <p>The router prompts you for the name of the image file you are copying to the Flash memory card.</p> <ul style="list-style-type: none"> imagename—Indicates the name of the image to be loaded onto the Flash memory card. <p>The router prompts you to enter the name under which you want the file to appear at the destination.</p> <ul style="list-style-type: none"> imagename1—Indicates the name of the image as it appears at the destination.
Step 3	<pre>copy tftp slaveslotslot-number:</pre> <p>Example:</p> <pre>ITP# copy tftp slaveslot0:</pre> <p>Address or name of remote host []? <i>ip-address</i></p> <p>Name of file to copy []? <i>imagename</i><Return> writing filename!!</p> <p>Destination file name? [<i>imagename1</i>] <Return> Accessing file 'imagename' on ip-address.. found !</p> <p>Loading imagename from ip-address (via Ethernet1/0): !</p>	<p>Uses TFTP to copy a high availability Cisco IOS image onto the Flash memory card of the standby RSP.</p> <ul style="list-style-type: none"> slaveslotslot-number—Specifies the Flash memory card of the standby RSP. <p>The router prompts you for the IP address of the TFTP server.</p> <ul style="list-style-type: none"> ip-address—Specifies the IP address of the TFTP server that contains the new image. <p>The router prompts you for the name of the image file you are copying to the Flash memory card.</p> <ul style="list-style-type: none"> imagename—Indicates the name of the image to be loaded onto the Flash memory card. <p>The router prompts you to enter the name under which you want the file to appear at the destination.</p> <ul style="list-style-type: none"> imagename1—Indicates the name of the image as it appears at the destination.

- Before you copy a file to Flash memory, be sure there is ample space available in Flash memory. Compare the size of the file you are copying to the amount of available Flash memory shown. If the space available is less than the space required by the file you will copy, the copy process will not continue and an error message similar to the following will be displayed;

```
%Error copying tftp://image@server/tftpboot/filelocation/imagename (Not enough space on device).
```


Configuring RPR+



Note

RPR+ should be configured on the ITP before any global SS7 configuration is done. This will allow Cisco IOS to save all configuration including route and GTT tables on both RSP cards.

To configure RPR+, enter the commands as shown below.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **hw-module slots***slot-number* **image** *file-spec*
4. **service single-slot-reload-enable**
5. **redundancy**
6. **mode rpr-plus**
7. **end**
8. **hw-module sec-cpu reset**

DETAILED STEPS

	Command	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	Purpose
Step 3	<pre>hw-module slotslot-number image file-spec</pre> <p>Example: ITP(config)# hw-module slot2 image slot0:rsp-pv-mz</p>	<p>Verifies that the specified image is compatible with RPR+ and exists on the standby RSP. If a high availability image is found, the running configuration is updated.</p> <ul style="list-style-type: none"> <i>slot-number</i>—Specifies the standby RSP slot where the Flash memory card is located. Valid numbers are slot 2 or slot 3 for a Cisco 7507 router or slot 6 or slot 7 for a Cisco 7513 router. <i>file-spec</i>—Indicates the Flash device and the name of the image on the standby RSP. <p>Note The image indicated by the <i>file-spec</i> attribute must be available on the local Flash device. Remote protocols such as Trivial File Transfer Protocol (TFTP) and remote copy protocol (RCP) are not available.</p>
Step 4	<pre>service single-slot-reload-enable</pre> <p>Example: ITP(config)# service single-slot-reload-enable</p>	Enable single line card reloading.
Step 5	<pre>redundancy</pre> <p>Example: ITP(config)# redundancy</p>	Enters redundancy mode.
Step 6	<pre>mode rpr-plus</pre> <p>Operating mode is RPR, configured mode is rpr-plus.</p> <p>Example: ITP(config-r)# mode rpr-plus</p>	Sets the redundancy mode to RPR+ on both the active and standby RSPs. HSA is the default redundancy mode.
Step 7	<pre>end</pre> <p>Example: ITP(config-r)# end</p>	Exits configuration mode.
Step 8	<pre>hw-module sec-cpu reset</pre> <p>Example: ITP# hw-module sec-cpu reset</p>	<p>Resets and reloads the standby RSP with the specified Cisco IOS image and executes the image.</p> <p>Note If you do not specify a Cisco IOS image in Step 2, this command loads and executes the bundled default IOS standby image. The system then operates in HSA mode.</p>

If a second RSP is added, then it is necessary to perform the following steps after RPR+ is enabled.

SUMMARY STEPS

1. enable

2. **copy running-config startup-config**
3. **copy slotslot-number:route-table slaveslotslot-number:route-table**
4. **copy slotslot-number:gtr-table slaveslotslot-number:gtr-table**
5. **hw-module sec-cpu reset**

DETAILED STEPS

	Command	Purpose
Step 1	enable Example: ITP> enable	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	copy running-config startup-config Example: ITP# copy running-config startup-config	Populate and save the current configuration on both primary and secondary RSP.
Step 3	copy slotslot-number:file slaveslotslot-number:file Example: ITP# copy slot0:mtp3-routes slaveslot0:mtp3-routes	Copy the MTP3 routing table (in the example, saved as slot0:mtp3-routes) to the flash card on the secondary RSP. This step can be omitted if no routing table has been saved. "slot0:" will have to be replaced with "disk0:" if a 128 MByte ATA pcmcia disk is used.
Step 4	copy slotslot-number:file slaveslotslot-number:file Example: ITP# copy slot0:gtr-table slaveslot0:gtr-table	Copy the GTR table (in the example, saved as slot0:gtr-table) to the flash card on the secondary RSP. This step can be omitted if no GTR is configured. "slot0:" should be replaced with "disk0:" if a 128 MByte ATA pcmcia disk is used.
Step 5	hw-module sec-cpu reset Example: ITP# hw-module sec-cpu reset	This step is mandatory if one of the two previous copy commands was entered. It will restart the secondary RSP and ensure that in the unlikely event of a switchover, correct tables are available.

Setting the Config-Register Boot Variable

Though it is not required, we recommend that you modify the software configuration register boot field so that the system boots the same image that you specified in the **hw-module slotslot-number image file-spec** command in the previous task section.

SUMMARY STEPS

1. **enable**
2. **show version**
3. **configure terminal**
4. **boot system flash slotslot-number:[imagename]**

5. `config-register 0x2102`
6. `Ctrl-Z1`
7. `reload`

DETAILED STEPS

	Command	Purpose
Step 1	<code>enable</code> Example: <code>ITP> enable</code>	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	<code>show version</code> Example: <code>ITP# show version</code>	Obtains the current configuration register setting.
Step 3	<code>configure terminal</code> Example: <code>ITP# configure terminal</code>	Enters configuration mode, selecting the terminal option.
Step 4	<code>boot system flash slotslot-number:[imagename]</code> Example: <code>ITP(config)# boot system flash slot 2:rsp-pv-mz</code>	Specifies the filename of an image stored in Flash memory. <ul style="list-style-type: none"> <i>imagename</i>—It is recommended that you set the boot variable so that the system boots the same image specified by the hw-module slotslot-number image file-spec command. See Step 3 of the “Configuring RPR+” section on page 69. <i>slot-number</i>—Specifies the active RSP slot where the Flash memory card is located. Valid numbers are slot 2 or slot 3 for a Cisco 7507 router and slot 6 or slot 7 for a Cisco 7513 router.
Step 5	<code>config-register value</code> Example: <code>ITP# config-register 0x2102</code>	Modifies the existing configuration register setting to reflect the way in which you want to load a system image. <i>value range</i> —0x0 to 0xFFFFFFFF
Step 6	<code>Ctrl-Z¹</code> Example: <code>ITP# Ctrl-z</code>	Exits configuration mode.
Step 7	<code>reload</code> Example: <code>ITP# reload</code>	Reboots the router to make your changes take effect.

1. Keyboard combination, not a typed command.

1. Keyboard combination, not a typed command.

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 12.2 Security Configuration Guide* at the following URL:

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

and to the *Cisco IOS Release 12.2 Security Command Reference* at the following URL:

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

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	Enables higher privilege levels, such as privileged EXEC mode.
	Example: ITP> enable	Enter your password if prompted.
Step 2	configure {terminal memory network}	Enters configuration mode, selecting the terminal option.
	Example: ITP# configure terminal	
Step 3	username username password password	Specifies the username and password.
	Example: ITP(config)# username admin password jo4fhe	

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

	Command	Purpose
Step 4	<pre>cs7 national-options {TFR multiple-congestion route-set-congestion-test combined-linkset-loadsharing}</pre> <p>Example: ITP(config)# cs7 national-options TFR</p>	<p>Specifies national options.</p> <p>The national options apply to the variants as follows:</p> <ul style="list-style-type: none"> • TFR: ITU and China SS7 Variants • multiple-congestion ITU and China SS7 Variants • route-set-congestion-test TTC SS7 Variant • combined-linkset-loadsharing configures the TTC variant to use the enhanced loadsharing algorithm. <p>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.</p>
Step 5	<pre>cs7 network-indicator {international national reserved spare}</pre> <p>Example: ITP(config)# cs7 network-indicator international</p>	<p>(Optional) Specifies the network indicator.</p> <p>The network indicator on the ITP must match the network indicator in use in the rest of the SS7 network. The default is national.</p>
Step 6	<pre>cs7 [instance instance-number] local-sccp-addr-ind {national international}</pre> <p>Example: ITP(config)# cs7 local-sccp-addr-ind international</p>	<p>(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).</p>

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

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

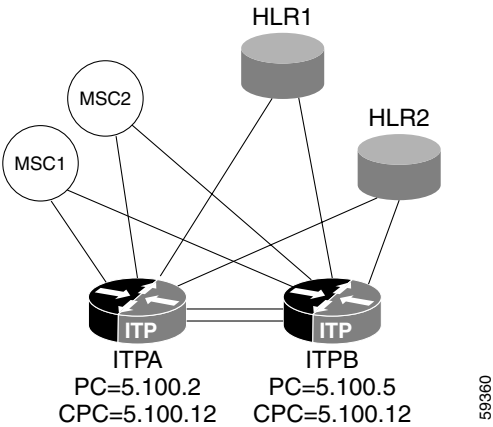
If you intend to configure a second linkset between the ITP and an adjacent node, you must specify a secondary local point code. To specify the secondary point code, use the following command in global configuration mode:

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: <pre>ITP(config)# cs7 capability-pc 5.100.12</pre>	

**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

Depending on your network configuration, you can configure the ITP to accommodate channelized T1/E1 links and High Speed Signaling Links (HSL) over ATM.

**Note**

We recommend that you do not mix link types (low speed links, high speed links, M2PA/XUA) on the same VIP.

**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**

On a 2600, because of the two SS7 links per WIC restriction, up to two slots on any T1/E1 interface can be used for SS7 links.

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

- [A Note About Clocking on the SS7 Port Adapter and SS7 Q.703 High Speed Port Adapter, page 79](#)
- [Configuring a Serial Interface and SS7 High-Speed MTP2 Encapsulation \(Q.703 Annex A\) on the SS7 Q.703 High Speed Port Adapter, page 80](#)
- [Configuring a Serial Interface and MTP2 Encapsulation on the SS7 Port Adapter, page 81](#)
- [Configuring SS7 over ATM High Speed Links \(HSL\), page 83](#)
- [Configuring SS7 ATM High Speed Links with BITS Network Clocking, page 86](#)

A Note About 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	<code>card type e1 slot bay</code>	Configures the card type.
	Example: <code>ITP(config)# card type e1 6 0</code>	
Step 2	<code>controller e1 slot/bay/port</code>	Configures an E1 controller.
	Example: <code>ITP(config)# controller e1 6/0/0</code>	

	Command	Purpose
Step 3	<code>framing crc4</code> Example: ITP(config-controller)# framing crc4	Specifies the framing format for E1 controller.
Step 4	<code>linestate debounce</code> Example: ITP(config-controller)# linestate debounce	Supresses rapid linestate transitions that may occur due to brief interruption of the framing on an E1 controller.
Step 5	<code>clock source {bits {primary secondary priority} internal line {primary secondary priority}}</code> Example: ITP(config-controller)# clock source internal	Specifies the clock source as internal.
Step 6	<code>linecode hdb3</code> 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	<code>channel-group channel-number timeslots 1-31</code> 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	<code>exit</code> Example: ITP(config-controller)# exit	Exit controller configuration mode and return to global configuration mode.
Step 9	ITP(config)# <code>interface serial number</code> Example: ITP(config)# interface serial 6/0/0:0	Configures a serial interface in global configuration mode and enters interface configuration mode.
Step 10	<code>encapsulation hs-mtp2</code> 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:

	Command	Purpose
Step 1	<code>card type {t1 e1} slot bay</code> Example: <code>ITP(config)# card type t1 1 1</code>	Configures the card type.
Step 2	<code>controller {t1 e1} slot/port-adapter-num/port</code> Example: <code>ITP(config)# controller t1 1/1/1</code>	Specifies the controller and enters controller configuration mode.
Step 3	<code>linestate debounce</code> Example: <code>ITP(config-controller)# linestate debounce</code>	(Optional for E1 controller configuration.) Suppresses rapid linestate transitions that may occur due to brief interruption of the framing on an E1 controller.
Step 4	<code>variant jtl</code> Example: <code>ITP(config-controller)# variant jtl</code>	(Optional) Applies to T1 interface only. Enables Japanese variations of the standard framing formats.

	Command	Purpose
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.
Step 11	ITP(config)# interface serial number Example: ITP(config)# interface serial 1	Configures a serial interface in global configuration mode and enters interface configuration mode.
Step 12	ITP(config-if)# encapsulation mtp2 Example: ITP(config)# encapsulation mtp2	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 84](#) (Required)
- [Configuring a Permanent Virtual Circuit \(PVC\), page 85](#) (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	<code>interface atm interface-number[.subinterface-number]</code> Example: ITP(config)# <code>interface atm 2/0.1</code>	Enters the configure ATM interface or configure ATM subinterface mode.
Step 2	<code>no shutdown</code>	Enables the interface.
Step 3	<code>framing esfadm</code> -OR- <code>framing crc4adm</code> For OC3 use the following: <code>atm framing sdh</code> -OR- <code>atm framing sonet</code> Example: ITP(config-if)# <code>framing crc4adm</code>	Specifies frame type (T1 only). -or- Specifies frame type (E1 only). Specifies SDH framing mode (OC3 only). -or- Specifies SONET framing mode (OC3 only).
Step 4	<code>clock-source {common internal line}</code> Example: ITP(config-if)# <code>clock-source internal</code>	(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	<code>interface atm interface-num</code> Example: ITP(config)#	Specifies an ATM interface and enters interface configuration mode.

	Command	Purpose
Step 2	<code>no shutdown</code>	Enables the interface.
	Example: <code>ITP(config-if)# no shutdown</code>	
Step 3	<code>atm sonet stm-1</code>	Specifies SDH (STM-1) framing.
	Example: <code>ITP(config-if)# atm sonet stm-1</code>	

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	<code>atm nni</code>	Selects service specific coordination function for Network Node Interface.
	Example: <code>ITP(config-if)# atm nni</code>	
Step 2	<code>pvc [name] {vpi/vci} [qsaal]</code>	Specifies the PVC. The default/recommended PVC number is 0/5.
	Example: <code>ITP(config-if)# pvc 0/5 qsaal</code>	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 qssal, and add these subinterfaces to the linkset.

To configure the linkset, see the “[Configuring Linksets](#)” section on page 93. To specify or tune optional HSL bundling, SSCF-NNI, or SSCOP parameters, see the “[Tuning HSL Parameters](#)” section on page 377 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	<code>controller {t1 e1} slot/port-adapter-num/port</code> Example: <code>ITP(config)# controller t1 1/1/1</code>	Specifies the controller and enters Controller configuration mode.
Step 2	<code>framing {sf esf}</code> Example: <code>ITP(config)# framing esf</code>	Specifies the framing format for T1.
Step 3	<code>clock source {bits {primary secondary priority} internal line {primary secondary priority}}</code> Example: <code>ITP(config-controller)# clock source bits primary</code>	Specifies the clock source as BITS primary source.
Step 4	<code>linecode {ami b8zs hdb3}</code> Example: <code>ITP(config-controller)# linecode b8zs</code>	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	<code>controller t1 slot/port-adapter-num/port</code> Example: <code>ITP(config)# controller t1 2/0/0</code>	Specifies controller 0 on the SS7 port adapter and enters controller configuration mode.
Step 2	<code>clock source {bits {primary secondary priority} internal line {primary secondary priority}}</code> Example: <code>ITP(config-controller)# clock source bits primary</code>	Specifies controller 0 on the SS7 port adapter as the the primary source of the BITS clock.
Step 3	<code>exit</code> Example: <code>ITP(config-controller)# exit</code>	Exits from controller configuration mode to global configuration mode.
Step 4	<code>controller t1 slot/port-adapter-num/port</code> Example: <code>ITP(config)# controller t1 2/0/1</code>	Specifies controller 1 on the SS7 port adapter and enters controller configuration mode.
Step 5	<code>clock source {bits {primary secondary priority} internal line {primary secondary priority}}</code> Example: <code>ITP(config-controller)# clock source bits secondary 1</code>	Specifies controller 1 on the SS7 port adapter as the first secondary source of the BITS clock.
Step 6	<code>exit</code> Example: <code>ITP(config-controller)# exit</code>	Exits from controller configuration mode to global configuration mode.
Step 7	<code>controller t1 slot/port-adapter-num/port</code> Example: <code>ITP(config)# controller t1 2/0/2</code>	Specifies controller 2 on the SS7 port adapter and enters controller configuration mode.
Step 8	<code>clock source {bits {primary secondary priority} internal line {primary secondary priority}}</code> Example: <code>ITP(config-controller)# clock source internal</code>	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	<code>exit</code> Example: <code>ITP(config-controller)# exit</code>	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	<p>Example:</p> <pre>ITP(config)# interface atm 12/0/0</pre> <p><code>no ip address</code> <code>no ima-group</code> <code>no atm ilmi-keepalive</code> <code>exit</code></p> <p>Example:</p> <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>	<p>Disables IP addressing.</p> <p>Disables inverse multiplexing over ATM (IMA) group.</p> <p>Disables ILMI keepalives.</p> <p>Exits from interface configuration mode to global configuration mode.</p>

	Command	Purpose
Step 3	<pre>interface atm interface-num</pre> <p>Example: ITP(config)# <code>interface atm 12/0/1</code></p>	Specifies ATM interface 12/0/1 and enters interface configuration mode.
Step 4	<pre>clock source {common [interface-num] internal line}</pre> <p>Example: ITP(config-if)# <code>clock source common 0</code></p>	<p>Specifies that this interface will receive the common BITS clock resource.</p> <p>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).</p>

Configuring the Clock Source for the Cisco 2811 Router

Packet voice and video are sensitive to time delays. To prevent mismatches and data slips, you must synchronize data flows to a single source of timing, known as the network clock. When a network clock is configured, the router is externally clocked and passes that clock signal to another slot/port or WAN Interface Card (WIC). Use of a network clock is configured by naming the interface cards that are participating in network clocking, and then selecting a port to act as the source of timing for the network clock. The Cisco 2811 router uses one clock source for the links, even if they're on different WICs.

You configure the port that is the source of timing as the clock source line (default). You need to configure the other ports as clock source internal. The **network-clock-select** command defines which port is the source of timing for the network clock. If the network-clock-select is not configured, then the internal clock of the router is used.

The user can configure a backup clock source using the *priority* variable of the **network-clock-select** command to determine which clock source is used first. They must also configure the port used as a backup clock source as a clock source line.

Configuring the Clock-Source

To configure the clock-source, as either line or internal, perform the following steps:

SUMMARY STEPS

- 1. **enable**
- 2. **configure terminal**
- 3. **controller**
- 4. **clock source**
- 5. **exit**
- 6. **network-clock-participate**
- 7. **network-clock-select priority**
- 8. **show network-clocks**
- 9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: <code>Router> enable</code>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<code>configure terminal</code> Example: <code>Router# configure terminal</code>	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<code>controller {t1 e1} slot/port</code> Example: <code>Router(config)# controller e1 1/0</code>	Enters controller configuration mode on the T1 or E1 controller for the specified slot/port.
Step 4	<code>clock source {line [primary] internal}</code> Example: <code>Router(config-controller)# clock source line</code>	<p>Specifies the source from which the phase-locked loop (PLL) on this port derives its clocking and, if the source is line, whether this port is the primary source. Keywords are as follows:</p> <ul style="list-style-type: none"> • line—Clock recovered from the line's receive data stream. This is the default. • primary—External source to which the port is connected. This option also puts a second port, which is generally connected to the PBX, into looped-time mode. Both ports are configured with line, but only the port connected to the external source is configured with primary. • internal—T1 or E1 controller internal PLL. <p>Note With the default, the clock source does not appear in the show running-config command output. Use the show controllers command to display the current source for a port.</p>
Step 5	<code>exit</code> Example: <code>Router(config-controller)# exit</code>	Exits the current mode.
Step 6	<code>network-clock-participate [slot slot-number wic wic-slot aim aim-slot-number]</code> Example: <code>Router(config)# network-clock-participate wic 0</code> Example: <code>Router(config)# network-clock-participate slot 5</code>	Allows the network module or WIC in the specified slot to use the network clock for its timing. Keywords depend on platform.
Step 7	<code>network-clock-select priority {t1 e1} slot/port</code> Example: <code>Router(config)# network-clock-select 1 e1 0/1</code>	<p>Specifies a slot/port to be used as a timing source for the network clock and the priority level for that port. The source that is given the highest priority is designated the primary source and is used first; if it becomes unavailable, the source with the second-highest priority is used, and so forth. This command is required if the clock source is from the line. The clocking is provided to the AIM, which then provides it to participating slots in the router. Keywords and arguments are as follows:</p> <ul style="list-style-type: none"> • <i>priority</i>—Priority for the clock source (1 is highest priority) • t1 or e1—T1 or E1 ports • <i>slot/port</i>—Slot and port for the controller clock source.

	Command or Action	Purpose
Step 8	show network-clocks	Displays the current chosen clock and the list of all sources of network clocks according to their priority.
	Example: Router# show network-clocks	
Step 9	exit	Exits the current mode.
	Example: Router(config)# exit	

Examples

The following example is the output from a clock source set to **line**:

```
router# show network-clocks
Network Clock Configuration
-----
Priority      Clock Source   Clock State   Clock Type
-----
1            E1 0/3/1      GOOD         E1
10           Backplane     GOOD         PLL

Current Primary Clock Source
-----
Priority      Clock Source   Clock State   Clock Type
-----
1            E1 0/3/1      GOOD         E1
```

The following example is the output from a clock source set to **internal**:

```
router# show network-clocks
Network Clock Configuration
-----
Priority      Clock Source   Clock State   Clock Type
-----
10           Backplane     GOOD         PLL

Current Primary Clock Source
-----
Priority      Clock Source   Clock State   Clock Type
-----
10           Backplane     GOOD         PLL
```

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.

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

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

**Note**

M2PA/SCTP offload is supported on the Cisco 7500 7600 platforms.
When M2PA/SCTP offload is enabled, only a single IP route per destination is allowed.

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

	Command	Purpose
Step 1	<code>cs7 local-peer local-port-number [offload slot bay]</code> Example: ITP(config)# cs7 local-peer 7000 offload 2 0	Specifies the local peer and puts you in local-peer submode. The keyword offload offloads link management of peer links to the VIP specified by the argument <i>slot</i> .
Step 2	<code>local-ip address</code> Example: ITP(config-cs7-lp)# local-ip 172.18.44.242	Configures the IP address for this local peer instance. You can repeat this step to configure backup IP addresses for this local end-point.

Configuring Linksets

**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.

A link is either a serial or ATM interface or a peer (virtual link) to a remote Cisco ITP node. Multiple links are grouped in a linkset. Each link must be assigned to one linkset and multiple links can be assigned to the 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.

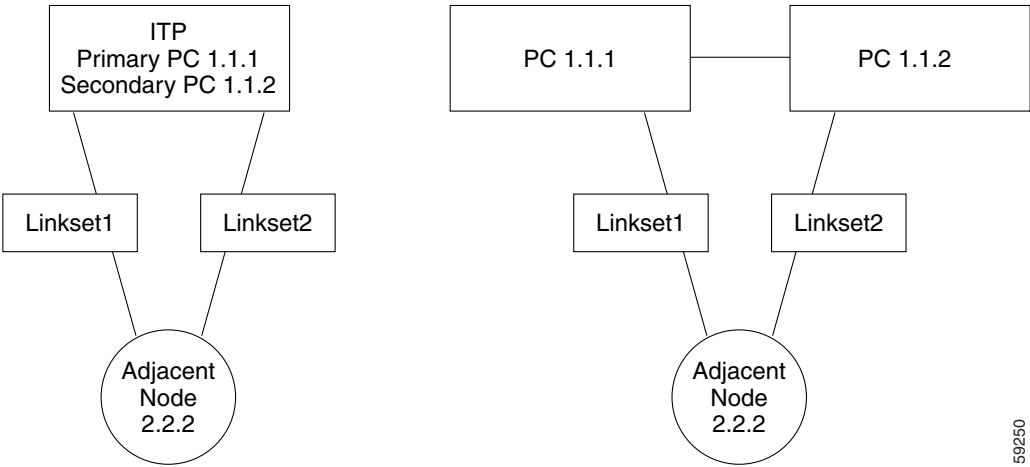
To specify a linkset, use the following command in global configuration mode:

Command	Purpose
<code>cs7 linkset ls-name adjacent-point-code</code> Example: ITP(config)# cs7 linkset LINKSET1 2.2.2	Specifies a linkset to an adjacent node and enters linkset configuration mode. Linkset names are case-specific.

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

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: <code>ITP(config)# cs7 linkset LINKSET1 2.2.2</code> <code>ITP(config-cs7-ls)exit</code> <code>ITP(config)# cs7 linkset LINKSET2 2.2.2</code>	

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 the following 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 that locates a binary version of the route table. To add route table contents, use the following command in route table configuration mode:

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

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 Cisco CS7 route table configuration mode:

Command	Purpose
<code>update route point-code [mask length] linkset ls-name [priority priority-value¹] [qos-class class]</code>	Updates a route in the routing table.
Example: ITP(config-cs7-rt)#	

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, therefore, are 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).

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: ITP(config-cs7-rt)#	

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: ITP(config-cs7-ls)#	

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
<code>link slc atm interface-number[.subinterface-number]</code>	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 <i>slc sctp remote-ip-addr [backup-remote-ip-addr ...] remote-port-num¹ local-port-num [passive]</i>	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 377](#) of the “Verifying, Monitor, and Tuning ITP” chapter.

Shutting Down and Restarting Linksets and Links



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/link.

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

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

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

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

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

Command	Purpose
cs7 linkset <i>ls-name point-code</i>	Specifies a linkset and puts you in linkset configuration mode.
Example: ITP(config)#	
link <i>slc</i> -OR- link <i>slc sctp remote-peer remote-instance local-instance</i> [passive]	Specifies a link and puts you in link configuration mode.
Example: ITP(config-ls)#	
shutdown	Disables the link.
Example: ITP(config-ls-link)# shutdown	
no shutdown	Brings the link back into the active state.
Example: ITP(config-ls-link)#	

Configuration Example of RPR+

In the following example, the active RSP is in slot 2 and the standby RSP is installed in slot 3 of a Cisco 7507 router.

```
ITP# copy tftp slot0:rsp-pv-mz
```

```

ITP# copy tftp slaveslot0:rsp-pv-mz
ITP# configure terminal
ITP(config)# hw-module slot 2 image slot0:rsp-pv-mz
ITP(config)# hw-module slot 3 image slot0:rsp-pv-mz
ITP(config)# redundancy
ITP(config-r)# mode rpr-plus
ITP(config-r)# end
ITP# hw-module sec-cpu reset
ITP# show running-config

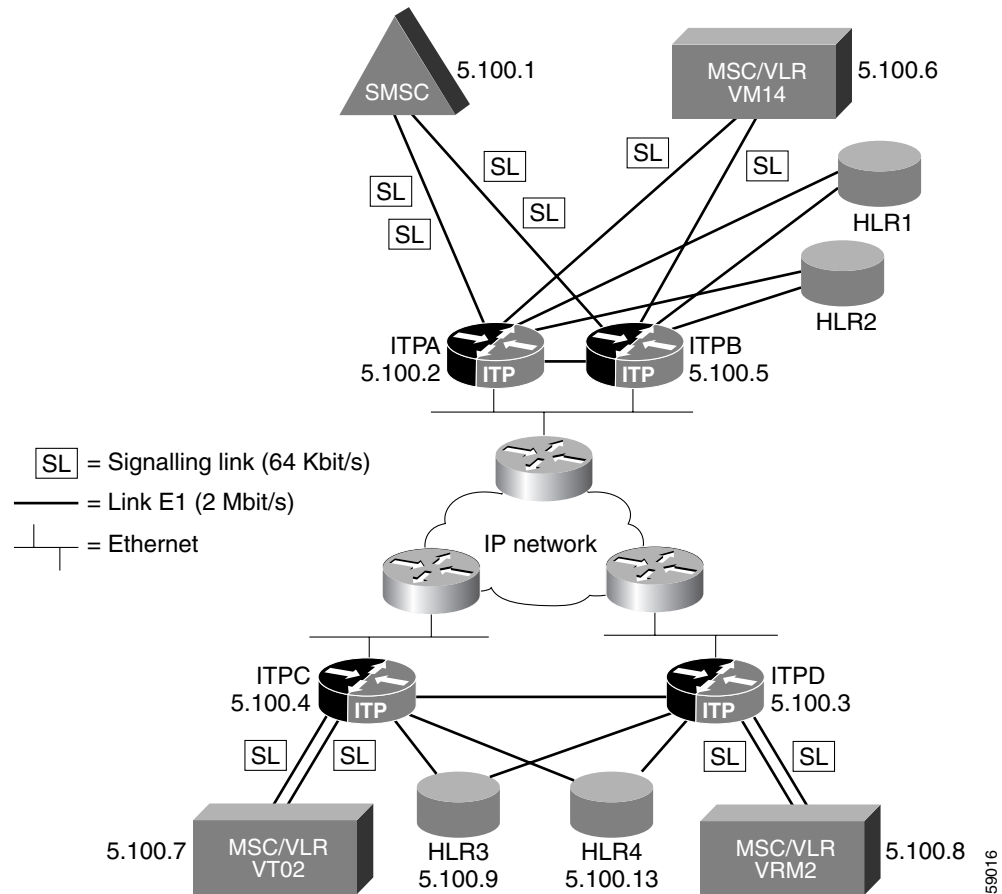
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service single-slot-reload-enable
!
hostname Router1
!
boot system rcp://path/to/image/rsp-boot-mz
boot system tftp://path/to/image/rsp-boot-mz
boot bootldr bootflash:rsp-boot-mz
enable password password
!
redundancy
mode rpr-plus !--indicates Redundancy mode has been configured for RPR+
!
hw-module slot 2 image slot0:rsp-pv-mz
hw-module slot 3 image slot0:rsp-pv-mz
ip subnet-zero
ip rcmd remote-username router1
ip cef distributed
ip host iphost 192.168.0.1
mpls traffic-eng auto-bw timers
!
!
controller T3 6/0/0
clock source line
!
!
interface Ethernet0/0/0
ip address 10.0.0.1 255.255.0.0
no ip directed-broadcast
ip route-cache distributed
no keepalive
.
.
.
exec-timeout 0 0
history size 40
transport preferred none
transport input none
line aux 0
line vty 0 4
login
!end

```


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$AFlH6u2CVGDRM5BMeuGmx/
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 offload 2 0
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$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 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 offload 2 0
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 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 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$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 offload 2 0
    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 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
```

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$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 offload 2 0
    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
```




Multiple Instances and Instance Translation

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

Feature History for Multiple Instances

Release	Modification
12.2(18)IXA	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.



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 112](#)
- [How to Configure Multiple Instances, page 113](#)
- [How to Configure Instance Translation, page 114](#)
- [Verifying the Multiple Instances Configuration, page 119](#)
- [Configuration Example for Multiple Instance, page 119](#)
- [Configuration Examples for Instance Translation, page 120](#)

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 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. 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.

If you enable the Multiple Instances feature, the **instance** keyword and *instance-number* argument are mandatory with the commands listed below:

- **cs7 capability-pc**
- **description (cs7 link)**
- **cs7 display-name**
- **cs7 fast-restart**
- **cs7 gtt address-conversion**
- **cs7 gtt application-group**
- **cs7 gtt concern-pelist**
- **cs7 gtt load**
- **cs7 gtt map**
- **cs7 gtt map sp**
- **cs7 gtt map ss**
- **cs7 gtt replace-db**
- **cs7 gtt selector**
- **cs7 linkset**

- [cs7 mtp3 event-history](#)
- [cs7 mtp3 timer](#)
- [cs7 mtp3 tuning](#)
- [cs7 national-options](#)
- [cs7 network-indicator](#)
- [cs7 network-name](#)
- [cs7 instance pc-conversion](#)
- [cs7 point-code](#)
- [cs7 point-code delimiter](#)
- [cs7 point-code format](#)
- [cs7 qos class](#)
- [cs7 remote-congestion-msgs](#)
- [cs7 route-mgmt-sls](#)
- [cs7 route-table](#)
- [cs7 secondary-pc](#)
- [cs7 sls-shift](#)
- [cs7 summary-routing-exception](#)
- [cs7 tfc-pacing-ratio](#)
- [cs7 variant](#)

How to Configure Instance Translation

This section include the following tasks and information:

- [Configuring Point Code Conversion, page 114](#)
- [Configuring Global Title Conversion, page 115](#)
- [Configuring Instance Conversion After Global Title Translation, page 118](#)

Configuring Point Code Conversion



Note

Conversion from ANSI, ITU, China to TTC variant is not supported. In the case of conversion between ANSI/China/ITU and ANSI/CHINA/ITU, the MSU size will change as a result of the different point codes size. If the conversion causes the MSU size to grow beyond the maximum MSU size of 273 bytes, the MSU is discarded.

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 alias-pc alias-instance 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>	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 pc 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 154 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 115](#)

[Creating a GTI Conversion Table, page 116](#)

[Creating a Subsystem Mapping Table, page 116](#)

[Creating a GTA Prefix Conversion Table, page 117](#)

[Assigning a Conversion Table to an Instance, page 117](#)

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 in a different instance.

- 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 in-ssn in-ssn out-ssn 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 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>]	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.

Command	Purpose
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.

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 ssn ssn cost pcssn</i>	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)#
```

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.

You can also indicate the instance-number in any of the following Privileged EXEC show commands:

- **show cs7 access-lists**
- **show cs7 accounting**
- **show cs7 gtt address-conversion**
- **show cs7 gtt application-group**
- **show cs7 gtt concern-pclist**
- **show cs7 gtt config**
- **show cs7 gtt gta**
- **show cs7 gtt map**
- **show cs7 gtt measurements**
- **show cs7 gtt selector**
- **show cs7 linkset**
- **show cs7 mtp3 event-history**
- **show cs7 mtp3 timers**
- **show cs7 point-codes**
- **show cs7 qos**
- **show cs7 route**

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

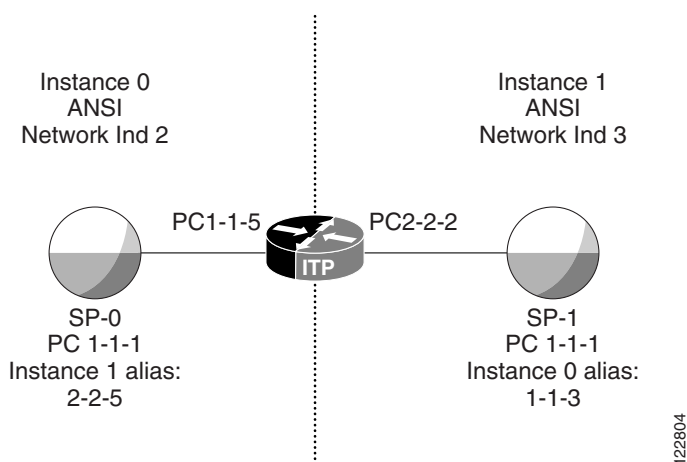
This section includes two examples:

- [Instance Translation: Instances with the Same Variant, page 120](#)
- [Instance Translation: Instances with Different Variants, page 122](#)

Instance Translation: Instances with the Same Variant

The following example configuration is illustrated in [Figure 7](#).

Figure 7 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	aces	1	SP-0	avail

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

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

```
ITP#show cs7 route
```

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

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

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

Destination	Prio	Linkset	Name	Route
1.1.1/24	aces	1	SP-1	avail
2.2.5/24	aces	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: Instances with Different Variants

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 sends any MSUs with unknown point codes in one instance to another instance. Also, any PCs in the MSU that require conversion but do not have an alias point code assigned, will be unchanged in the new instance.

In the following example, MSUs can be sent for any point code from instance 0 to instance 1:

```
cs7 instance 1 pc-conversion default 0
```

The above example will not allow MSUs to be sent from instance 1 to instance 0, however. To only allow MSUs with a DPC of 2.2.4 or 2.2.5 to be sent from instance 1 to instance 0, enter the following commands:

```
cs7 instance 0 pc-conversion 2.2.4 alias-pc 1 2.2.4
cs7 instance 0 pc-conversion 2.2.5 alias-pc 1 2.2.5
```



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(18)IXA	This 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.



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 124](#)
This section describes the functional components of GTT and provides the basic commands to enable them.
- [Storing and Loading GTT Configuration Data, page 127](#)
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.
- [Configuring GTT: 6 Scenarios, page 136](#)
This section describes the specific tasks and commands for configuring GTT, using 6 real-world scenarios.

- [Configuring Global Title Address Conversion, page 154](#)

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 115 of the “[Multiple Instances and Instance Translation](#)” chapter.

- [Verifying Global Title Translations, page 155](#)

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

- [Logging GTT Errors with the ITP Logging Facility, page 157](#)

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

- [Configuration Example for GTT, page 160](#)

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](#)” section on page 136:

- 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 124](#)
- [GTT Global Title Address Entries, page 125](#)
- [GTT Application Groups, page 126](#)
- [GTT Mated Application Entries, page 127](#)

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 selector tt tt gti gti np np	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 9 subsystems per point code in the GTT Mated Application table. (See [GTT Mated Application Entries, page 127.](#))
- 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 can 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] [qos-class qos]	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]	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 share 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.
- A PC/SSN entry cannot be deleted if it is referenced by an entry in the GTA table.
- The primary and backup point-code cannot be identical.
- There is a maximum of 9 subsystems per point-code allowed.
- The PC can not be equal to the node's self PC, capability PC, or secondary PC.

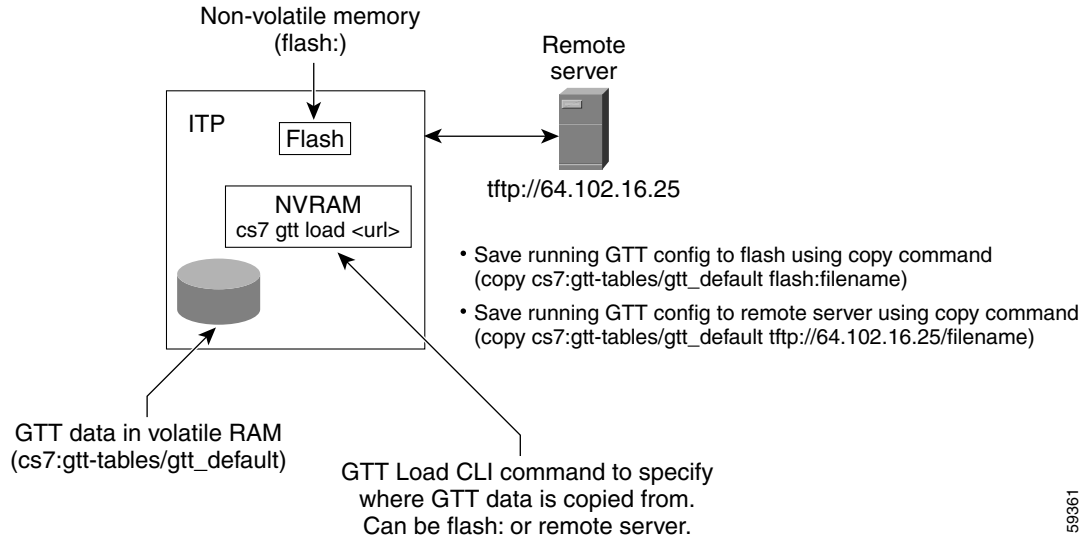
To configure a GTT MAP entry, use the following command in global configuration mode:

Command	Purpose
Router(config)# cs7 gtt map ppc pssn [flags] mult [bpc] [bssn]	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 8](#) 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 128](#)
- [Loading a GTT Table from a Remote File Server or Flash \(Existing GTT Data\), page 129](#)
- [Bulk Loading/Replacing GTT Database, page 129](#)
- [Syntax and Format Rules for Creating a GTT Database Download File, page 129](#)

Figure 8 GTT Table Loading

59361

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 URL	Specify the URL location from which, upon ITP reload, the GTT database will be loaded.

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.

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. 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. Users who require the ability to generate GTT tables offline must use these guidelines to create a syntactically and semantically correct file that may be loaded to the ITP.

Command Identifiers in a GTT Database Download File

Table 3 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 3 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.
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 4](#) lists the current GTT table versions by ITP software version.

Table 4 *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 5](#) lists the values for each parameter of the GTT commands that can be specified in a GTT database download file.

Table 5 *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 4)
<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}

Table 5 GTT Command Parameter Values (continued)

<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]selectorname,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.1]*,*cost,pc,ri*,*[ssn]*

Example:

aapp0, cost, 1, 1012, gt,

- Syntax for version 2.0:

[d]agroup-name,*[mult.1]*,*cost,pc,ri*,*[ssn]*,*[asname]*

Example:

aapp0, cost, 1, , , , as0

- Syntax for version 3.0:

[d]agroup-name,*[mult.1]*,*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.1]*,*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,psnn,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]`

Displaying Current GTT Configuration

Since the GTT data on an ITP is not stored in NVRAM, commands such as **show run** will not display the current configuration. To display the current running configuration regarding GTT use the following command in privileged EXEC mode:

Command	Purpose
Router# show cs7 gtt config	Display the current running configuration of GTT.

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 136](#)
- [Configuring Intermediate GTT To Load Balance MSUs Across Two Or More Point Codes, page 139](#)
- [Configuring Final GTT To Route MSUs to a Solitary Point Code, page 142](#)
- [Configuring Final GTT To Route MSUs to a Primary and Backup Point Code and SSN \(Dominant Mode\), page 145](#)
- [Configuring Final GTT To Load Balance MSUs Across a Group of Point Codes and Subsystems, page 148](#)
- [Configuring Final GTT to an SUA AS with a Backup Point Code \(Dominant Mode\), page 151](#)

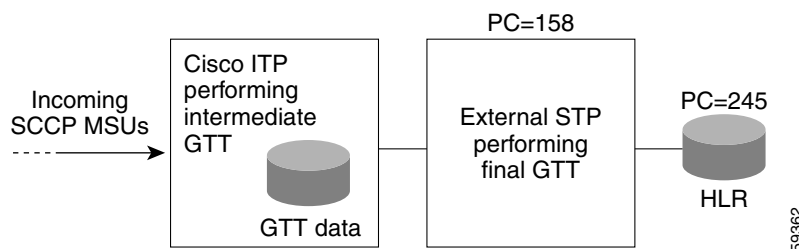
Rules For Removing GTT Configurations:

- 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.
- 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 9](#).

Figure 9 *Intermediate GTT With One Destination*



The ITP on the left side of [Figure 9](#) 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.

For the example, the command and the output would be:

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

```

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

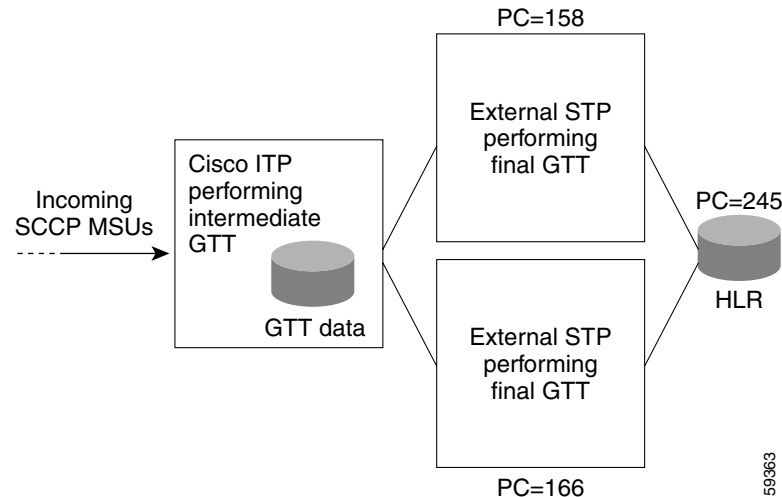
GTA            PC           RI     SSN   TT   App-Grp   QOS   ASname
-----
3330810        158           gt
```

To delete a GTT configuration, follow the rules in the [“Rules For Removing GTT Configurations:”](#) section on page 136.

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

This configuration describes the scenario shown in [Figure 10](#).

Figure 10 *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 10](#) 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 the shared mode, all items in an application group must be given a unique cost (1-8). 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 <i>selector</i>	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.
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

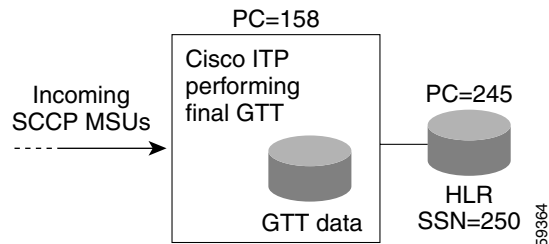
GTA             PC             RI     SSN   TT   App-Grp   QOS   ASname
-----
3330810         158             gt           intergroup1
328
```

To delete a GTT configuration, follow the rules in the [“Rules For Removing GTT Configurations:”](#) section on page 136.

Configuring Final GTT To Route MSUs to a Solitary Point Code

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

Figure 11 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 11](#) 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 selector	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 gta result-type pc routing-indicator ssn ssn	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 6 describes the fields in the **show cs7 gtt map** display.

Table 6 *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**

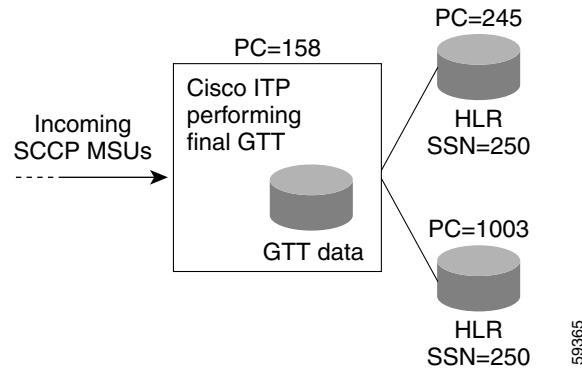
Whenever final GTT is provisioned with an explicit subsystem from a GTA entry such as the one for GTA=3335114, a GTT MAP (Mated Application) entry is required. The ITP will automatically create a solitary MAP as needed when the GTA entry is created. The GTT MAP entry is used internally by the ITP to 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 145](#). 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 136](#).

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 12](#)

Figure 12 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 12](#) 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.

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.

Command	Purpose
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 gta c7gsp
```

```

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

GTA            PC            RI    SSN  TT  App-Grp  QOS  ASname
-----
3330810        158            gt
3335114        245            pcssn 250
328                                intergroup1
339            245            pcssn 250

```

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

```

PPC      PSSN  MULT  BPC      BSSN  ConPCLst  RRC ADJ  Ref
245      250   dom   1003     250           on  no   2

```



Note

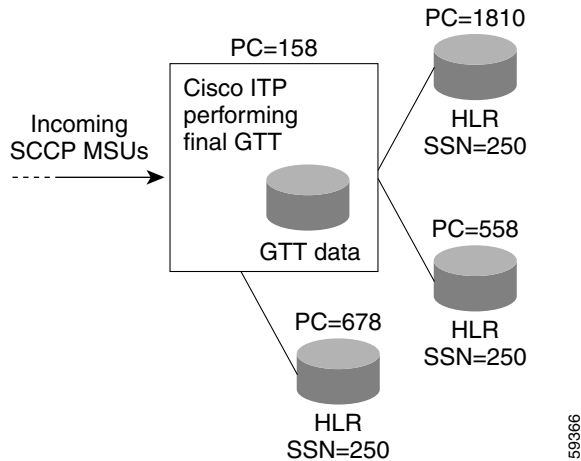
You can not delete any map entry that references another MAP entry. You must first change all entries that reference it to **sol** before you can delete the entry with the **no cs7 gtt map** command. To modify a MAP entry you must replace the entire command, including all keywords and arguments.

To delete a GTT configuration, follow the rules in the [“Rules For Removing GTT Configurations:”](#) section on page 136.

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

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

Figure 13 *Final GTT Load Balanced Across Multiple PC/SSN Nodes*



This example is similar to the example shown in [Figure 10](#) 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 13](#) 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)# 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
```

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

```
Selector Name  TT  GTI  NP  NAI  DFLTQOS  #GTAs
-----
c7gsp          0   4   1   3           5

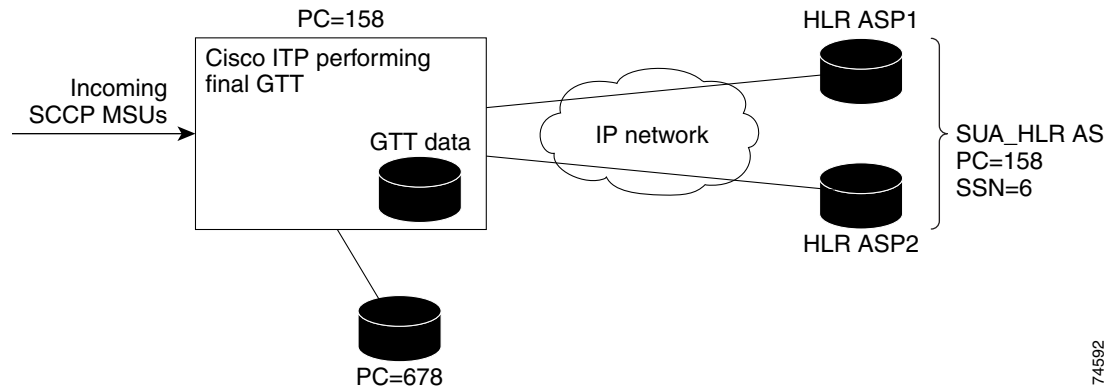
GTA            PC            RI      SSN  TT  App-Grp  QOS  ASname
-----
3330810        158            gt
3335114        245            pcssn  250
328                                intergroup1
339            245            pcssn  250
900                                finalgroup1
```

To delete a GTT configuration, follow the rules in the [“Rules For Removing GTT Configurations:”](#) section on page 136.

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

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

Figure 14 Final GTT to an SUA AS with a Backup PC/SSN in SS7 Network



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 14](#) 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 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 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 submode.

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 cost ssn ssn routing-indicator</i>	Adds an SUA or M3UA AS name to the application group.
Router(config-cs7-gtt-app-grp)# pc <i>point-code ssn ssn cost routing-indicator</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)# 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 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           : 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
```

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

```
Selector Name  TT  GTI  NP  NAI  DFLTQOS  #GTAs
-----
c7gsp          0   4   1   3                5

GTA            PC            RI      SSN  TT  App-Grp      QOS  ASname
-----
3330810        158            gt
3335114        245            pcssn  250
328                                intergroup1
339            245            pcssn  250
900                                finalgroup1
```

To delete a GTT configuration, follow the rules in the [“Rules For Removing GTT Configurations:”](#) section on page 136.

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 115](#) 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.

To define an 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 155](#)
- [SCCP Accounting, page 156](#)
- [Subsystem Status, page 156](#)

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.

SSCP 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 its 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 SSCP application must process SSCP 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 7 on page 158](#) 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 7 lists and describes GTT Errors

Table 7 *GTT Error Log*

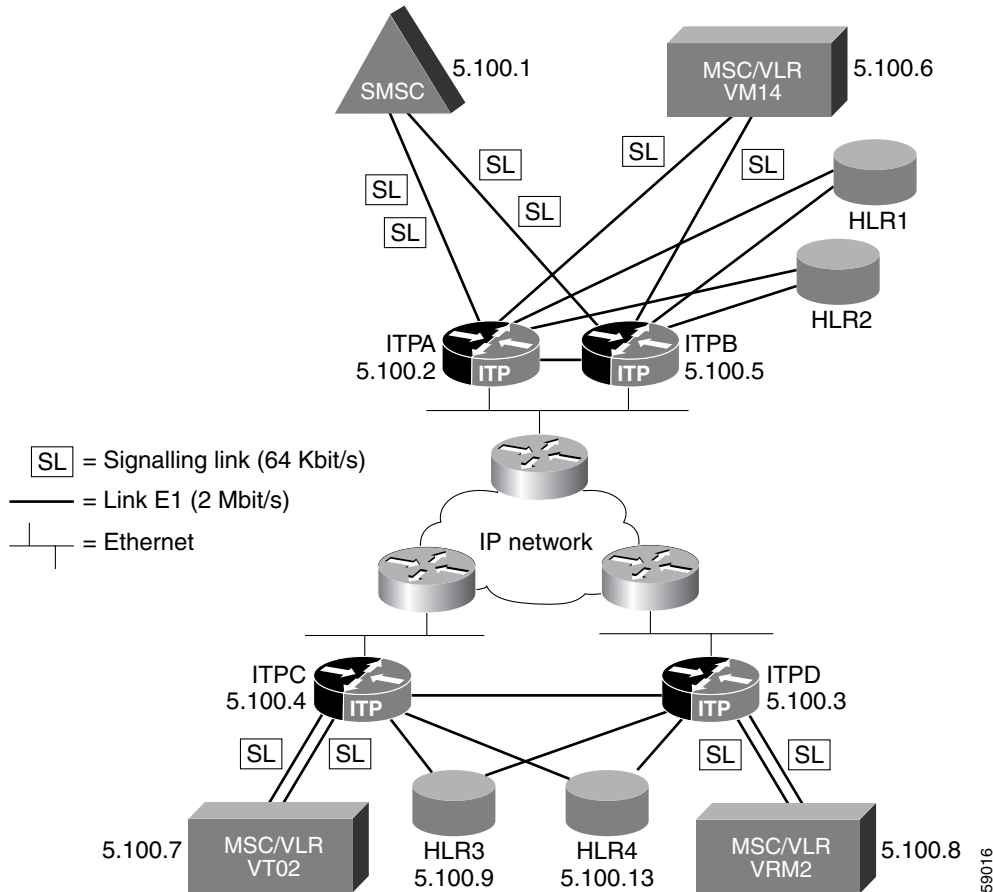
Error Text	Description
CdPA SSN does not exist in GTT MAP Table.	The ITP received an MSU requiring GTT routing for which the SSN in the called party was not configured in the ITP's GTT MAP table.
Translated DPC unavailable.	The ITP received an MSU requiring GTT routing for which the translated DPC in 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.
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.

Table 7 **GTT Error Log (continued)**

Error Text	Description
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.

Configuration Example for GTT

Figure 15 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 15](#).

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

```
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 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
  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 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

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

```

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

```

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(18)IXA	This feature was extended to the IOS software release for ITP on the Cisco 7600 platform.
12.2(18)IXC	Added support for C-Link Backup Routing of M3UA/SUA Traffic

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 172](#)
- [How to Configure Signaling Gateways, page 179](#)
- [ITP Signaling Gateway Configuration Examples, page 185](#)



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.

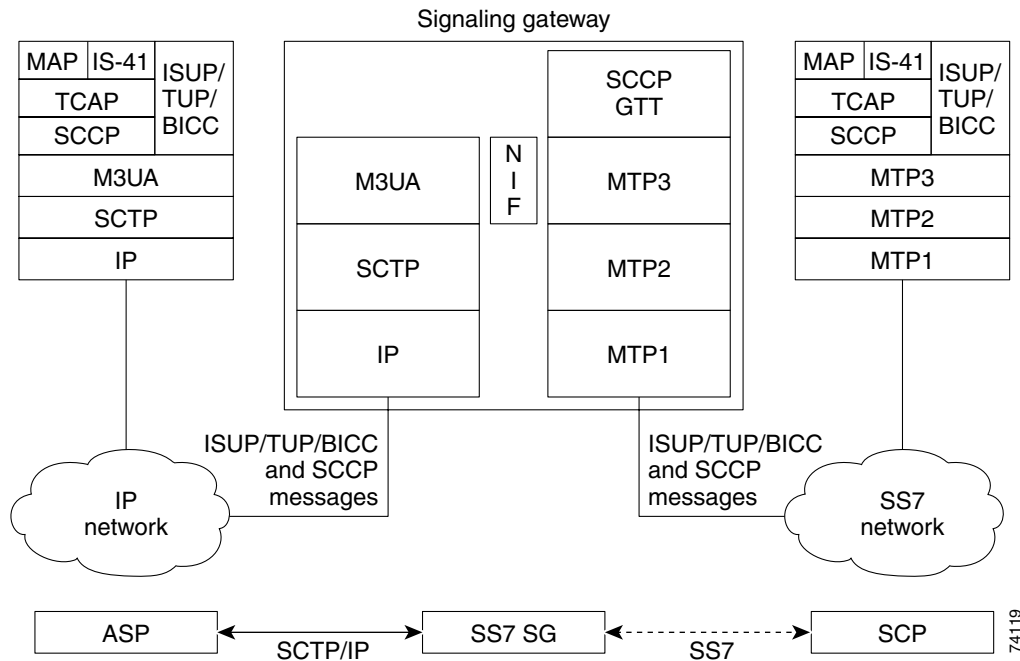
The following sections provide an overview of the main components and features of the Cisco ITP SG:

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 16](#) 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 16 M3UA Signaling Gateway Protocol Stacks

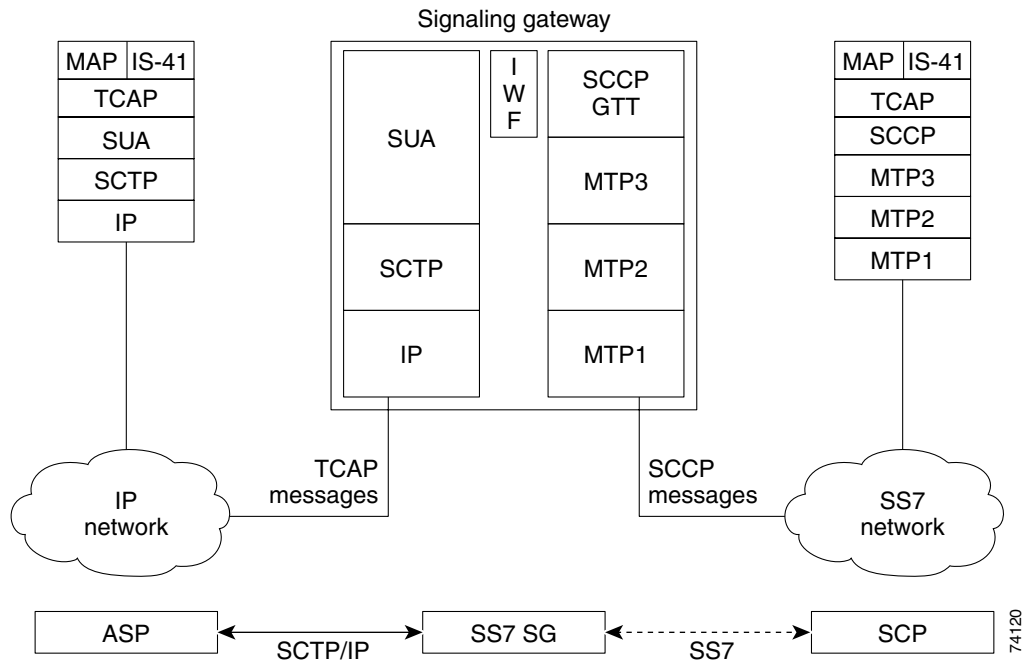
In Figure 16 the legacy SS7 SCP on the far right uses MTP1, MTP2, and MTP3 for transporting SCCP and ISUP messages into the network. The SG terminates the SS7 links, translates the MTP3 messages into M3UA messages, and transports them to the ASP over SCTP/IP. M3UA at the ASP delivers SCCP and ISUP messages.

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 17 depicts the relationship between the legacy SS7 SCP, the SUA SG, the IP-based ASP, and the protocol stacks.

Figure 17 *SUA Signaling Gateway Protocol Stacks*

In Figure 17 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 and Mated SGs

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 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) configured on its mate.

**Note**

C-Link routing takes priority over SGMP routing.

C-Link Backup Routing of M3UA/SUA Traffic

The C-link Backup Routing feature provides backup routing to M3UA and SUA ASs using an MTP3/M2PA linkset to a remote SG serving the same ASs over SCTP/IP. This configurable software feature 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 SGMP 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.

Using an MTP3/M2PA linkset offers improved capacity and redundancy compared to the single SCTP association used by SGMP. Additionally, unlike SGMP, C-link traffic forwarding is completely offloaded on the Cisco 7600 platforms.

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 SGMP, 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 SGMP 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 179](#)
- [Enabling and Disabling M3UA or SUA on the ITP SG, page 180](#)
- [Defining an SG Mated Pair, page 181](#)
- [Defining an Application Server Process \(ASP\), page 182](#)
- [Defining Application Servers \(AS\) and Routing Keys, page 184](#)
- [Enabling M3UA Extended User Part Unavailable \(UPU\) Operation, page 185](#)

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.
Step 5	Router(config)# cs7 point-code delimiter [dot 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 or SUA on the ITP SG

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 <i>local-port-number</i> [offload slot bay]	Specifies a local port for inbound connections and enters CS7 M3UA submode.
Router(config-cs7-m3ua)# local-ip <i>ip-address</i>	Configures a local IP address for use by M3UA. The local-ip <i>ip-address</i> 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 377](#) 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.

Command	Purpose
Router(config)# cs7 m3ua <i>local-port-number</i>	Specifies a local port for inbound connections and enters CS7 M3UA submode.
Router(config-cs7-m3ua)# local-ip <i>ip-address</i>	Configures a local IP address for use by M3UA. The local-ip <i>ip-address</i> 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 377](#) of the “Verifying, Monitor, and Tuning ITP” chapter.

Enabling SUA and SUA SCTP Offload

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. On the 7500 platform, you can use the **offload** keyword to offload SUA SCTP processing to the linecard. This feature increases forwarding performance. When offload is enabled, only a single IP route per destination is allowed.

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
Router(config)# cs7 sua <i>local-port-number</i> [offload <i>slot bay</i>]	Specifies a local port for inbound connections and enters CS7 SUA submode. If offload is enabled, only a single IP route per destination is allowed.
Router(config-cs7-sua)# local-ip <i>ip-address</i>	Configures a local IP address for use by SUA. If you are configuring SUA SCTP offload, the local-ip <i>ip-address</i> must be an IP address that was already configured on the linecard to which you are offloading this SUA instance.

Command	Purpose
Router(config)# cs7 sgmp <i>local-port</i>	Enable SGMP and specify 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</i> <i>remote-port</i> [passive]	Define the mated SG name and remote port number and enable CS7 mated-sg submode. The passive keyword specifies no attempt to initiate the connection to the mate.
Router(config-cs7-mated-sg) remote-ip <i>remote-ip</i>	Specify the remote IP address of the Mate.
Router(config-cs7-mated-sg) qos-class <i>class</i>	Defines the QoS class for the SG mated pair.

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 377](#) of the “Verifying, Monitor, and Tuning ITP” chapter.

**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.

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 <i>si qos-class 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.

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.

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 dpc [opc <i>pc-mask</i>] [si { isup tup sccp }] [[cic <i>cic-min 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 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 <i>msec</i>	Specifies the recovery timeout value, in milliseconds. The valid range is 1 to 2000 msec. The default is 2000 msec.

Command	Purpose
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:

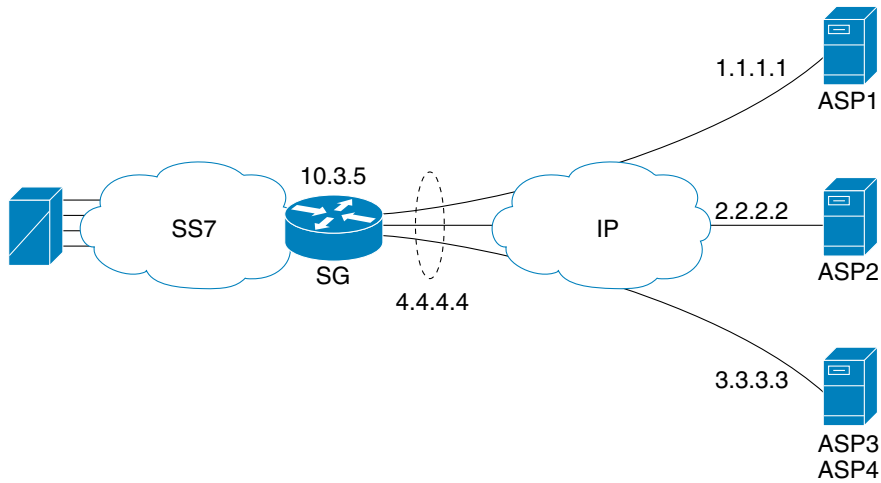
Command	Purpose
ITP(config)# cs7 m3ua extended-upu	Extends M3UA UPU Operation. In all cases, UPU is rate-limited to no more than 1 per second per SI value.

ITP Signaling Gateway Configuration Examples

This section includes examples for the following aspects of ITP SG configuration:

- [M3UA Configuration Example, page 186](#)
- [SUA Configuration Example, page 186](#)
- [ITP Signaling Gateway: ASPs with Unique Point Codes Configuration Example, page 187](#)
- [ITP SG Mated-SG Configuration Example, page 188](#)
- [ITP SG GTT Configuration Example, page 190](#)
- [ITP SG QoS Configuration Examples, page 191](#)

Figure 18 illustrates the M3UA and SUA configuration examples that follow.

Figure 18 **ITP Signaling Gateway**

74459

M3UA Configuration Example

This configuration is illustrated in [Figure 18](#).

```
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 offload 1 1
 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 18](#).

```
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 offload 2 0
 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

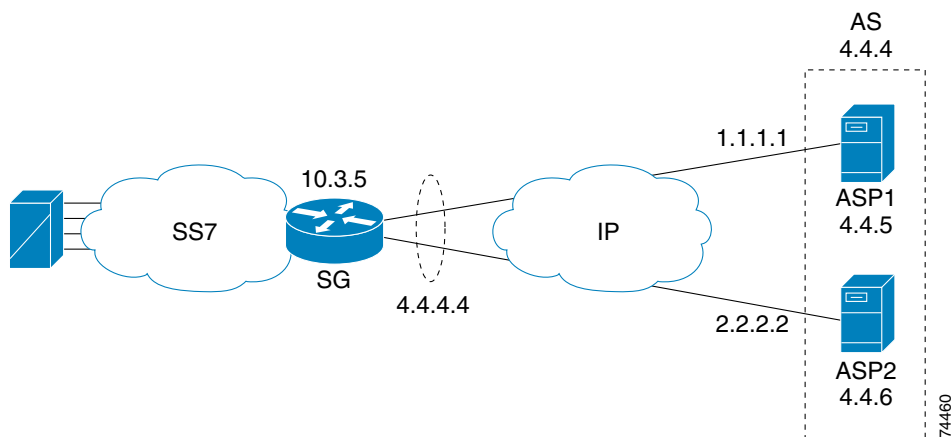
cs7 as BLUE sua
 routing-key 100 10.3.8 ssn 8
 asp ASP1
 asp ASP2
 traffic-mode override

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 19 ITP Signaling Gateway: ASPs with Unique Point Codes



The following configuration example is illustrated in [Figure 19](#).

```

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 offload 1 1

```

```

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

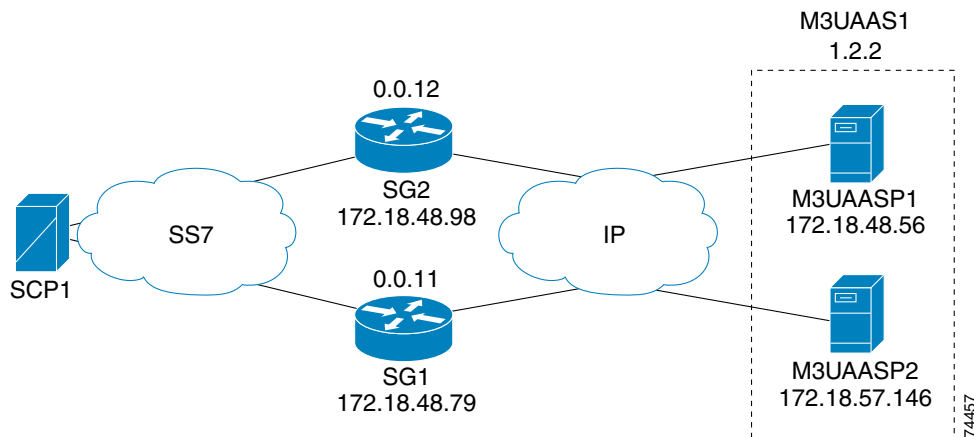
cs7 as ISUPASP1 m3ua
  routing-key 200 4.4.5
  asp ASP1

cs7 as ISUPASP2 m3ua
  routing-key 300 4.4.6
  asp ASP2

```

ITP SG Mated-SG Configuration Example

Figure 20 ITP Signaling Gateway: Mated-SG



The following configuration example is illustrated in [Figure 20](#).

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 offload 1 1
  local-ip 172.18.48.79
!
cs7 sgmp 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:

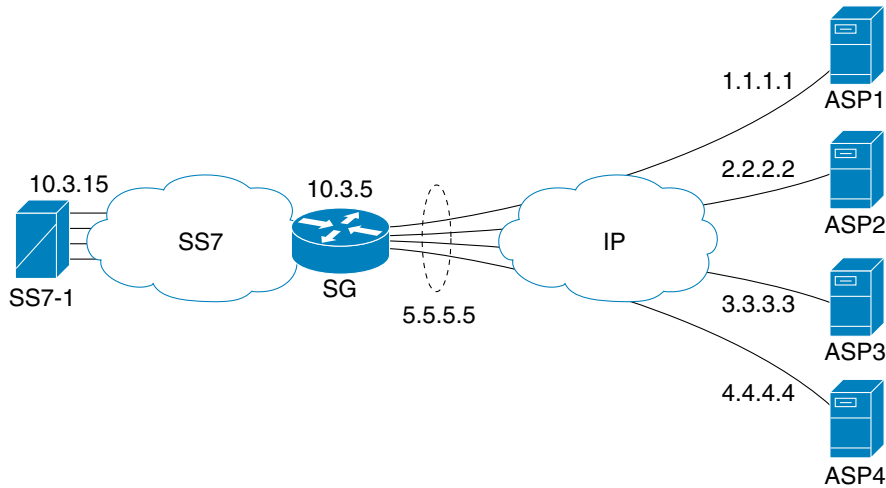
```

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 offload 1 1
    local-ip 172.18.48.98
!
cs7 sgmp 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 21 ITP Signaling Gateway: GTT



74461

The following configuration example is illustrated in [Figure 21](#).

```
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 offload 2 0
 local-ip 5.5.5.5

cs7 m3ua 15000 offload 1 1
 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 offload 1 1
  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 offload 1 1
    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 offload 1 1
    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 307.

```

cs7 qos class 3
    qos-ip-precedence 3
cs7 qos class 5
    qos-ip-dscp 40

```

```
!  
cs7 m3ua 2905 offload 1 1  
    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 ITP Gateway Screening feature (GWS) 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 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
12.2(18)IXA	Extended ITP to the Cisco 7600 platform
12.2(18)IXC	Added support for GWS SCCP error return
12.2(18)IXD	Integrated GWS and MLR triggers

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 GWS, page 196](#)
- [How to Configure GWS, page 210](#)
- [Monitoring GWS, page 223](#)
- [Configuration Examples for GWS, page 227](#)
- [Additional References, page 230](#)

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.

**Note**

On an ITP Cisco 7600 platform, the GSW configuration is downloaded to the FlexWAN and the message logs and statistics are uploaded to the route processor (RP). These operations would be performed after a brief delay (10 seconds at most). For example, when a GWS rule is added, it will not take effect immediately on the FlexWAN. It might take 10 seconds (at most) to transmit that rule to all the FlexWANs.

The following sections provide more detail about GWS:

- [GWS Tables, page 196](#)
- [GWS Table Matching Order for Incoming Packets, page 207](#)

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 8](#) shows an example of an allowed screening table, in this case an allowed opc table:

Table 8 **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 22 shows chained screening tables that screen incoming messages based on Linkset, OPC, and SI. Figure 23 shows chained screening tables that screen incoming messages based on AS, OPC, and SI.

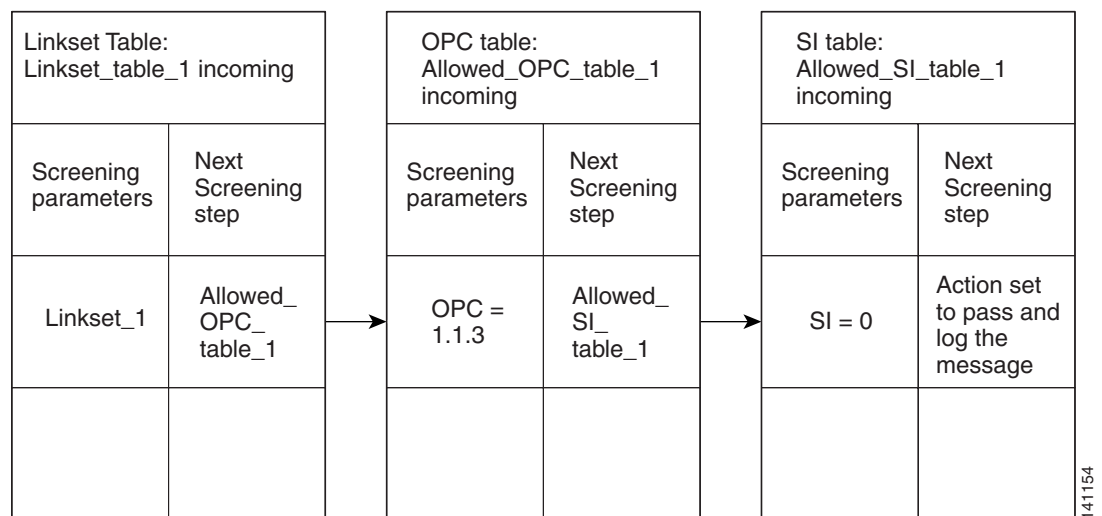
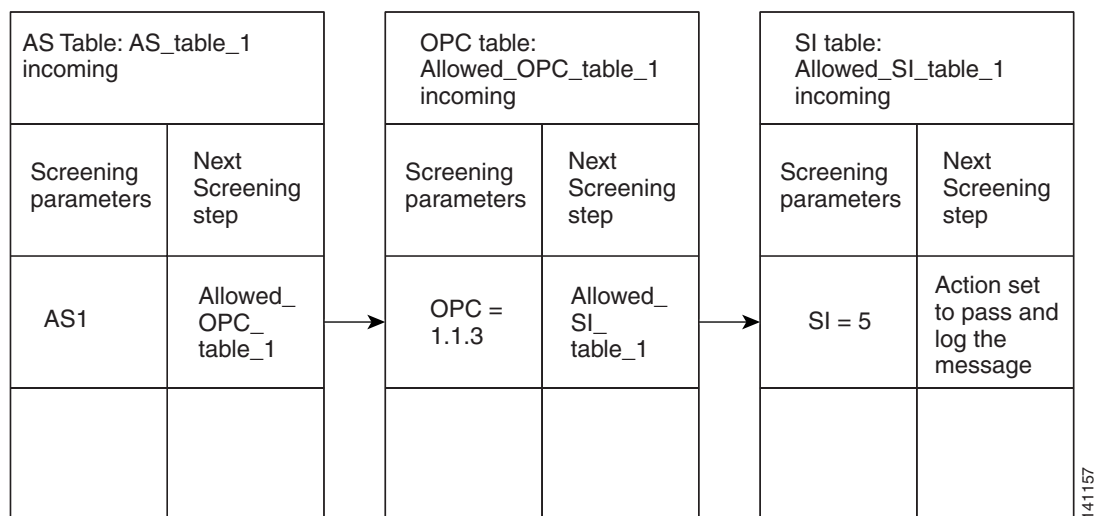
Figure 22 **Chained Screening Tables - MTP****Figure 23** **Chained Screening Tables - xUA**

Table 9, Table 10, and Table 11 list valid GWS screening table types and the valid configuration commands for each type:

Table 9 *MTP Parameters*

Table Type	Description	Screening Commands
aff-dest	Affected destination in MTP management messages.	<ul style="list-style-type: none"> pc-range default
dpc	Destination Point Code	<ul style="list-style-type: none"> pc-range default
mtp-msg-type	MTP message type	<ul style="list-style-type: none"> si mtp-msg-h0 mtp-msg-h1-range si mtp-msg-type default
opc	Originating Point Code	<ul style="list-style-type: none"> pc-range default
sio	SIO Table	<ul style="list-style-type: none"> si default

Table 10 *SCCP Parameters*

Table Type	Description	Screening Commands
aff-pc-ssn	Affected PC-SSN in SCCP management messages <ul style="list-style-type: none"> Affected PC Affected SSN 	<ul style="list-style-type: none"> pc-range ssn default
cdpa-gta-prefix	CdPA GTA Prefix Table <ul style="list-style-type: none"> Minimum Digits Maximum Digits GTA prefix 	<ul style="list-style-type: none"> gta-prefix default
cdpa-gta-range	CdPA GTA Range Table <ul style="list-style-type: none"> GTA range 	<ul style="list-style-type: none"> gta-start default
cdpa-pc-ssn	Called Party Address PC-SSN <ul style="list-style-type: none"> CdPA-SSN CdPA-PC CdPA SCMG format ID 	<ul style="list-style-type: none"> pc-range ssn default

Table 10 **SCCP Parameters (continued)**

Table Type	Description	Screening Commands
cdpa-selector	Called Party Selector <ul style="list-style-type: none"> • TT (Translation Type) • GTI (Global Title Indicator) • NP (Numbering Plan) • NAI (Nature of Address Indicator) 	<ul style="list-style-type: none"> • tt-range • default
cgpa-gta-prefix	CgPA GTA Prefix Table <ul style="list-style-type: none"> • Minimum Digits • Maximum Digits • GTA prefix 	<ul style="list-style-type: none"> • gta-prefix • default
cgpa-gta-range	CgPA GTA Range Table <ul style="list-style-type: none"> • GTA range 	<ul style="list-style-type: none"> • gta-start • default
cgpa-pc-ssn	Calling Party Address PC-SSN <ul style="list-style-type: none"> • CgPA-SSN • CgPA-PC 	<ul style="list-style-type: none"> • pc-range ssn • default
cgpa-selector	Calling Party Selector <ul style="list-style-type: none"> • TT (Translation Type) • GTI (Global Title Indicator) • NP (Numbering Plan) • NAI (Nature of Address Indicator) 	<ul style="list-style-type: none"> • tt-range • default
sccp-msg-hdr	SCCP Header Message Type	<ul style="list-style-type: none"> • sccp-msg • default

Table 11 **ISUP Parameters**

Table Type	Description	Screening Commands
isup-msg-type	ISUP message type (IAM, ACM, etc.)	<ul style="list-style-type: none"> • isup-msg-type • default

Table 12 shows possible next step chained table types given the current table.

Table 12 **Next Step Tables**

Current Table	Possible Next Step Tables
Gateway linkset or AS	<ul style="list-style-type: none"> • Allowed opc • Blocked opc • Allowed sio • Blocked sio • Allowed dpc • Blocked dpc • Action-set to allow block the message
Allowed opc	<ul style="list-style-type: none"> • 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	<p>For default:</p> <ul style="list-style-type: none"> • Allowed sio • Blocked sio • Allowed dpc • Blocked dpc • Allowed cgpa-pc-ssn • Blocked cgpa-pc-ssn <p>For each entry:</p> <ul style="list-style-type: none"> • Action-set to block the message

Table 12 **Next Step Tables (continued)**

Current Table	Possible Next Step Tables
Allowed sio	<ul style="list-style-type: none"> Blocked sio Allowed dpc Blocked dpc <p>If si = 0</p> <ul style="list-style-type: none"> Allowed aff-dest Blocked aff-dest Allowed mtp-msg-type Blocked mtp-msg-type <p>If si = 1 or 2</p> <ul style="list-style-type: none"> Allowed mtp-msg-type Blocked mtp-msg-type <p>If si = 3</p> <ul style="list-style-type: none"> Allowed cgpa-pc-ssn Blocked cgpa-pc-ssn Allowed cdpa-pc-ssn Blocked cdpa-pc-ssn Allowed sccp-msg-hdr Blocked sccp-msg-hdr <p>If si = 5</p> <ul style="list-style-type: none"> Allowed isup-msg-type Blocked isup-msg-type <p>Action-set to allow block message</p>

Table 12 Next Step Tables (continued)

Current Table	Possible Next Step Tables
Blocked sio	<p>For default</p> <ul style="list-style-type: none"> Allowed dpc Blocked dpc <p>If si = 0</p> <ul style="list-style-type: none"> Allowed aff-dest Blocked aff-dest Allowed mtp-msg-type Blocked mtp-msg-type <p>If si = 1 or 2</p> <ul style="list-style-type: none"> Allowed mtp-msg-type Blocked mtp-msg-type <p>If si = 3</p> <ul style="list-style-type: none"> Allowed cgpa-pc-ssn Blocked cgpa-pc-ssn Allowed cdpa-pc-ssn Blocked cdpa-pc-ssn Allowed sccp-msg-hdr Blocked sccp-msg-hdr <p>If si = 5</p> <ul style="list-style-type: none"> Allowed isup-msg-type Blocked isup-msg-type <p>For each entry</p> <ul style="list-style-type: none"> Action-set to block message
Allowed dpc	<ul style="list-style-type: none"> 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 12 *Next Step Tables (continued)*

Current Table	Possible Next Step Tables
Blocked dpc	<p>For default</p> <ul style="list-style-type: none"> • Allowed aff-dest • Blocked aff-dest • Allowed cgpa-pc-ssn • Blocked cgpa-pc-ssn • Allowed isup-msg-type • Blocked isup-msg-type <p>For each entry</p> <ul style="list-style-type: none"> • Action-set to block message
Allowed mtp-msg-type	<ul style="list-style-type: none"> • Blocked mtp-msg-type • Allowed dpc • Blocked dpc • Allowed aff-dest • Blocked aff-dest • Action-set to allow block message
Blocked mtp-msg-type	<p>For default</p> <ul style="list-style-type: none"> • Allowed dpc • Blocked dpc • Allowed aff-dest • Blocked aff-dest <p>For each entry</p> <ul style="list-style-type: none"> • Action-set to block message
Allowed aff-dest	<ul style="list-style-type: none"> • Blocked aff-dest • Action-set to allow block message
Blocked aff-dest	<p>For default</p> <ul style="list-style-type: none"> • No table allowed <p>For each entry</p> <ul style="list-style-type: none"> • Action-set to block message

Table 12 **Next Step Tables (continued)**

Current Table	Possible Next Step Tables
Allowed cgpa-pc-ssn	<ul style="list-style-type: none"> 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	<p>For default</p> <ul style="list-style-type: none"> Allowed sccp-msg-hdr Blocked sccp-msg-hdr Allowed cgpa-selector Blocked cgpa-selector Allowed cdpa-pc-ssn Blocked cdpa-pc-ssn <p>For each entry</p> <ul style="list-style-type: none"> Action-set to block message
Allowed sccp-msg-hdr	<ul style="list-style-type: none"> 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	<p>For default</p> <ul style="list-style-type: none"> Allowed cgpa-selector Blocked cgpa-selector Allowed cdpa-pc-ssn Blocked cdpa-pc-ssn <p>For each entry</p> <ul style="list-style-type: none"> Action-set to block message

Table 12 **Next Step Tables (continued)**

Current Table	Possible Next Step Tables
Allowed cgpa-selector	<ul style="list-style-type: none"> Blocked cgpa-selector Allowed cdpa-pc-ssn Blocked cdpa-pc-ssn Allowed cgpa-digit-screening Blocked cgpa-digit-screening Allowed cgpa-gta-prefix Blocked cgpa-gta-prefix Action-set to allow block message
Blocked cgpa-selector	<p>For default</p> <ul style="list-style-type: none"> Allowed cdpa-pc-ssn Blocked cdpa-pc-ssn Allowed cgpa-digit-screening Blocked cgpa-digit-screening Allowed cgpa-gta-prefix Blocked cgpa-gta-prefix <p>For each entry</p> <ul style="list-style-type: none"> Action-set to block message
Allowed cgpa-gta-range	<ul style="list-style-type: none"> Blocked cgpa-digit-screening Allowed cdpa-pc-ssn Blocked cdpa-pc-ssn Action-set to allow block message
Allowed cgpa-gta-prefix	<ul style="list-style-type: none"> Blocked cgpa-gta-prefix Allowed cdpa-pc-ssn Blocked cdpa-pc-ssn Action-set to allow block message
Blocked cgpa-gta-range	<p>For default</p> <ul style="list-style-type: none"> Allowed cdpa-pc-ssn Blocked cdpa-pc-ssn <p>For each entry</p> <ul style="list-style-type: none"> Action-set to block message
Blocked cgpa-gta-prefix	<p>For default</p> <ul style="list-style-type: none"> Allowed cdpa-pc-ssn Blocked cdpa-pc-ssn <p>For each entry</p> <ul style="list-style-type: none"> Action-set to block message

Table 12 **Next Step Tables (continued)**

Current Table	Possible Next Step Tables
Allowed cdpa-pc-ssn	<ul style="list-style-type: none"> 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	<p>For default</p> <ul style="list-style-type: none"> Allowed cdpa-selector Blocked cdpa-selector Allowed aff-pc-ssn (if SSN = 1) Blocked aff-pc-ssn (if SSN = 1) <p>For each entry</p> <ul style="list-style-type: none"> Action-set to block message
Allowed cdpa-selector	<ul style="list-style-type: none"> 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	<p>For default</p> <ul style="list-style-type: none"> Allowed cdpa-gta-range Blocked cdpa-gta-range Allowed cdpa-gta-prefix Blocked cdpa-gta-prefix <p>For each entry</p> <ul style="list-style-type: none"> Action-set to block message
Allowed cdpa-gta-range	<ul style="list-style-type: none"> Blocked cdpa-gta-range Action-set to allow block message
Allowed cdpa-gta-prefix	<ul style="list-style-type: none"> Blocked cdpa-gta-range Blocked cdpa-gta-prefix Action-set to allow block message
Blocked cdpa-gta-range	<p>For default</p> <ul style="list-style-type: none"> No table allowed <p>For each entry</p> <ul style="list-style-type: none"> Action-set to block message

Table 12 *Next Step Tables (continued)*

Current Table	Possible Next Step Tables
Blocked cdpa-gta-prefix	For default <ul style="list-style-type: none"> No table allowed For each entry <ul style="list-style-type: none"> Action-set to block message
Allowed aff-pc-ssn	<ul style="list-style-type: none"> Blocked aff-pc-ssn Action-set to allow block message
Blocked aff-pc-ssn	For default <ul style="list-style-type: none"> No table allowed For each entry <ul style="list-style-type: none"> Action-set to block message
Allowed isup-msg-type	<ul style="list-style-type: none"> Blocked isup-msg-type Action-set to allow block message
Blocked isup-msg-type	For default <ul style="list-style-type: none"> No table allowed For each entry <ul style="list-style-type: none"> 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 267.

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 24](#) illustrates outgoing message processing with ACL, GWS, TTMAPPING. [Figure 25](#) illustrates incoming messages and including MLR routing processing through GWS.

Figure 24 *Outgoing Message Processing with ACS, GWS, TTMAPPING*

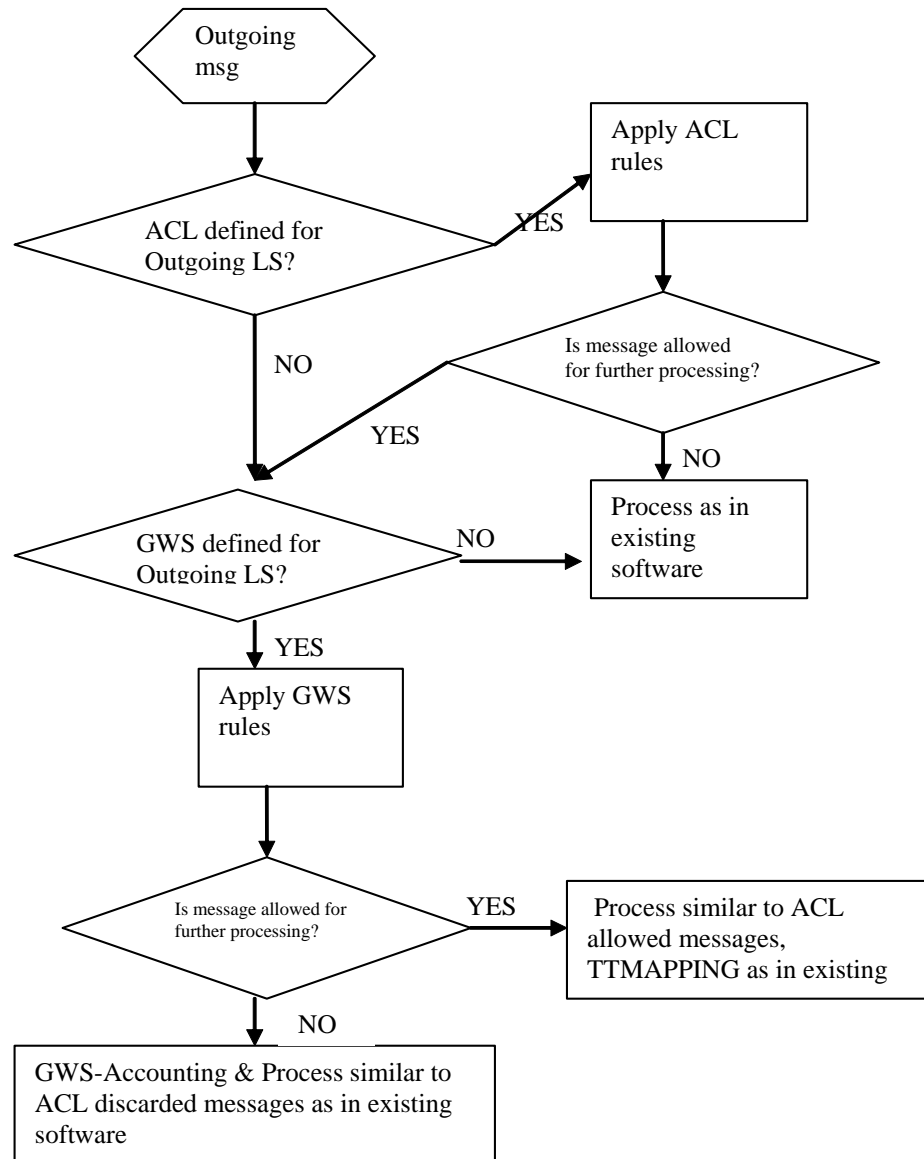
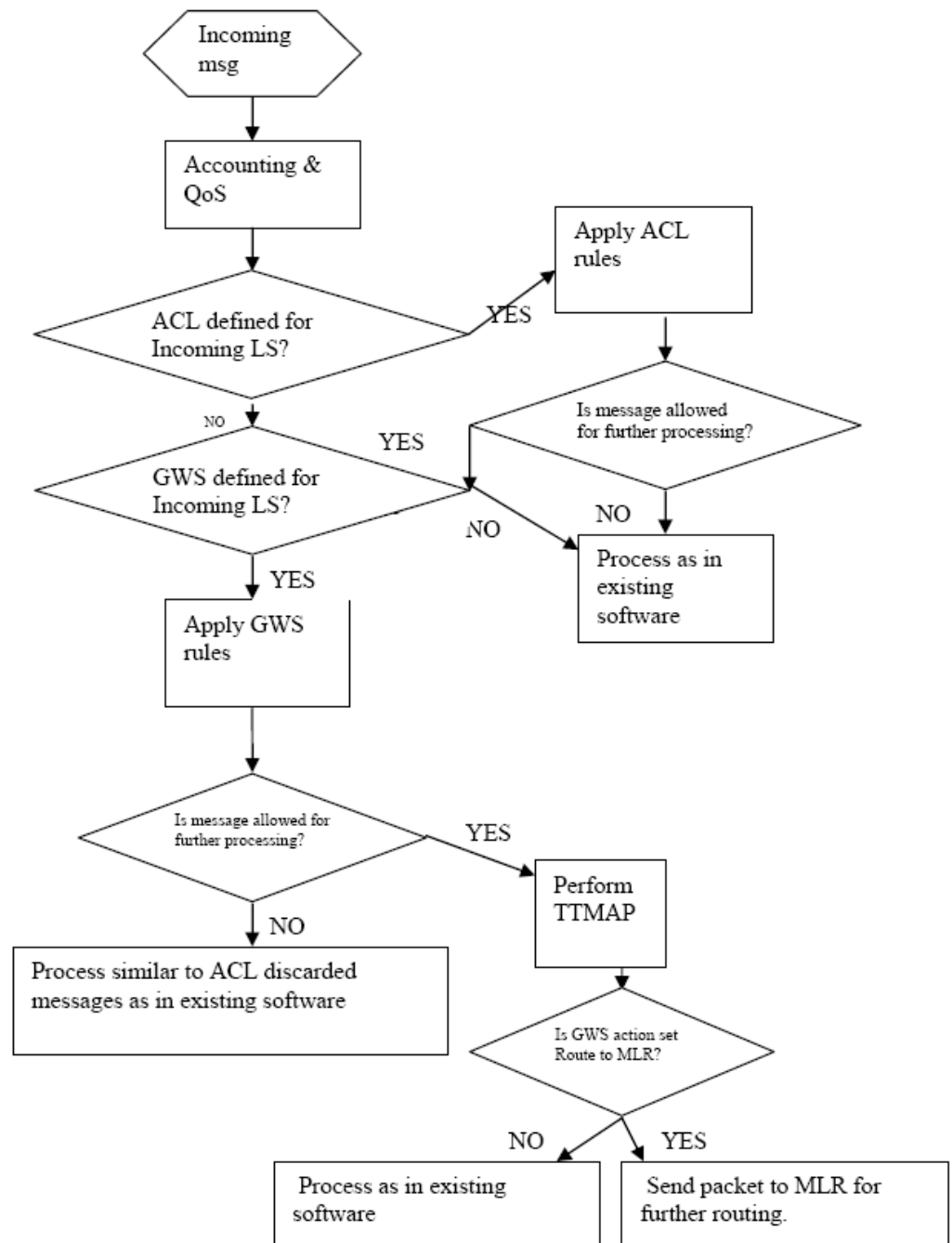


Figure 25 **Processing of Incoming Messages**

How to Configure GWS

This section describes how to configure basic GWS and enhanced GWS. You configure GWS by defining an access list and applying it to a linkset definition. Enhanced GWS adds additional intelligence to message screening. It supports linksets, ASes, and existing screening and routing features, including access lists and Global Title Translation.

Enhanced GWS can also return a UDTs to the source of the SCCP packet when the SCCP packet is dropped. You configure a return UDTs when you define the GWS action set in enhanced GWS.

- [Configuring Basic GWS with Access Lists](#)
- [Configuring Enhanced GWS](#)

Configuring Basic GWS with Access Lists

Basic 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.

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> aftp <i>point-code wildcard-mask</i> cdpa <i>point-code wildcard-mask</i> cgpa <i>point-code wildcard-mask</i> selector all] 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 to_morehead 1.1.1	Specifies a linkset and enters linkset configuration mode.
Step 5	access-group {2700-2999 name} [in out] Example: ITP(config-cs7-ls)# access-group 2703 in	Applies the access list to the linkset.

What to Do Next

If appropriate for your configuration, define GWS action sets.

Defining GWS Action Sets

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `cs7 [instance n] gws default`
4. `[inbound] result nextStep`
5. `[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]}]`
6. `disable-mlr`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: <code>ITP> enable</code>	Enables privileged EXEC mode.
Step 2	<code>configure terminal</code> Example: <code>ITP# configure terminal</code>	Enters global configuration mode.
Step 3	<code>cs7 [instance n] gws default</code> Example: <code>Router(config)# cs7 gws default</code>	Applies globally to all link sets, all ASs, and all local applications in the CS7 instance.
Step 4	<code>[inbound] result <i>nextStep</i></code> Example: <code>Router(config-gws-default)# inbound result <i>nextStep</i></code>	<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.

Command or Action	Purpose
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> <p>Example: Router(config)# cs7 instance 0 gws action-set mlr ruleset GWS_MLR_RULE</p>	<p>Configures a GWS action-set.</p> <p>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.</p> <p>Note GWS action sets are instance based.</p> <p>mlr {ruleset <rule-set-name> group <result-group-name>}—(Optional) keyword allows the screened packet to be processed for routing by MLR.</p>
Step 6 <pre>disable-mlr</pre> <p>Example: ITP(cfg-cs7-mlr-options)# disable-mlr</p>	<p>(Optional) Disables all MLR routing for the specified instance.</p>

**Note**

For more information on the integration of MLR and GWS, see the “[Define the MLR Triggers with GWS](#)” section on page 266. To enable MLR, perform the configuration tasks described in the following sections of the [MLR Routing and Screening](#) chapter: [Define MLR Global Options](#), page 234, [Define the MLR Group](#), page 235, and [Defining the MLR Modify-Profile](#), page 238

Table 13 shows SCCP parameters.

Table 13 **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)
0X0A	Destination cannot perform reassembly (applicable only to XUDT and XUDTS)
0X0B	SCCP failure (only ITU)

Table 13 **UDTS Return Cause Values**

Value (hex)	Description
0x0C	SCCP Hop counter violation (applicable only to XUDT and XUDTS)
0x0D (ITU)	Segmentation not supported
0x0E (ITU)	Segmentation failure
0x0F to 0x0FF (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)

What to Do Next

Define GWS tables.

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 table-name type table-type [action allowed blocked] [gtt pregtt postgtt] Example: ITP(cfg-cs7-mlr-options)# cs7 instance 0 gws table cdpa-sel type 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 . <ul style="list-style-type: none"> • type cdpa_selector—(Optional) defines the table type as CdPA. CdPA is the SCCP Called Party Address field. <ul style="list-style-type: none"> – 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 cdpa_selector. • type sio—(Optional) specifies a service indicator in a table type sio. The following service indicator types are available: <ul style="list-style-type: none"> – 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

What to Do Next

Define entries in GWS tables.

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 12](#).



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.

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 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 14 .
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 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 14 .
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
<pre>si si [priority-range priority-start [priority-end]] result {action action-set-name table tablename}</pre> <p>Example: ITP(config-gws-sio-table)# si sccp result table PCSSN1</p>	Valid for the following table types: sio
<pre>tt-range tt-start [tt-end] [gti gti [np np nai nai]] result {action action-set-name table tablename}</pre> <p>Example: ITP(config-gws-cdpa-sel-table)# tt-range 5 10 gti 2 result table PGTA1</p>	<p>Valid for the following table types: cgpa-selector, cdpa-selector</p> <p>The gti gti parameter may only be specified if the variant is ITU.</p> <p>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 15.</p>

A wildcard indicator (*) can be used to indicate a range of point codes, as shown in [Table 14](#).

Table 14 *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 15](#).

Table 15 *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*] **gws linkset name** *ls-name*
4. **inbound** [**logging type** {**allow** | **block** | **both**} [**test**] {**silent** | **file** [**verbose**] | **console** [**verbose**] | **file** [**verbose**] **console** [**verbose**]}] **result** {**action** *action-set-name* | **table** *tablename*}
5. **outbound** [**logging type** {**allow** | **block** | **both**} [**test**] {**silent** | **file** [**verbose**] | **console** [**verbose**] | **file** [**verbose**] **console** [**verbose**]}] **result** {**action** *action-set-name* | **table** *tablename*}
6. **exit**
7. **cs7** [*instance instance*] **gws linkset default**
8. **inbound** [**logging type** {**allow** | **block** | **both**} [**test**] {**silent** | **file** [**verbose**] | **console** [**verbose**] | **file** [**verbose**] **console** [**verbose**]}] **result** {**action** *action-set-name* | **table** *tablename*}
9. **outbound** [**logging type** {**allow** | **block** | **both**} [**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 instance-number] gws linkset name ls-name 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.
Step 4	inbound [logging type {allow block both} [test] {silent file [verbose] console [verbose] file [verbose] console [verbose]}] result {action action-set-name table tablename} Example: ITP(config-gws-ls)# inbound result table allowed-dpcl	Specifies the inbound screening result on the linkset.
Step 5	outbound [logging type {allow block both} [test] {silent file [verbose] console [verbose] file [verbose] console [verbose]}] result {action action-set-name table tablename} Example: ITP(config-gws-ls)# outbound result action ALLOW	Specifies outbound screening result on the linkset.
Step 6	exit Example: ITP(config-gws-ls)# exit	Exits gateway linkset configuration mode and enables global configuration mode.
Step 7	cs7 [instance instance-number] gws linkset default 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 8	<pre>inbound [logging type {allow block both} [test] {silent file [verbose] console [verbose] file [verbose] console [verbose]}} result {action action-set-name table tablename}</pre> <p>Example: ITP(config-gws-ls)# inbound result action blocked-ver</p>	Specifies default inbound screening.
Step 9	<pre>outbound [logging type {allow block both} [test] {silent file [verbose] console [verbose] file [verbose] console [verbose]}} result {action action-set-name table tablename}</pre> <p>Example: ITP(config-gws-ls)# outbound result action blocked-ver</p>	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*] as name *as-name***
4. **inbound [logging type {allow | block | both} [test] {silent | file [verbose] | console [verbose] | file [verbose] console [verbose]}} result {action *action-set-name* | table *tablename*}**
5. **outbound [logging type {allow | block | both} [test] {silent | file [verbose] | console [verbose] | file [verbose] console [verbose]}} result {action *action-set-name* | table *tablename*}**
6. **exit**
7. **cs7 [instance *instance*] as default**
8. **inbound [logging type {allow | block | both} [test] {silent | file [verbose] | console [verbose] | file [verbose] console [verbose]}} result {action *action-set-name* | table *tablename*}**
9. **outbound [logging type {allow | block | both} [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 instance-number] gws as name as-name 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 {allow block both} [test] {silent file [verbose] console [verbose] file [verbose] console [verbose]}] result {action action-set-name table tablename} Example: ITP(config-gws-as)# inbound result action ALLOW	Specifies the inbound screening result for the AS,.
Step 5	outbound [logging type {allow block both} [test] {silent file [verbose] console [verbose] file [verbose] console [verbose]}] result {action action-set-name table tablename} Example: ITP(config-gws-as)# outbound result action ALLOW	Specifies the outbound screening result for the AS
Step 6	exit Example: ITP(config)# exit	Exits gws AS configuration mode and enables global configuration mode.
Step 7	cs7 [instance instance-number] gws as default Example: ITP(config)# cs7 instance 0 gws as default	Defines the AS table default entry.

	Command or Action	Purpose
Step 8	<pre>inbound [logging type {allow block both} [test] {silent file [verbose] console [verbose] file [verbose] console [verbose]]} result {action action-set-name table tablename}</pre> <p>Example: ITP(config-gws-as)# inbound logging type block file console verbose result table SIO0</p>	Specifies default inbound screening for the AS.
Step 9	<pre>outbound [logging type {allow block both} [test] {silent file [verbose] console [verbose] file [verbose] console [verbose]]} result {action action-set-name table tablename}</pre> <p>Example: ITP(config-gws-as)# outbound result action BLOCK</p>	Specifies default outbound screening for the AS.
Step 10	<pre>exit</pre> <p>Example: ITP(config)# exit</p>	Exits gws AS configuration mode and enables global configuration mode.

What to Do Next

Perform monitoring tasks as needed.

Monitoring GWS

- [Message Logging, page 223](#)
- [Verifying GWS Configuration, page 226](#)

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. 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}**

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} 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**]

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 as	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.

Configuration Examples for GWS

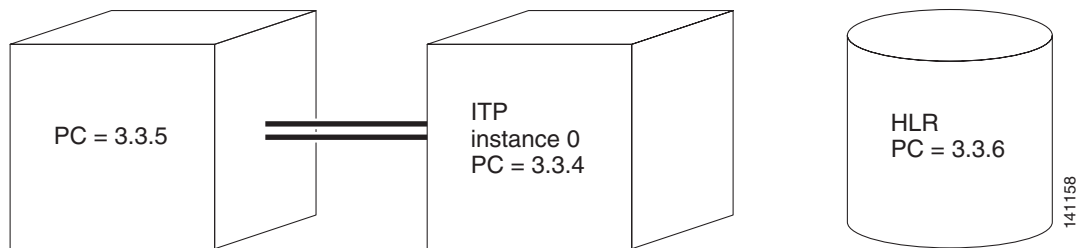
This section provides configuration examples of GWS in the following scenarios:

- [GWS Scenario: Linkset with Allowed DPC, page 227](#)
- [GWS Scenario: XUA AS with Allowed DPC, page 228](#)
- [GWS Scenario with CgPA, CdPA, page 229](#)

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 26 *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

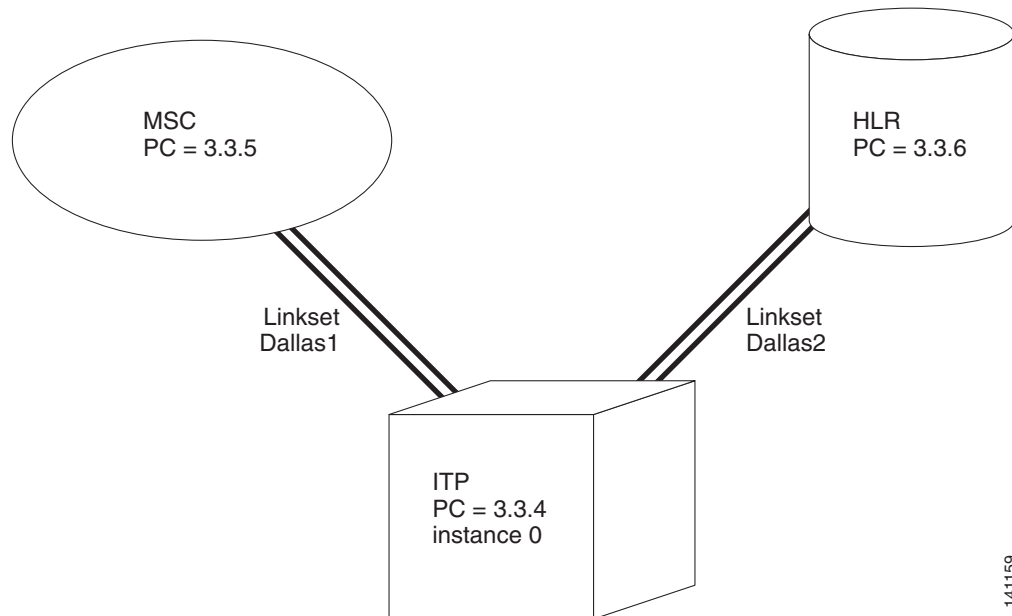
! Define the gateway AS table default entry
cs7 in 0 gws as default
  inbound result action-set blocked-ver
cs7 in 0 gws as default
  outbound result action-set blocked-ver

```


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 27 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 Multi-Layer SMS Routing

Release	Modification
12.(18)IX	Introduced feature
12.2(18)IXA	Added the MLR Call Tracing feature
12.2(18)IXB	<ul style="list-style-type: none">Extended MAP operation support to include all GSM-MAP (3GPP TS 29.002 version 5.9.0 Release 5) operations in MLR rules (Table 20 and Table 21)The protocol keywords gsm map and ansi-41 were added to the rule commandAdded global option to insert DPC into the cdPa point code for packets that are MLR-routed
12.2(18)IXC	<ul style="list-style-type: none">Added support for SCCP/MAP address modification for SRI-SM messagesAdded MLR global option modify-failureAdded MLR global option preserve-opcAdded support to return UDTs if MLR rule or MLR address table blocks a SCCP packet
12.2(18)IXD	<ul style="list-style-type: none">Integrated GWS and MLR triggersSMS MO proxy capability extended to the Cisco 7600

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 234](#)
- [How to Configure MLR-Based Screening, page 269](#)
- [Verifying and Monitoring Multi Layer SMS Routing, page 274](#)
- [Configuration Examples of Multi-layer SMS Routing, page 276](#)

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 Multi-layer SMS Rulesets” section on page 250](#).

For ITU TCAP and GSM-MAP, MLR supports routing on the following operations (See [Table 22](#)):

- 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 16 describes the Multi-layer routing trigger types and their function.

Table 16 **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 Multi-layer SMS routing, 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 Multi-Layer SMS routing feature, perform the configuration tasks described in the following sections:

- [Define MLR Global Options, page 234](#)
- [Define the MLR Group, page 235](#)
- [Defining the MLR Modify-Profile, page 238](#)
- [Creating and Managing Address Tables, page 242 \(Optional\)](#)
- [Define One or More Multi-layer SMS Rulesets, page 250](#)
- [Define the MLR Triggers, page 266](#)

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	<code>enable</code> Example: <code>ITP> enable</code>	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	<code>configure {terminal memory network}</code> Example: <code>ITP# configure terminal</code>	Enters global configuration mode.
Step 3	<code>cs7 [instance instance-number] mlr options</code> Example: <code>ITP(config)# cs7 instance 1 mlr options</code>	(Optional) Specifies an MLR result option command and enables the CS7 MLR options configuration mode.
Step 4	<code>insert-dpc-in-cdpa</code> Example: <code>ITP(cfg-cs7-mlr-options)# insert-dpc-in-cdpa</code>	(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	<code>preserve-opc</code> Example: <code>ITP(cfg-cs7-mlr-options)# preserve-opc</code>	(Optional) Preserves the original originating point code (OPC) when an MLR result is selected in this instance.
Step 6	<code>modify-failure {discard resume sccp-error sccp-error}</code> Example: <code>ITP(cfg-cs7-mlr-options)# modify failure resume</code>	(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	<code>disable-mlr</code> Example: <code>ITP(cfg-cs7-mlr-options)# disable-mlr</code>	(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 destinations 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 Multi-Layer SMS Routing 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. Congested resources are used only if no available, non-congested destinations exist.

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. However, DMSR does not currently support asname results within an SMS result group, so DMSR can reference only MLR groups that contain no asname results.

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. **pc** *dest-pc* [**ssn** *ssn*] [**order** *order*] [**weight** *weight*]
7. **unavailable-routing** {*discard* | *resume*}

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.

	Command or Action	Purpose
Step 2	<pre>configure {terminal memory network}</pre> <p>Example: ITP# configure terminal</p>	Enters global configuration mode.
Step 3	<pre>cs7 [instance instance-number] mlr result name [protocol {gsm-map ansi41}] [mode {wrr dest-sme-binding}]</pre> <p>Example: ITP(config)# cs7 mlr result VAS-GRP</p>	Specifies an MLR result group command and enables the MLR results configuration mode.
Step 4	<pre>asname as-name [order order] [weight weight]</pre> <p>Example: ITP(cfg-cs7-mlr-result)# asname VOTING-AS1 weight 1</p>	<p>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.</p> <ul style="list-style-type: none"> • order order 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 weight 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.
Step 5	<pre>gt addr-string [tt tt [gti gti] [np np nai nai]] [order order] [weight weight]</pre> <p>Example: ITP(cfg-cs7-mlr-result)# gt 9991234 tt 0 gti 4 np 1 nai 4 weight 1</p>	<p>Specifies an outbound global title destination from within a result group.</p> <ul style="list-style-type: none"> • tt tt Identifies a translation type specified within the address. Integer in the range 0 through 255. • gti gti 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 np 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 nai Identifies the nature of the specified address. Configured only when the gti parameter value is 4. Integer in the range 0 through 127. • order order 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 weight 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 6	<pre>pc dest-pc [ssn ssn] [order order] [weight weight]</pre> <p>Example: ITP(cfg-cs7-mlr-result)# pc 3.3.1 weight 0</p>	<p>Specifies a destination point code. The destination point code must exist in the MTP3 routing table; its state is extracted from MTP3 for availability purposes.</p> <ul style="list-style-type: none"> • order order 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 weight 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 7	<pre>unavailable-routing {discard resume}</pre> <p>Example: ITP(cfg-cs7-mlr-result)# unavailable-routing resume</p>	<p>Specifies the routing of a packet when no members are available.</p> <ul style="list-style-type: none"> • 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 a 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	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	
Step 3	cs7 mlr modify-profile <i>profile-name protocol operation-name</i>	Defines SCCP and MAP addresses to modify in MLR routed messages.
	Example: cs7 mlr modify-profile SRISM gsm-map sri-sm	<ul style="list-style-type: none"> • <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. <p>Note You can create multiple modify profiles for each instance but can specify only one profile within a rule.</p>

Command or Action	Purpose
<p>Step 4</p> <pre>orig-smsc [prefix {prefix-remove-num *}{prefix-add-digits *}] [ton new-ton] [np new-np]</pre> <p>Example:</p> <pre>cs7 mlr modify-profile SRISM gsm-map sri-sm orig-smsc prefix 2 351</pre>	<p>Specifies the originating service center address.</p> <ul style="list-style-type: none"> • 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
<p>Step 5</p>	<pre> 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>] </pre> <p>Example:</p> <pre> cs7 mlr modify-profile SRISM gsm-map sri-sm orig-smsc prefix 2 351 cgpa gt prefix 2 351 </pre>	<p>Indicates that the SCCP calling party address (CgPA) needs modification.</p> <p>Note The CgPA routing indicator (RI) is unchanged during these modifications.</p> <ul style="list-style-type: none"> • 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 simply ignored. • prefix—specifies that prefix modification will be performed 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 “*” should be specified. 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> 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 242](#)
- [Creating and Loading a Stored Address Table File, page 245](#)
- [Replacing an Address Table File, page 248](#)

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* [**exact**] [**result** {**asname** *asname* | **block** | **continue** | **group** *group-name* | **pc** *dest-pc* [**ssn** *ssn*] | **gt** *addr-string* [**tt** *tt* **gti** {**2** | **4** **np** *np* **nai** *nai*}]}}]
5. **load** *URL*
6. **exit**
7. **cs7 save address-table mlr** *table-name url*

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 address-table <i>tablename</i> Example: ITP(config)# cs7 mlr address-table addrtbl1	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

Command or Action	Purpose
<p>addr <i>address</i> [exact] [result {<i>asname asname</i> block [sccp-error <<i>sccp-error</i>>] continue group <i>group-name</i> pc <i>dest-pc</i> [ssn <i>ssn</i>] gt <i>addr-string</i> [tt <i>tt</i> gti {2 4} np <i>np</i> nai <i>nai</i>}]}]</p> <p>Example:</p> <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>	<p>Configures one or more addresses in the address table.</p> <p>exact specifies that the configured address must exactly match.</p> <p>result indicates that the address will be handled in one of the following ways:</p> <p>Note If a rule contains multiple table-based parameters (such as <i>dest-sme-table</i>, <i>orig-sme-table</i>, or <i>orig-imsi-table</i>), then any result configured on an <i>addr</i> entry of an address-table is ignored.</p> <ul style="list-style-type: none"> • 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. • rule <i>rule-number</i> indicates that routing should proceed with a specified target rule number. • group <i>group-name</i> indicates that the message will be routed according to a named result-group. • 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. • 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.

Command or Action	Purpose
Step 5	<div data-bbox="196 264 305 289">load <i>URL</i></div> <div data-bbox="196 478 621 558"> Example: ITP(cfg-cs7-mlr-addr-table)# load disk0:mlraddrtbl </div> <div data-bbox="821 264 1492 1241"> (Optional) Specifies an address table file to load at startup. <ul style="list-style-type: none"> • 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 • rcp: 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 </div>
Step 6	<div data-bbox="196 1255 253 1281">exit</div> <div data-bbox="196 1465 621 1528"> Example: ITP(cfg-cs7-mlr-addr-table)# exit </div> <div data-bbox="821 1255 1206 1281">Exit to global configuration mode.</div>
Step 7	<div data-bbox="196 1539 711 1564">cs7 save address-table mlr <i>tablename url</i></div> <div data-bbox="196 1749 792 1829"> Example: ITP(config)#cs7 save address-table mlr addrtbl1 disk0:mlraddrtbl </div> <div data-bbox="821 1539 1492 1837">Saves the address table to an external location and file (url).</div>

Creating and Loading a Stored Address Table File

Address tables are typically created and stored to a file using the CLI. However, you may also create address tables externally from the ITP and then read the file into the ITP. For users interested in this option, the format for ITP address table files is specified below.

In this task you use any text editor to create a file of addresses. When you configure the ITP, you specify the table name and the location from which you will load the file of address table entries upon reboot. If necessary, you can add addresses to the file using the CLI. If you do add address entries, you must save the address table in order to have the updated list of addresses load upon reboot.

Each line in an address file must follow the following format:

line-identifier,token1,[token-n+1],[token-n+2], ... [token-n+x]]eol

Where line-identifier identifies the mandatory and optional tokens on a line and to which entity the line applies. All tokens are order dependant and follow the order specified in [Table 17](#).

[Table 17](#) lists the supported line identifiers for address tables and lists the syntax for each line.

Table 17 **Line Identifiers**

Line Identifier	Description	Syntax
ver	Specifies the version, variant, instance, network name and type.	<i>major,minor,variant,[instance],[network-name],type</i>
mlr	Specifies an MLR address table entry	<i>addr-tbl-name,address,result-id,[result-value],[result-options]</i>
!	Specifies a comment. Not parsed.	

[Table 18](#) describes and lists the values all of the tokens listed in [Table 17](#).

Table 18 **Token Identifiers**

Token	Description	Supported Value(s)
<i>major</i>	Indicates the major version associated with the file.	1
<i>minor</i>	Indicates the minor version associated with the file.	0, 1, 2, 3
<i>instance</i>	If the address-table file is associated with a particular instance, this field is used to convey that instance.	0 - 7
<i>variant</i>	Specifies the variant associated with a particular file.	ANSI, ITU, TTC
<i>network-name</i>	User-specified network name associated with the instance.	Alphanumeric string variable length maximum 19 characters
<i>addr-tbl-name</i>	User-specified name identifying the address table where the entry belongs.	Alphanumeric string variable length maximum 12 characters
<i>address</i>	User-specified address.	Variable length hexadecimal string 1 to 20 digits

Table 18 **Token Identifiers (continued)**

Token	Description	Supported Value(s)
result-id	Identifies the result type configured by the user.	as Result is an asname. bl Result is to block address with optional configuration of sccp-error for MLR results. cn Result is to continue. nr Result is to continue with the next SMS rule gr Result is a group pc Result is a pc pcssn Result is a pc and ssn gt Result is a gt address and selector
result-value	The result value of the MLR entry. The contents are dictated by the result identifier. See Table 18 .	Possible result values: <ul style="list-style-type: none"> • Variable length string if result identifier is as, gr, smpp, or ucp • Null if result identifier is bl, cn, or nr • Hexadecimal point code if result is pc • Hexadecimal point code and decimal ssn if result is pcssn • Variable length digit string, decimal <i>tt</i>, <i>gti</i>, <i>np</i>, and <i>nai</i> values if result is gt
result-options	User-configured option applied to entry.	Ex Specifies exact match.

[Table 18](#) lists the MLR result value tokens listed in [Table 18](#).

Table 19 **MLR Result Identifier Syntax**

Result Identifier	Version (maj, min)	Result Value Syntax	Supported Value(s)
bl	1, 3	<i>sc:<sccp-error></i>	0x00 to 0xFF for SCCP-Error. Sccp-error is optional. This is implemented only for MLR address tables
cn	1, 0		null
gr	1, 0	<i>group-name</i>	Alphanumeric string with a maximum of 12 characters.
pc	1, 0	<i>pc</i>	Hexadecimal point code

Table 19 MLR Result Identifier Syntax

Result Identifier	Version (maj, min)	Result Value Syntax	Supported Value(s)
pcssn	1, 0	<i>pc-ssn</i>	<i>pc</i> Hexadecimal point code. <i>ssn</i> Decimal value in range 2 - 255
gt	1, 1	<ul style="list-style-type: none"> gt:-gt tt:-tt gti:-gti np:-np nai:-nai 	<i>gt</i> Hexadecimal digit string with a maximum variable length of 15 digits. <i>tt</i> Decimal value in 0-255 range. Note ansi defaults to 10, itu defaults to 0 <i>gti</i> 2 or 4. Note ansi defaults to 2, itu defaults to 4 <i>np</i> Decimal value in 0-15 range, for gti=2, use 253 to indicate invalid. Note ansi defaults to 253, itu defaults to 1 <i>nai</i> decimal value in 0-127 range, for gti=2, use 253 to indicate invalid. Note ansi defaults to 253, itu defaults to 4

To create and load a stored address table file, 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.

	Command or Action	Purpose
Step 4	<pre>cs7 mlr address-table tablename</pre> <p>Example: ITP(config)# cs7 mlr address-table addrtbl1</p>	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 5	<pre>load URL</pre> <p>Example: ITP(cfg-cs7-mlr-addr-table)# load disk0:mlraddrtbl</p>	(Optional) Specifies an address table file to load at startup. <ul style="list-style-type: none"> • 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

Replacing an Address Table File

You can replace an existing address table. 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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cs7 address-table replace mlr *tablename url***

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 address-table replace mlr tablename url Example: ITP(config)# cs7 address-table replace mlr addrtbl1 disk0:mlraddrtbl1	Replaces an existing address table with one specified in a URL.

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
```

Define One or More Multi-layer SMS 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

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:

- The new keyword **ton** replaces the keyword **noa**. 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 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 20](#) and [Table 21](#) list the GSM-MAP and GSM-MAP Version 1 operation names mapped to ITP operation names.

Table 22 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 20 *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

Table 20 *GSM-MAP Operation Name Mapping to ITP CLI Operation Name (continued)*

Operation Name in GSM-MAP Specification	ITP CLI Operation Name	Opcode Value
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
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

Table 20 *GSM-MAP Operation Name Mapping to ITP CLI Operation Name (continued)*

Operation Name in GSM-MAP Specification	ITP CLI Operation Name	Opcode Value
updateLocation	updLoc	2
NoteMM-Event	noteMMEvent	89

Table 21 *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 22](#) allow you to route and screen based on MAP parameters and MAP-user parameters.

[Table 22](#) lists the parameters that are valid based on the specified **rule** operation.

Table 22 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
allow-multi-message-dialogue 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	

To define a multi-layer SMS ruleset, perform the following steps.

SUMMARY STEPS

Steps 1 through 4 are required. Steps 5 through 19 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. **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*] | **pc** *dest-pc* [*ssn ssn*] | **asname** *as-name* | **group** *result-group* | **block** | **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
<p>Step 3</p> <pre>cs7 [instance instance-number] mlr ruleset name [protocol {gsm-map ansi-41}]</pre> <p>Example: Router(config)#cs7 mlr ruleset MLR_RULES</p>	<p>Specifies an MLR ruleset and application layer protocol filter for the ruleset.</p> <ul style="list-style-type: none"> • <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. <ul style="list-style-type: none"> – 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. <p>Configuring the cs7 mlr ruleset command enables CS7 MLR ruleset configuration mode.</p>
<p>Step 4</p> <pre>rule order {{gsm-map ansi-41} operation-name [default] all-operations}</pre> <p>Example: ITP(cfg-cs7-mlr-set)# rule 5 gsm-map sms-mo</p>	<p>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.</p> <ul style="list-style-type: none"> • <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. <p>Configuring the rule command enables MLR ruleset-rule configuration mode in which you configure the input conditions of the rule.</p>

	Command or Action	Purpose
Step 5	allow-multi-msg-dialogue Example: ITP(cfg-cs7-mlr-set-rule)# allow-multi-msg-dialogue	Specifies that all messages including multi-message dialogues match the rule. Only valid for default rules.
Step 6	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 7

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>]	<p>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.</p> <ul style="list-style-type: none"> • <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: <ul style="list-style-type: none"> – [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 8	<p>dest-sme-table <i>table-name</i> [<i>dest-sme-addr-type</i>]</p> <p>Example: ITP(cfg-cs7-mlr-set-rule)# dest-sme-table MLR-ADDRS</p>	<p>Specifies an SMS address table or an MLR address table of destination SME addresses.</p> <ul style="list-style-type: none"> • <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: <ul style="list-style-type: none"> – [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 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.

	Command or Action	Purpose
Step 9	<p>dest-smsc { * <i>dest-addr</i> } [<i>addr-type</i>] [exact] [min-digits <i>min</i>] [max-digits <i>max</i>]</p> <p>Example: ITP(cfg-cs7-mlr-set-rule)# dest-smsc 18005551212</p>	<p>Specifies the destination SMSC.</p> <ul style="list-style-type: none"> • <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: <ul style="list-style-type: none"> – [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 10	<p>match-unknown-ton-np</p> <p>Example: ITP(cfg-cs7-mlr-set-rule)# match-unknown-ton-np</p>	<p>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.</p>
Step 11	<p>multi-message-dialogue</p> <p>Example: ITP(cfg-cs7-mlr-set-rule)# multi-message-dialogue</p>	<p>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 multi-message-dialogue command is specified, no other routing parameters may be configured for the rule.</p>

	Command or Action	Purpose
Step 12	<p>orig-imsi { * <i>imsi-address</i> unknown } [exact] [min-digits <i>min</i>] [max-digits <i>max</i>]</p> <p>Example: ITP(cfg-cs7-mlr-set-rule)# orig-imsi unknown</p>	<p>Specifies the origin IMSI address.</p> <ul style="list-style-type: none"> • <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 13	<p>orig-imsi-table <i>tablename</i> [ton <i>ton-value</i> np <i>np-value</i>]</p> <p>Example: ITP(cfg-cs7-mlr-set-rule)# orig-imsi-table addrtbl2</p>	<p>Specifies SMS address table or an MLR address table of origin IMSI addresses (address-table).</p> <ul style="list-style-type: none"> • <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 14	<p>orig-sme { * <i>orig-addr</i> } [<i>orig-sme-addr-type</i>] [exact] [min-digits <i>min</i>] [max-digits <i>max</i>]</p> <p>Example: ITP(cfg-cs7-mlr-set-rule)# orig-sme 12345</p>	<p>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.</p> <ul style="list-style-type: none"> • <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: <ul style="list-style-type: none"> – 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 15	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). <ul style="list-style-type: none"> • <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 16	orig-smsc { * <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. <ul style="list-style-type: none"> • <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: <ul style="list-style-type: none"> – 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 17	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.. <ul style="list-style-type: none"> • <i>protocol-id</i> Protocol identifier integer. Valid range is 0 to 255.
Step 18	preserve-opc Example: ITP(cfg-cs7-mlr-set-rule)# preserve-opc	Preserves the originating point code (OPC) when a rule is matched.
Step 19	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. <ul style="list-style-type: none"> • <i>id</i> Integer in the range 0 - 65535.

	Command or Action	Purpose
Step 20	<pre>modify-profile <i>profile-name</i></pre> Example: <pre>cs7 mlr ruleset FROM_MMSC rule 10 sri-sm default orig-smsc 397777777 modify-profile SRISM result route</pre>	<p>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.</p> <ul style="list-style-type: none">• <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
<p>Step 21</p> <pre>result {gt addr-string [gt-addr-type] pc dest-pc [ssn ssn] asname as-name group result-group block [scp-error <scp-error-name>] continue route}</pre>	<p>Specifies the processing that will be performed on a packet that matches the specified trigger and rule. One result must be specified.</p> <ul style="list-style-type: none"> gt addr-string Specifies that the message will be routed using SCCP global title. Valid <i>addr-string</i> is 1 to 15 hexadecimal digits. <ul style="list-style-type: none"> 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. 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. 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. An integer value from 0 to 15. nai Identifies the nature of specified address. Only specified when the gti parameter value is 4. An integer value from 0 to 127. pc dpc Specifies that the message will be routed using the specified destination point code (dpc) <ul style="list-style-type: none"> ssn ssn (Optional) Specifies that the messages route using the subsystem number (ssn). Valid range is 2 to 255.

Command or Action	Purpose
<p>Example:</p> <pre>ITP(cfg-cs7-mlr-set-rule)# result block</pre>	
<p>Example:</p> <pre>ITP(cfg-cs7-mlr-set-rule)# cs7 mlr ruleset FROM_MMSC rule 10 sri-sm default orig-smsc 397777777 modify-profile SRISM result route</pre>	<ul style="list-style-type: none">• aname <i>aname</i> Specifies that the message will route to a particular destination M3UA or SUA application server. Valid <i>aname</i> is 1 to 12 characters.• group <i>result-group</i> Specifies that the message will route using a result group. Valid <i>result-group</i> is 1 to 12 characters.• block Specifies the messages matching this rule will drop.• scp-error Provides a return UDTs with the configured <i>sccp-error-name</i> if the received UDT has the return-on-error option set.• 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 266](#)
- [Information About MLR Triggers with GWS, page 266](#)
- [Define MLR Triggers with Proprietary Method, page 267](#)

**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 212 or “[Defining Entries in GWS Tables](#)” section on page 216 in .

Information About MLR Triggers with GWS

In Cisco IOS 12.2(18)IXD and later releases, 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 releases prior to Cisco IOS 12.2(18)IXD 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.

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 IOS 12.2(18)IXD and later releases support 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 207](#)

Define MLR Triggers with Proprietary Method

To define the Multi-layer SMS routing table with proprieta y 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*}}
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.

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.

	Command or Action	Purpose
Step 4	<pre>trigger {mtp3 [{dpc point-code} {opc point-code} [si indicator]} cdpa {gt¹ {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 pc [ssn ssn] asname asname gt gta [gt-addr-type] group groupname}]</pre> <p>Example: Router(config-cs7-mlr)# trigger cdpa gt 9991117770 ruleset RULESET-5</p>	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	<pre>cdpa {gt {selector addr-string} [gt-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> <p>Example: Router(cfg-cs7-mlr-trigger)# cdpa gt 9991117770 ruleset RULESET-5</p>	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.
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> <p>Example: Router(cfg-cs7-mlr-trigger)# cGpa gt 9991116 ruleset RULESET-5</p>	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> <p>Example: Router(cfg-cs7-mlr-trigger)# default ruleset DEFAULT-RULES</p>	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 270](#)

- [Blocking Based on cgPa, cdPa, and SMS MAP Operation Code, page 272](#)
- [Blocking Based on cgPa, cdPa and SMS MO/MT Routing Parameters, page 272](#)

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 selector tt tt gti gti np np Example: ITP(config)# cs7 gtt selector e164 tt 10	Names and configures the GTT selector and enables CS7 GTT selector submenu. MLR primary GT triggers re-use the existing GTT selector table entity containing lists of GTA entries used to perform Global Title Translation.

	Command or Action	Purpose
Step 4	<pre>gta gta app-grp app-grp</pre> <p>Example: ITP(config-cs7-gtt-selector)# gta 11111 app-grp GROUP1</p>	Defines a GTA that translates to a GTT application group.
Step 5	<pre>gta gta asname as-name {gt pcssn} [ssn ssn] [ntt newtt] [qos-class qos]</pre> <p>Example: ITP(config-cs7-gtt-selector)# gta 22222 asname GREENASP3 pcssn</p>	Defines a GTA that translates to an M3UA or SUA Application Server name.
Step 6	<pre>gta gta pcssn pc {gt pcssn} [ssn ssn] [ntt newtt]</pre> <p>Example: ITP(config-cs7-gtt-selector)# gta 33333 pcssn 1.1.1 pcssn</p>	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 Multi Layer SMS 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 226 for these commands.

To display information about the MLR configuration, perform the following steps in privileged EXEC mode:

Command	Purpose
Router# show cs7 mlr-all <i>commands</i>	Displays all the mlr show commands.
Router# show cs7 instance-number mlr address-table <i>table-name</i>	Displays the addresses matched within the table.
Router# show cs7 instance-number 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. <ul style="list-style-type: none"> <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 [instance-number] 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 instance-number 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 instance-number 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 instance-number mlr statistics <i>name</i>	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 instance-number mlr table <i>name detail</i>	Displays the parameters and results associated with each routing trigger.
Router# show cs7 instance-number 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 instance-number mlr table name 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.
Router# show monitor event-trace [all-traces] [component {all back time clock time from-boot seconds latest parameters}]	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 table all	Enables all debugs.
Router# debug cs7 mlr table error	Debugs error events.
Router# debug cs7 mlr table info	Displays informational events
Router# debug cs7 mlr table packet	Displays packet events.

Configuration Examples of Multi-layer SMS Routing

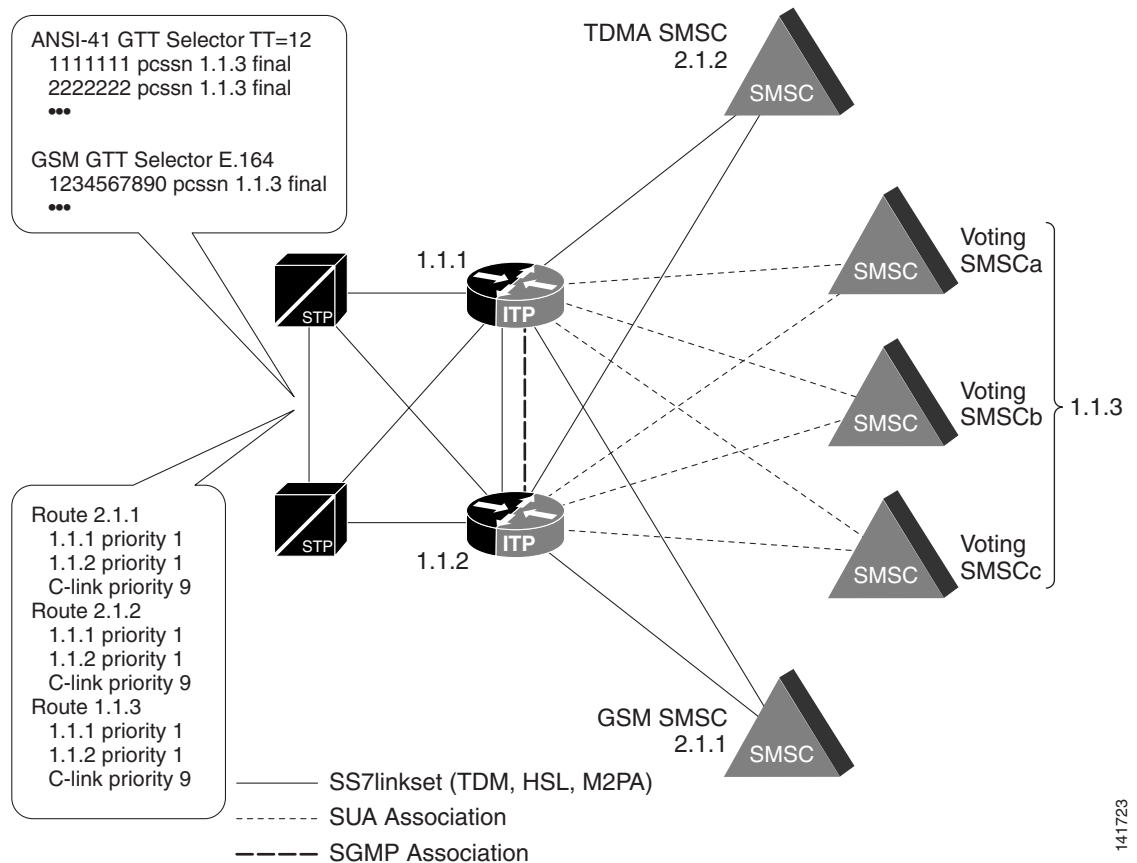
This section includes the following examples:

- [Configuration Example for Multi-Layer Routing: ITP Receives All SMS-MO Traffic in GT-Routed Network, page 277](#)
- [Configuration Example for Multi-Layer Routing: Legacy SMSC Retains Point Code in PC-Routed Network, page 279](#)
- [Configuration Example for Multi-Layer Routing: MLR Distribution to MTP3-Based SMSCs, page 282](#)
- [Examples of Configuring Routing based on Operation types, page 283](#)
- [Example of Routing with B-Address Binding, page 284](#)
- [Configuration Example of Address Modification, page 285](#)

Configuration Example for Multi-Layer Routing: 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 28](#).

Figure 28 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

```

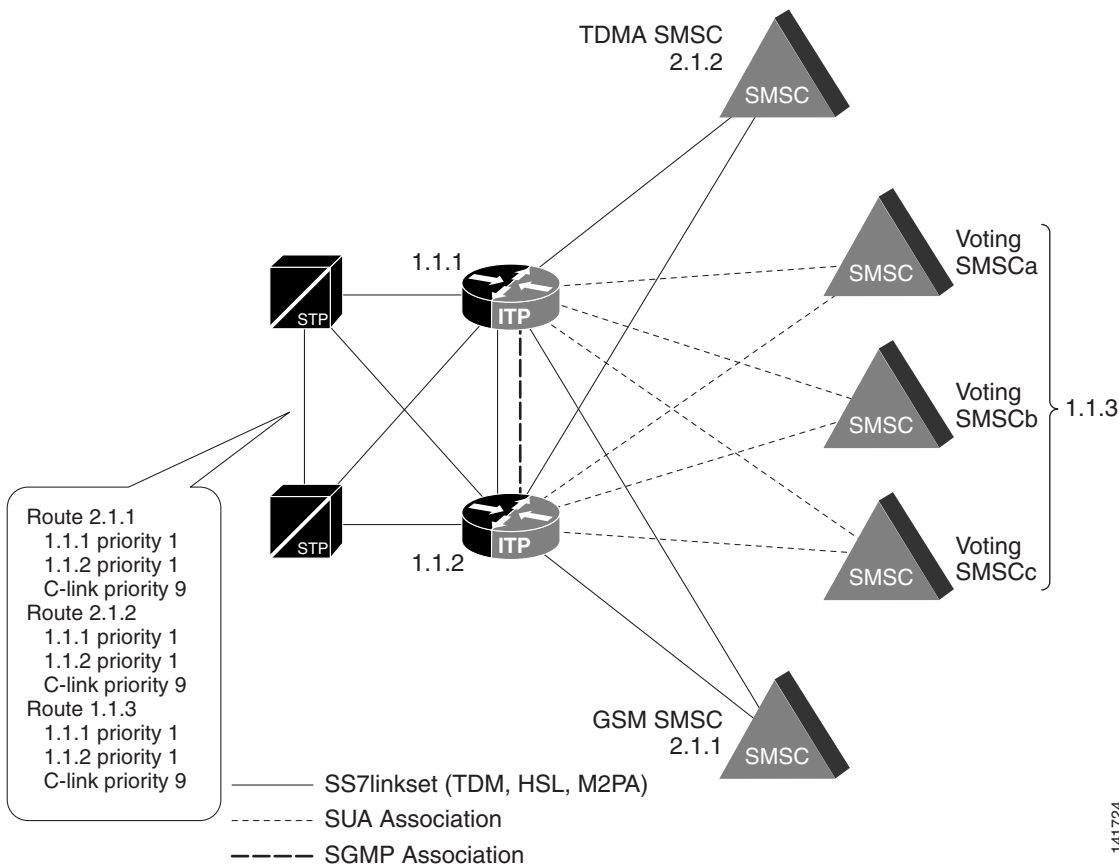
```
rule 2 ansi-41 smsnot
  dest-sme table VSMSC-ADDRS
rule 3 ansi-41 smdpp default
  result group TDMA-SMSCS
rule 4 ansi-41 smsnot default
  result group TDMA-SMSCS

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 Multi-Layer Routing: 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 29](#)

Figure 29 .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

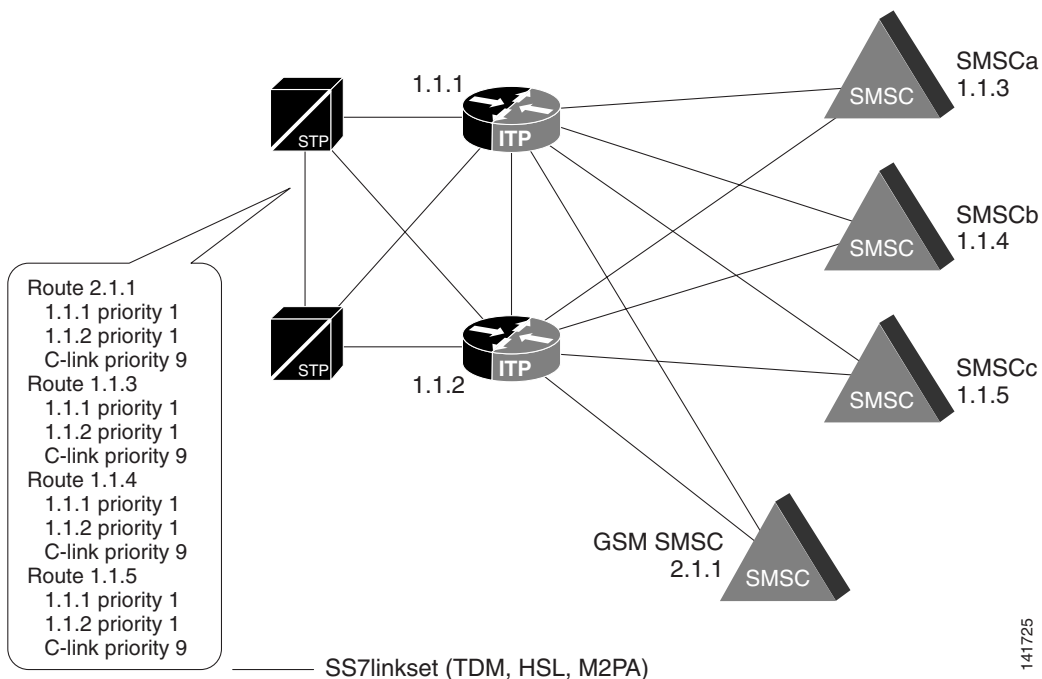
cs7 instance 1 mlr table SMS-TABLE
  trigger mtp3 dpc 2.1.1 si 3
  cdpa pc 2.1.1 ssn 8 ruleset GHOST-RULES
  trigger mtp3 dpc 2.1.2 si 3
  cdpa pc 2.1.2 ssn 11 ruleset TDMA-RULES

```

Configuration Example for Multi-Layer Routing: 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 30.

Figure 30 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 397777777 tt 0 gti 4 np 1 nai 4 ruleset FROM_MMSC
```




MTP3 Offload



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 MTP3 Offload feature allows MTP3 message forwarding and Global Title Translation (GTT) to be performed on the VIPs.

Feature History for MTP3 Offload

Release	Modification
12.2(18)IX	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

- [Restrictions for MTP3 Offload, page 287](#)
- [Information About MTP3 Offload, page 288](#)
- [How to Configure MTP3 Offload, page 288](#)
- [Verifying MTP3 Offload, page 288](#)

Restrictions for MTP3 Offload

For MTP3 Offload, separate VIPs are required for each protocol (LSL, HSL, M2PA/SCTP, xUA/SCTP).

Information About MTP3 Offload

MTP3 Offload is an ITP feature that allows MTP3 message forwarding and Global Title Translation (GTT) to be performed on the VIPs.

Each VIP has a copy of the GTT tables, MTP3 route tables and link and linkset status for the entire ITP. The RSP executes the MTP3 and SCCP management procedures and updates each VIP with status changes that affect MTP3 forwarding and GTT. The MTP3 forwarding occurs VIP to VIP, without using the RSP.

MTP3 Offload eliminates the single process-switch queue because each line card can independently fast switch the majority of SS7 data packets. MTP3 Offload provides combined linkset support, SLS rotation support, GTT and QOS link selection support.

How to Configure MTP3 Offload



Note

Prior to IOS Release 12.2(20)SW, the MTP3 Offload feature and the Instance Translation feature could not be configured simultaneously. That restriction has been removed with IOS Release 12.2(20)SW.

To configure MTP3 offload, use the following command in global configuration mode:

Command	Purpose
Router(config)# cs7 offload mtp3	Enables MTP3 offload on all VIPs.

The **cs7 offload mtp3** command will take effect when the ITP is reloaded.

Verifying MTP3 Offload

To verify the MTP3 Offload feature, use the following command in EXEC mode:

Command	Purpose
Router# show cs7 offload mtp3	Displays the current status, counters, and events maintained by the MTP3 offload feature.



ITP Non-Stop Operation (NSO)

The ITP Non-Stop Operation (NSO) feature is an enhancement to the ITP High Availability support on the Cisco7600 platform. It allows the ITP running on a Cisco7600 router to continue operation in the event of a Supervisor 720 failure.

Feature History for ITP NSO

Release	Modification
12.2(18)IXA	This feature was extended to the IOS software release for ITP on the Cisco 7600 platform.

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

- [Restrictions for ITP NSO, page 290](#)
- [Information About ITP NSO, page 290](#)
- [How to Configure ITP NSO, page 290](#)
- [Monitoring NSO, page 294](#)
- [Configuration Example for ITP NSO, page 294](#)

Restrictions for ITP NSO

The ITP NSO feature is supported on the Cisco 7600 router.

Information About ITP NSO

A switchover is a disruptive event in the SS7 and SIGTRAN networks. MTP2, M2PA and HSL links are brought down and a full MTP3 restart occurs. Any messages that were queued at the time of the switchover are lost. M3UA and SUA (collectively referred to as xUA) SCTP associations are closed.

The ITP NSO feature minimizes the disruption caused by a Supervisor switchover by keeping the ITP links and xUA associations active and avoiding an MTP3 restart. This is accomplished by taking advantage of the offloaded forwarding on the FlexWANs and synchronizing ITP state information from the Active Supervisor to the Standby Supervisor.

How to Configure ITP NSO

Configuring the ITP NSO feature consists of the following tasks:

- [Configuring M2PA Offload, page 290](#)
- [Configuring xUA SCTP Offload, page 291](#)
- [Configuring Stateful Switchover Redundancy Mode, page 292](#)
- [Enabling ITP NSO, page 293](#)

Configuring M2PA Offload

All M2PA SCTP instances must be offloaded. This allows M2PA links to remain active if the active Supervisor fails.

M2PA Offload

M2PA Offload is an ITP feature on the 7600 that enables M2PA message handling to be performed on the FlexWANs.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cs7 local-peer *port-number* offload *slot-number* bay**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	cs7 local-peer port-number offload slot-number bay Example: Router(config)# cs7 local-peer 1024 offload 6 0	Creates an M2PA SCTP instance and offloads the M2PA SCTP processing to the specified FlexWAN.

What to Do Next

Configure xUA SCTP Offload.

Configuring xUA SCTP Offload

All xUA instances must be offloaded. This allows xUA ASP connections to remain active if the active Supervisor fails.

xUA SCTP Offload

M3UA and SUA use SCTP to communicate with Application Server Processes (ASPs). This feature offloads the SCTP processing for xUA ASPsFlexWANs.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cs7 m3ua port-number offload slot-number bay**
4. **cs7 sua port-number offload slot-number bay**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	cs7 m3ua port-number offload slot-number bay Example: Router(config)# cs7 m3ua 1024 offload 6 0	Creates an M3UA instance and enables the offload of M3UA SCTP processing to a specifiedFlexWAN.
Step 4	cs7 sua port-number offload slot-number bay Example: Router(config)# cs7 sua 2048 offload 7 0	Creates an SUA instance and enables the offload of SUA SCTP processing to a specifiedFlexWAN.

What to Do Next

Configure Stateful Switchover Redundancy Mode.

Configuring Stateful Switchover Redundancy Mode

Configuring Stateful Switchover (SSO) redundancy mode allows the ITP NSO feature to track the redundancy state of the Cisco7600.

SSO is the IOS High Availability feature that allows one Supervisor on a 7600 to immediately take over for the other Supervisor in the event of a Supervisor failure. SSO supports synchronization of line card, protocol, and application state information between Supervisors for supported features and protocols (a “hot standby”).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **boot system flash device:image-name**
4. **redundancy**
5. **mode sso**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enables global configuration mode.
Step 3	boot system flash device:image-name Example: Router(config)# boot system flash disk0:s72033-itpk9v-mz	Indicates the location of the image to be loaded. The command is issued on the Active Supervisor and is synchronized to the running-config of the Standby Supervisor.
Step 4	redundancy Example: Router(config)# redundancy	Enables redundancy configuration mode.
Step 5	mode sso Example: Router(config-red)# mode sso	Sets the redundancy mode to SSO.

What to Do Next

Configure ITP NSO.

Enabling ITP NSO

Enabling ITP NSO instructs the ITP protocols on the active Supervisor to synchronize the operational state to the standbySupervisor.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>	Enables privileged EXEC mode.
	Example: <code>Router> enable</code>	<ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<code>configure terminal</code>	Enters global configuration mode.
	Example: <code>Router# configure terminal</code>	
Step 3	<code>cs7 nso</code>	Enables ITP NSO.
	Example: <code>Router(config)# cs7 nso</code>	

What to Do Next

You have enabled ITP NSO and saved the configuration. At this point the ITP is in NSO mode and ready for hot switchovers.

76007600SSO is the IOS High Availability feature that allows one Supervisor on a 7600 to immediately take over for the other Supervisor in the event of a Supervisor failure. SSO supports synchronization of line card, protocol, and application state information between Supervisors for supported features and protocols (a “hot standby”).

Monitoring NSO

Use the following commands to display NSO and MTP3 offload status.

SUMMARY STEPS

1. `show cs7 nso`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>show cs7 nso</code>	Displays the status of NSO.
	Example: <code>Router# show cs7 nso state</code>	

Configuration Example for ITP NSO

```
boot system flash disk0:s72033-itpk9v-mz
card type t1 41
cs7 variant ANSI
cs7 network-name ITP1
```

```
cs7 point-code 3.4.5
cs7 nso
!
redundancy
  mode sso
!
controller T1 4/1/0
  framing esf
  clock source internal
  linecode b8zs
  channel-group 0 timeslots 1 speed 56
!
interface FastEthernet3/0/0
  ip address 10.0.0.1 255.0.0.0
!
controller T1 4/1/0
  framing esf
  clock source internal
  linecode b8zs
  channel-group 0 timeslots 1 speed 56
!
interface Serial4/1/0:0
  no ip address
  encapsulation mtp2
!
cs7 local-peer 2001 offload 3 0
  local-ip 10.0.0.1
!
cs7 linkset to_bogey 1.2.3
  link 0 Serial4/1/0:0
!
cs7 linkset to_bacall 4.5.6
  link 0 sctp 10.0.0.2 2002 2001
!
end
```




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.

Feature History for ITP QoS

Release	Modification
12.2(18)IXA	This feature was extended to the IOS software release for ITP on the Cisco 7600 platform.

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 297](#)
- [How to Configure ITP QoS, page 299](#)
- [Verifying ITP QoS, page 307](#)
- [QOS Configuration Example, page 308](#)

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 300](#)
- [Specifying Access List Classification, page 301](#)
- [Specifying Service Indicator Classification, page 302](#)
- [Specifying SCCP Packet Classification, page 303](#)
- [Specifying Destination Point Code Classification, page 305](#)
- [Specifying a QoS classification for an ASP, page 306](#)
- [Specifying QoS Routing Over M2PA Links, page 307](#)

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 class	Defines a QoS class and enters QoS class configuration mode.
Step 2	Router(config-cs7-qos)# qos-ip-precedence class	Defines an IP precedence for the class.
Step 3	Router(config-cs7-qos)# exit	Exits CS7 QoS configuration submenu, and enters global configuration mode.
Step 4	Router(config)# cs7 linkset ls-name adj-pc	Specifies an input linkset and enters linkset configuration submenu.
Step 5	Router(config-cs7-ls)# match any qos-class class	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 ls-name adj-pc	Specifies an output linkset and enters linkset configuration submenu.
Step 8	Router(config-cs7-ls)# link slc	Specifies a link in the linkset and enters link configuration mode.
Step 9	Router(config-cs7-ls-link)# qos-class class	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 slc	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 class	Defines a QoS class and enters QoS class configuration mode.
Step 2	Router(config-cs7-qos)# qos-ip-precedence class	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 class	Defines a QoS class and enters QoS class configuration mode.
Step 5	Router(config-cs7-qos)# qos-ip-precedence class	Defines an IP precedence for the class.
Step 6	Router(config)# cs7 linkset ls-name adj-pc	Specifies an input linkset and enters linkset configuration submode.
Step 7	Router(config-cs7-ls)# match si si qos-class class	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 ls-name adj-pc	Specifies an output linkset and enters linkset configuration submode.
Step 10	Router(config-cs7-ls)# link slc	Specifies a link in the linkset and enters link configuration mode.
Step 11	Router(config-cs7-ls-link)# qos-class class	Assigns QoS class to link.
Step 12	Router(config-cs7-ls)# link slc	Specifies a link in the linkset and enters link configuration mode.
Step 13	Router(config-cs7-ls-link)# qos-class class	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 slc	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.
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 mask linkset <i>ls-name priority priority-value qos-class class</i>	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.
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 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 [m3ua sua]</i>	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.

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      any      to_newyork
2    3      10      si 3     to_chicago
3    5      10      si 5     to_chicago
4    4      2700   access-group  to_atlanta
5    5      26     none
6    3      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
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

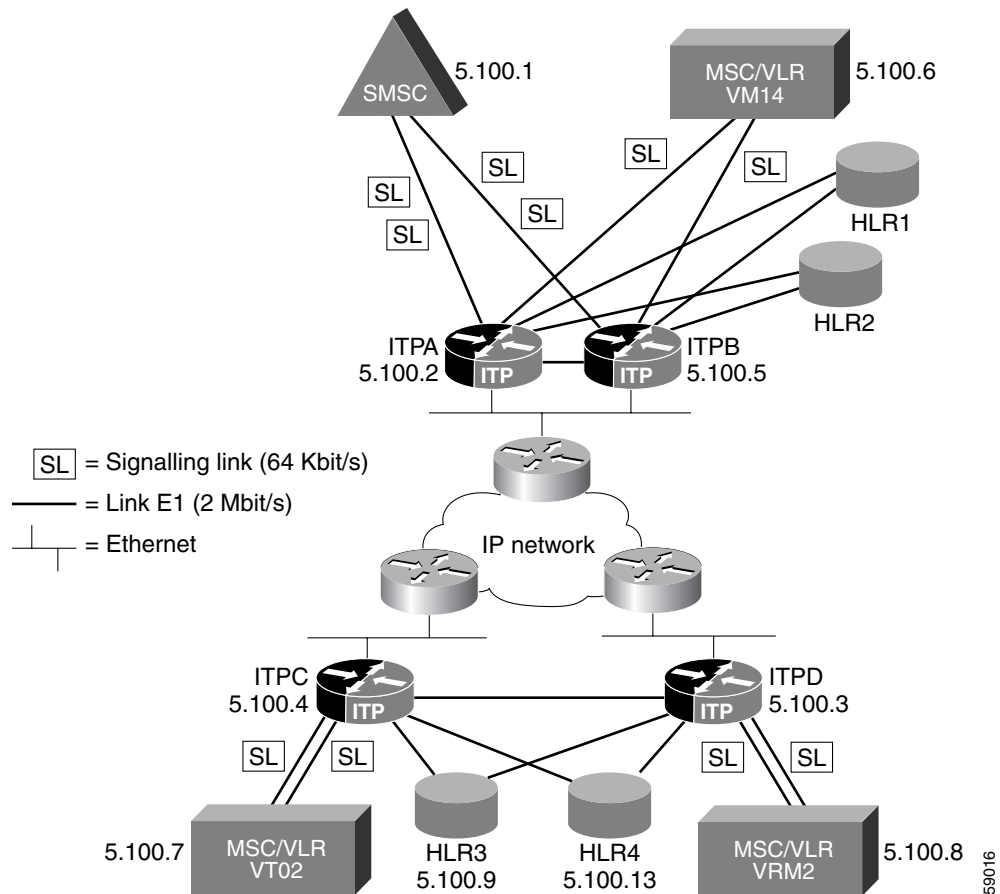
This section includes the following examples of ITP QoS packet classification and Cisco IOS QoS packet scheduling and queuing:

- [Service Indicator Packet Classification and Access List Classification, page 310](#)
- [SCCP Packet Classification, page 312](#)
- [Input Linkset Classification, page 315](#)
- [Destination Point Code Classification, page 317](#)
- [Cisco IOS QoS Packet Scheduling and Queuing, page 319](#)
- [ITP SG QoS Configuration Examples, page 322](#)

The network configuration is illustrated in [Figure 31](#).

→ The arrow symbol indicates the specific configuration statements that implement QoS on each ITP.

Figure 31 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 **smisc** 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 vm14 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 $l$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 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

```

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 307.

```

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(18)IXA	This feature was extended to the IOS software release for ITP on the Cisco 7600 platform.
12.2(18)IXD	Added enhanced load sharing to improve load distribution among available links.

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 MTP3 Load Sharing, page 325](#)
- [Information About SCCP Load Sharing, page 327](#)
- [How to Configure SCCP Load Sharing, page 328](#)

How to Configure MTP3 Load Sharing

This section describes some of the possible configuration options for MTP3 load sharing.

How to Configure 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 created 3-bit hash 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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cs7** [**instance** *instance-number*] **sls-opc-dpc** [**opc-shift** *<opc-shift-number>*] [**dpc-shift** *<dpc-shift-number>*]
4. **cs7** [**instance** *instance-number*] **sls-shift** { *sls-shift-value* }

	Command	Purpose
Step 1	enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
	Example: Router> enable	
Step 2	configure terminal	Enters global configuration mode.
	Example: Router# configure terminal	

Command	Purpose
Step 3 <code>cs7 [instance instance-number] sls-opc-dpc [opc-shift <opc-shift-number>] [dpc-shift <dpc-shift-number>]</code> Example: <pre>ITP(config)# cs7 instance 4 sls-opc-dpc dpc-shift 7 dpc-shift 4</pre>	(Optional) Creates a 3-bit hash from a 6-bit subset taken from the OPC and DPC. <ul style="list-style-type: none"> • 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>pc-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 number of bit positions from which the 6-bits are selected.
Step 4 <code>cs7 [instance instance-number] sls-shift {sls-shift-value}</code> Example: <pre>ITP(config)# cs7 instance 0 sls-shift 3 or ITP(config-cs7-ls)# sls-shift 3</pre>	(Optional) Shifts which SLS bits are used for link and linkset selection. The range is from 0 to 3. The default is 0. <ul style="list-style-type: none"> • 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.

Information About SCCP Load Sharing

Signaling Connection Control Part (SCCP) is software that 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 2 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 8 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 8 destinations based on a least cost available algorithm using a GTT Application Group. (multiplicity = cost).
- 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 8 destinations based on the SLS bits using a GTT Application Group. (multiplicity = share).
- Class 1 traffic can be load-shared among a maximum of 8 destinations based on a least cost available algorithm using a GTT Application Group in conjunction with the SLS bits. (multiplicity = cost).

How to Configure 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 8 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 SLS. This situation may be configured to share between up to 8 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 SLS shall be 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 23 *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 SLS depending on the protocol class. This is equivalent to the share mode described earlier.

Table 24 *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 SLS). 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 25 *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 dominate modes. The advantage of using a GTT MAP instead of an application group is memory savings. An application group uses approximately 156 bytes 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 26 **Reference for Scenario 5**

Item	Cost
A - Final	1
B - Final	1
C - Intermediate	2
D - Intermediate	2

How to Configure SCCP 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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cs7 [instance *instance-number*] distribute-sccp-sequenced**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• 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>] distribute-sccp-sequenced Example: Router(config)# cs7 instance 1 distribute-sccp-sequenced	Disable SCCP load sharing recognition of class and sequencing. <ul style="list-style-type: none">• 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.• <i>instance-number</i>—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
```




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.

Feature History for Summary Routing and ANSI Cluster Routing

Release	Modification
12.2(18)IXA	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 Summary Routing and ANSI Cluster Routing, page 333](#)
- [How to Configure Summary Routes, page 336](#)
- [How to Configure ANSI Cluster Routing, page 338](#)

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 0-27 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
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	acce		2	sirius		avail	allowed	avail
			3	castor		avail	allowed	avail
			4	pollux		avail	allowed	avail
1.0.0/3	acce		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 (RSP/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, RSP/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. Routeset 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. Routeset 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 routeset 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 prio priority-value	Adds a summary route to the table.

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 system	Specifies the name of the route table and enters route table configuration mode.
Router(config-cs7-rt)# update route point-code {[255.255.0 /16 linkset ls-name prio priority-value	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 341](#)
- [Monitoring ITP, page 352](#)
- [Tuning ITP, page 377](#)

Feature History for Verifying, Monitoring, and Tuning the ITP

Release	Modification
12.2(18)IXA	This feature was introduced.



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   mscl             avail
                      9   momo             avail
5.5.5/14             acces 1   mscl             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   mscl             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 VIP
 - MTP3 offload has been permanently disabled on a VIP by the system due to excessive errors. When MTP3 offload has been permanently disabled on a VIP (by the system) all links on that VIP 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	mocl	avail	PROHIB	UNAVAIL
			9	momo	avail	PROHIB	UNAVAIL
5.5.5/14	acces		1	mocl	avail	allowed	avail
			9	momo	avail	allowed	avail
6.6.1/14	INACC		1	mica	avail	PROHIB	UNAVAIL
			9	malo	avail	PROHIB	UNAVAIL
6.6.6/14	acces		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 0/0
CS7 MTP2 states for interface Serial0/0
Protocol version for interface Serial0/0 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.

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 155 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 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
```

Routing

AS Name	State	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: as1          State: down          Type: SUA
RoutContext: 111      Traffic mode: loadshare roundrobin
Mate AS state: unknwn  Recovery tmout: 2000 ms  Recovery queue depth: 0
QOS Class: 0          Burst recovery tmout: 4000 ms
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.

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 352](#)
- [Enabling Simple Network Management Protocol, page 353](#)
- [Monitoring the Cisco ITP, page 354](#)

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# 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# logging host	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# 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 [grr-map-state] [link-congestion] [link-state] [link-utilization] [linkset-state] [route-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:

Commands	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 `ciscoGrtDestStateChange` notification.

To specify the maximum number of route management state changes allowed per window, use the **cs7 snmp mgmt-max-window** global configuration command:

Commands	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 `ciscoGrtMgmtStateChange` notification.

Monitoring the Cisco ITP

This section includes information about the following tasks:

- [Monitoring CPU/Memory, page 355](#)
- [Monitoring Linksets and Links, page 356](#)
- [Monitoring MTP2 Links/Interfaces, page 357](#)
- [Monitoring M2PA Links/Interfaces, page 362](#)
- [Monitoring GTT Measurements, page 366](#)
- [Monitoring M3UA or SUA, page 366](#)
- [Monitoring AS, ASP, Mated-SG, page 368](#)
- [Monitoring Routes, page 373](#)
- [Monitoring Gateway Screening Violations, page 374](#)
- [Monitoring System Messages, page 374](#)
- [Monitoring Accounting, page 375](#)

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 VIP
 - MTP3 offload has been permanently disabled on a VIP by the system due to excessive errors. When MTP3 offload has been permanently disabled on a VIP (by the system) all links on that VIP 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

```

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 stats 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_SIISSCount      = 2
LSSU_XMIT_SIPOCount       = 0
LSSU_XMIT_SIPOECount      = 0
LSSU_XMIT_SIBCount        = 0
LSSU_XMIT_SIBECCount      = 0
LSSU_RCV_Count            = 2
LSSU_RCV_SIISSCount       = 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 application-group <i>name</i>	Displays GTT measurements kept on a application group basis.

To display measurements for the line card, (available only if MTP3 offload is enabled and only on the Cisco 7500 platform) 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 367](#)
- [Monitoring SUA, page 367](#)
- [Monitoring Point Code Status, page 367](#)
- [Monitoring AS, page 368](#)
- [Monitoring ASP, page 369](#)
- [Monitoring SGMP and Mated SG Pairs, page 371](#)

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 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: as1          State: down          Type: SUA
RoutContxt: 111      Traffic mode: loadshare roundrobin
Mate AS state: unknwn Recovery tmout: 2000 ms Recovery queue depth: 0
QOS Class: 0         Burst recovery tmout: 4000 ms
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
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 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 No Cfg As For Asp: 0
XUA Notify Messages Sent Stats
NOTIFY-AS Inactive: 0
NOTIFY-AS Pending: 0
NOTIFY-Alt ASP Active: 0
Outbound SSNM From SS7 Stats
TFAs Rcvd: 0
TFRs Rcvd: 0
Cong 0 TFCs Rcvd: 0
Cong 2 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
Inbound SSNM to SS7 Stats
TFAs Sent: 0
TFRs Sent: 0
Cong 0 TFCs Sent: 0
Cong 2 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
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
ERR Inv Routing Context:0
ERR Subsystem Status :0
NOTIFY-AS Active: 0
NOTIFY-Insuf ASP: 0
NOTIFY-ASP Failure: 0
TFPs Rcvd: 0
UPUs Rcvd: 0
Cong 1 TFCs Rcvd: 0
Cong 3 TFCs Rcvd: 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
TFPs Sent: 0
UPUs Sent: 0
Cong 1 TFCs Sent: 0
Cong 3 TFCs Sent: 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
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 SGMP and Mated SG Pairs

The following is sample output from the **show cs7 sgmp** command:

```

Router#show cs7 sgmp
SGMP Local port: 14002      State: active      SCTP instance handle: 3
Local ip address:          172.18.48.39
Number of active SGMP 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: 20000
Assoc retransmissions: 10
Minimum RTO: 1000 ms
Bundle status: on
Keep alive status: true
Cumulative sack timeout: 200 ms
Path retransmissions: 4
Maximum RTO: 1000 ms
Bundle timeout: 5 ms
Keep alive timeout: 30000 ms

```

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: SGMP
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: SGMP
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 AS Route Table

The following is output from the **show cs7 asroute** command:

```
Router# show cs7 asroute
```


AsRoute Name	Routing Context	Routing Key Dpc	State
-----	-----	-----	-----
aaa	111222	8.7.5	M3UA inactive
vp1	7777	7.7.7	shutdown

The following is sample output from the **show cs7 asroute** command (in the default brief format):

```
Router# show cs7 asroute name scp2 detail
```

```
AS Route Name: scp2           State: M3UA restricted      Type: M3UA
Routing context: 6666        Routing key DPC: 6.7.8
  AS Name: kure2.as1         AS Route State: unavail    Priority: 2
  Mated SG Name: bermuda     Mated SG State: avail     Priority: 4
```

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# <code>show cs7 access-lists</code>	Displays ITP access lists.
Router# <code>show cs7 accounting [access-violations] [checkpoint]</code>	Displays accounting details.
Router# <code>show cs7 as [[m3ua [include-gtt exclude-gtt only-gtt]] [sua [include-gtt exclude-gtt only-gtt]] [all [include-gtt exclude-gtt only-gtt]] [name asname]] [operational active all] [statistics detail brief]</code>	Displays CS7 AS statistics.

Command	Purpose
Router# show cs7 asp [m3ua sua all name <i>asp-name</i> asname <i>asname</i>] [statistics [detail] bindings detail event-history]	Displays CS7 ASP statistics.
Router# show cs7 asroute [name <i>name</i>] [active operational] [detail event-history statistics]	Displays CS7 AS Route Table statistics.
Router# show cs7 gtt	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 <i>port-num</i>] [peer <i>ls-name</i> [slc]] [state <i>ls-name</i> [slc]] [stats <i>ls-name</i> [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.
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 point-code	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 [destination] [brief detailed]	Displays the routing table.
Router# show cs7 sgmp	Displays Signaling Gateway Mate Protocol (SGMP) 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 377](#)
- [Tuning MTP3 Timers, page 380](#)
- [Tuning MTP2 Parameters, page 380](#)
- [Tuning SCTP Parameters, page 384](#)

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 377](#)

[Specify HSL Parameters on a Link, page 379](#)

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 name	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 Paramters

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.

Command	Purpose
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.
Router(config-cs7-profile-hsl)# sscop nax-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.

Command	Purpose
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 377](#) 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 ls-name	Specifies the linkset to which you will apply the profile, and enters linkset configuration mode.
Router(config-cs7-ls)# link slc	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 {1-3}	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 380](#)
- [Specifying MTP2 Parameters in a CS7 Profile, page 382](#)
- [Specifying MTP2 Parameters Individually, page 383](#)

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

MTP2 packet bundling is supported on the Cisco 7500 only. 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 20000 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 submode.
Router(config-cs7-profile)# mtp2	Enables the CS7 profile submode 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). MTP2 packet bundling is supported on the Cisco 7500 only.
Router(config-cs7-profile-mtp2)# timer { <i>t1</i> <i>t2</i> <i>t3</i> <i>t4e</i> <i>t4n</i> <i>t5</i> <i>t6</i> <i>t7</i> <i>ttc timer</i> } <i>msec</i>	Specifies the following MTP2 timers: ¹ <ul style="list-style-type: none"> 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 { <i>t1</i> <i>t2</i> <i>t3</i> <i>t4e</i> <i>t4n</i> <i>t5</i> <i>t6</i> <i>t7</i> } <i>msec</i>	Specifies the following MTP2 timers: ¹ <ul style="list-style-type: none"> • <i>t1</i> -- T1 (alignment ready) • <i>t2</i> -- T2 (not aligned) • <i>t3</i> -- T3 (aligned) • <i>t4e</i> -- T4E (emergency proving period) • <i>t4n</i> -- T4N (normal proving period) • <i>t5</i> -- T5 (sending SIB) • <i>t6</i> -- T6 (remote congestion) • <i>t7</i> -- 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 RSP and MTP2 on the VIP, 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 <i>msec</i>	Enables bundling and specifies the bundling interval (the length of time to wait for packets before sending a bundle).

**Note**

Bundling of MTP2 packets is supported on the Cisco 7500 router only.

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 <i>packets</i>	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 384](#)
- [Tuning SCTP Parameters for M2PA, page 387](#)
- [Tuning SCTP Parameters for M3UA, SGMP, and SUA, page 388](#)
- [Tuning SCTP Parameters for an ASP, page 389](#)
- [Tuning AS Options, page 389](#)
- [Tuning SCTP Parameters for a Mated SG, page 390](#)
- [Tuning SCTP Parameters for Satellite Channels, page 391](#)

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. 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 must 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 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 20000 packets for SGMP.

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-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-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-link)# cumulative-sack <i>msec</i>	Configures the cumulative selective acknowledgment time-out value for the link.
Router(config-cs7-link)# init-retransmit <i>max-retries</i>	Configures the number of retransmissions for peer initialization messages.
Router(config-cs7-link)# init-timeout <i>msec</i>	Configures the maximum time-out value for retransmission initialization messages.
Router(config-cs7-link)# ip-precedence <i>ip-tos</i>	Sets the IP precedence.
Router(config-cs7-link)# ip-dscp <i>ip-tos</i>	Sets the IP Differential Services Code Point.
Router(config-cs7-link)# keepalive <i>msec</i>	Enable a peer link keepalive interval.
Router(config-cs7-link)# path-retransmit <i>max-retries</i>	Configures path retransmissions on a remote peer address.
Router(config-cs7-link)# peer-timer <i>msec</i>	Configures the alignment-ready timer.
Router(config-cs7-link)# retransmit-timeout <i>milliseconds</i>	Configure the retransmission time-out value on a link.
Router(config-cs7-link)# tx-queue-depth <i>queue-depth</i>	Adjust the number of packets that M2PA will queue for transmission.

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.

Tuning SCTP Parameters for M3UA, SGMP, 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, SGMP, or SUA local instance use the following commands in either CS7 M3UA, CS7 SGMP, 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. Range is 5000 to 65535 bytes. Default is 24000.
Router(config-cs7-m3ua)# retransmit-timeout <i>rto-min</i>	Specifies the minimum retransmission timeout value used when a new SCTP association is started with the local port. Range is 300 to 60000 milliseconds. Default is 1000.
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>	Specifies the minimum retransmission timeout value for the association. Range is 300 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. Range is 100 to 20000 packets. 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 msec	(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 max-returns	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 msec	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 msec	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 msec	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 max-retries	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 class	Specifies the QoS class for the packets sent to the SG Mate.
Router(config-cs7-mated-sg)# retransmit-timeout rto-min	Specifies the minimum retransmission timeout value for the association. Range is 300 to 60000 milliseconds. Default is the value specified under the local port instance.
Router(config-cs7-mated-sg)# tx-queue-depth queue-depth	Determines the onset and abate thresholds for congestion on transmit queue. Specifies the maximum transmit queue depth for the association. Range is 100 to 20000 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 391](#)
- [Tuning Sctp on Satellite Channels, page 392](#)
- [Verifying Sctp Parameters on Satellite Channels, page 394](#)

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.

```
sshtresh = 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 392](#).

**Note**

It is extremely important to understand that the behavior of the SCTP congestion control algorithms are not compliant with RFC 2960 when these parameters are changed to values other than their defaults. These parameters 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-cwd-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)# 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)# idle-cwnd-rate msec	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)# init-cwnd-size msec	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.
Router(config-cs7-ls)# init-timeout msec	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.

Command	Purpose
Router(config-cs7-ls)# 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)# retransmit-timeout <i>rto-min</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 300 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 <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 publications.

- [access-group, page 400](#)
- [access-list, page 401](#)
- [accounting, page 404](#)
- [active-asps-target, page 405](#)
- [addr \(cs7 mlr address-table\), page 406](#)
- [adjacent-sp-restart, page 408](#)
- [allow-multi-message-dialogue, page 409](#)
- [asname \(cs7 gtt application group\), page 410](#)
- [asname \(cs7 mlr result\), page 412](#)
- [asp, page 414](#)
- [assoc-retransmit \(cs7 asp\), page 416](#)
- [assoc-retransmit \(cs7 link\), page 417](#)
- [assoc-retransmit \(cs7 m2pa profile\), page 418](#)
- [assoc-retransmit \(cs7 m3ua\), page 419](#)
- [assoc-retransmit \(cs7 mated-sg\), page 420](#)
- [assoc-retransmit \(cs7 sgmp\), page 421](#)
- [assoc-retransmit \(cs7 sua\), page 422](#)
- [atm nni, page 423](#)
- [block, page 424](#)
- [broadcast, page 425](#)
- [bundling \(cs7 asp\), page 427](#)
- [bundling \(CS7 Link\), page 428](#)
- [bundling \(cs7 m2pa profile\), page 430](#)
- [bundling \(cs7 m3ua\), page 432](#)
- [bundling \(cs7 mated-sg\), page 433](#)
- [bundling \(cs7 profile\), page 434](#)

- [bundling \(cs7 sgmp\), page 436](#)
- [bundling \(cs7 sua\), page 437](#)
- [burst-recovery-timeout, page 438](#)
- [cdpa \(cs7 mlr table trigger\), page 439](#)
- [clear cs7 accounting, page 447](#)
- [cgpa \(cs7 mlr table trigger\), page 444](#)
- [clear cs7 accounting, page 447](#)
- [clear cs7 all, page 448](#)
- [clear cs7 as, page 449](#)
- [clear cs7 asp, page 450](#)
- [clear cs7 dynamic-route, page 451](#)
- [clear cs7 gtt-meas, page 452](#)
- [clear cs7 mated-sg statistics, page 453](#)
- [clear cs7 mtp3 event-history, page 454](#)
- [clear cs7 pointcode event-history, page 455](#)
- [clear cs7 statistics, page 456](#)
- [clear cs7 tcap statistics, page 458](#)
- [clock source \(controller\), page 459](#)
- [clock source \(interface\), page 461](#)
- [cs7 accounting, page 463](#)
- [cs7 address-table replace, page 464](#)
- [cs7 as, page 465](#)
- [cs7 asp, page 467](#)
- [cs7 capability-pc, page 469](#)
- [cs7 clli, page 471](#)
- [cs7 description, page 472](#)
- [cs7 display-name, page 473](#)
- [cs7 distribute-sccp-unsequenced, page 475](#)
- [cs7 fast-restart, page 476](#)
- [cs7 gtt address-conversion, page 477](#)
- [cs7 gtt application-group, page 478](#)
- [cs7 gtt concern-pclist, page 479](#)
- [cs7 gtt load, page 481](#)
- [cs7 gtt map, page 482](#)
- [cs7 gtt map sp, page 485](#)
- [cs7 gtt map ss, page 486](#)
- [cs7 gtt replace-db, page 488](#)
- [cs7 gtt selector, page 489](#)

- [cs7 gws action-set, page 491](#)
- [cs7 gws as, page 493](#)
- [cs7 gws linkset, page 494](#)
- [cs7 gws table, page 495](#)
- [cs7 host, page 497](#)
- [cs7 inhibit, page 499](#)
- [cs7 instance pc-conversion, page 500](#)
- [cs7 instance pc-conversion default, page 501](#)
- [cs7 linkset, page 503](#)
- [cs7 local-peer, page 505](#)
- [cs7 local-sccp-addr-ind, page 507](#)
- [cs7 log, page 509](#)
- [cs7 log checkpoint, page 511](#)
- [cs7 m3ua, page 512](#)
- [cs7 m3ua extended-upu, page 514](#)
- [cs7 mated-sg, page 515](#)
- [cs7 max-dynamic-routes, page 517](#)
- [cs7 mlr address-table, page 518](#)
- [cs7 mlr modify-profile, page 519](#)
- [cs7 mlr options, page 520](#)
- [cs7 mlr result, page 521](#)
- [cs7 mlr ruleset, page 524](#)
- [cs7 mlr table, page 526](#)
- [cs7 msu-rates notification-interval, page 528](#)
- [cs7 msu-rates sample-interval, page 529](#)
- [cs7 msu-rates threshold-default, page 530](#)
- [cs7 msu-rates threshold-proc, page 532](#)
- [cs7 mtp3 event-history, page 534](#)
- [cs7 mtp3 timer, page 536](#)
- [cs7 mtp3 tuning, page 541](#)
- [cs7 multi-instance, page 543](#)
- [cs7 national-options, page 544](#)
- [cs7 network-indicator, page 546](#)
- [cs7 network-name, page 547](#)
- [cs7 nso, page 548](#)
- [cs7 paklog, page 549](#)
- [cs7 point-code, page 551](#)
- [cs7 point-code delimiter, page 552](#)

- [cs7 point-code format, page 553](#)
- [cs7 profile, page 555](#)
- [cs7 prompt enhanced, page 557](#)
- [cs7 qos class, page 558](#)
- [cs7 remote-congestion-msgs, page 559](#)
- [cs7 route-mgmt-sls, page 560](#)
- [cs7 route-table, page 562](#)
- [cs7 save address-table, page 563](#)
- [cs7 save gtt-table, page 564](#)
- [cs7 save log, page 565](#)
- [cs7 save route-table, page 567](#)
- [cs7 sccp gti-conversion, page 568](#)
- [cs7 sccp instance-conversion, page 569](#)
- [cs7 sccp ssn-conversion, page 571](#)
- [cs7 secondary-pc, page 572](#)
- [cs7 sg-event-history, page 573](#)
- [cs7 sgmp, page 574](#)
- [cs7 sls-shift, page 576](#)
- [cs7 snmp dest-max-window, page 577](#)
- [cs7 snmp mgmt-max-window, page 578](#)
- [cs7 sua, page 579](#)
- [cs7 sua-allow-xudt-request, page 581](#)
- [cs7 summary-routing-exception, page 582](#)
- [cs7 tcap tid-timer, page 583](#)
- [cs7 tcap variant, page 584](#)
- [cs7 tfc-pacing-ratio, page 585](#)
- [cs7 uninhibit, page 586](#)
- [cs7 upgrade analysis, page 587](#)
- [cs7 upgrade module, page 590](#)
- [cs7 util-abate, page 591](#)
- [cs7 util-plan-capacity, page 592](#)
- [cs7 util-sample-interval, page 593](#)
- [cs7 util-threshold, page 594](#)
- [cs7 variant, page 595](#)
- [cs7 xua-as-based-congestion, page 597](#)
- [cs7 xua-ssnm-filtering, page 598](#)
- [cs7 xua-tfc-allowed, page 599](#)
- [cumulative-sack \(CS7 ASP\), page 600](#)

- [cumulative-sack \(CS7 Link\)](#), page 601
- [cumulative-sack \(cs7 m2pa profile\)](#), page 602
- [cumulative-sack \(CS7 M3UA\)](#), page 603
- [cumulative-sack \(cs7 mated-sg\)](#), page 604
- [cumulative-sack \(CS7 SGMP\)](#), page 605
- [cumulative-sack \(cs7 sua\)](#), page 606
- [default](#), page 607
- [default result](#), page 609
- [description \(cs7 link\)](#), page 610
- [description \(cs7 linkset\)](#), page 611
- [dest-port \(cs7 mlr ruleset rule\)](#), page 612
- [dest-sme \(cs7 mlr ruleset rule\)](#), page 613
- [dest-sme-table \(cs7 mlr ruleset rule\)](#), page 616
- [dest-smsc \(cs7 mlr ruleset rule\)](#), page 618
- [display-name \(cs7 link\)](#), page 620
- [display-name \(cs7 linkset\)](#), page 621

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	Apply this access list to inbound packets.
out	Apply this access list to outbound packets.

Defaults

No default behavior or values.

Command Modes

CS7 linkset submode

Command History

Release	Modification
12.2(1)MB	This command was introduced.

Usage Guidelines

The access-group command allows you to assign an ITP access list to a linkset to screen either inbound or outbound packets.

Examples

The following example assigns 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** global configuration command. 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	Indicate the specific instance, if the Multiple Instances feature is enabled.
<i>instance-number</i>	Instance number.
compiled	Enable IP access-list compilation.
dynamic-extended	Extend the dynamic ACL.
rate-limit	Simple rate-limit access list.
<i>precedence</i>	Precedence. Valid range is 0 through 7.
mask	Use a precedence bitmask.
<i>precedence-bitmask</i>	Precedence bitmask. Valid range is 0 through 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>	The 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>	The 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	Keyword indicating that pattern-matching is to be used in determining 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>	The 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>	The 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	Permit or deny all (other) packets.
remark line	Include a remark.

Defaults

Any message that does not match any of the access-list entries is, by default, denied. bal configuration

Command History

Release	Modification
12.2(1)MB	This command was introduced for Cisco ITP.
12.2(4)MB	The aftpc , cdpa , cgpa , and selector keywords were added.

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 is a method of screening MSUs on inbound and outbound linkset.

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 keywords **selector** and **cgpa** enable screening on the inbound linkset.

The keywords **aftpc** and **cdpa** enable screening on the outbound linkset.

Examples

The following example defines 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 will cause all SCCP management packets with affected point code 7.5.4 and SSN 10 to be dropped, and 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

To enable accounting of inbound and outbound frames on a linkset, use the **accounting** CS7 linkset submode command. 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 enabled by default.

Command Modes CS7 linkset submode

Command History	Release	Modification
	12.2(1)MB	This command was introduced.

Usage Guidelines Because accounting is enabled by default, only the **no** form of the command will be displayed as output of the **show configuration** command.

Examples The following example disables accounting on the linkset named michael:

```
cs7 linkset michael 10.1.1
no accounting
```

Related Commands	Command	Description
	clear cs7 accounting	Clears the ITP accounting databases.

active-asps-target

To enable sending an “Insufficient ASP Resources Active in AS” Notify message to maintain a minimum number of active ASPs in the AS, use the **active-asps-target** command in CS7 AS configuration mode. To remove the configuration, use the **no** form of this command.

active-asps-target *active-asps-target*

no active-asps-target *active-asps-target*

Syntax Description	<i>active-asps-target</i>	The minimum desired number of active ASPs in the AS. The range is 1 to 4294967295.
---------------------------	---------------------------	--

Defaults	No default behavior or values.
-----------------	--------------------------------

Command Modes	CS7 AS
----------------------	--------

Command History	Release	Modification
	12.2(19)SW	This command was introduced.

Usage Guidelines	When an ASP becomes inactive in a loadshare (bindings or round-robin) or broadcast AS, and the remaining number of ASPs is less than the active-asps-target specification, a Notify message is sent to all inactive ASPs in the AS.
	The AS state remains independent of whether there are sufficient resources active. Because traffic mode is optional on the AS and can be defined by the first active ASP, the active-asp-target value is configurable on all ASes and is ignored if the traffic mode is override.

Examples	The following example sets the minimum desired number of active ASPs in the AS to 50:
	<code>active-asps-target 50</code>

Related Commands	Command	Description
	show cs7 asp	Display ASP information.

addr (cs7 mlr address-table)

To specify an MLR address within the MLR address table, use the **addr** CS7 MLR address table configuration mode command. To remove the definition, use the **no** form of this command.

addr *address* [**exact**] [**result** {**asname** *asname* | **block** | **continue** | **group** *group-name* | **gt** *addr-string* [**tt** *tt* **gti** {**2** | **4** **np** *np* **nai** *nai*} | **pc** *pc* [**ssn** *ssn*] | [**sccp-error** *error*]}]

no addr *address* [**exact**] [**result** {**asname** *asname* | **block** | **continue** | **group** *group-name* **gt** *addr-string* [**tt** *tt* **gti** {**2** | **4** **np** *np* **nai** *nai*} | **pc** *pc* [**ssn** *ssn*]}]

Syntax Description

<i>address</i>	Address of 1 to 20 hexadecimal digits.
exact	(Optional) Configured address must match addr exactly.
result	(Optional) Configure result.
asname	(Optional) Message will be routed to an AS.
<i>asname</i>	AS name.
block	(Optional) Message will be dropped.
continue	(Message) Message processing will continue.
group	(Optional) Message will be routed using an <u>MLR or SMS</u> result group.
<i>group-name</i>	Group-name
gt	(Optional) Specifies that the message will be routed using SCCP global title. The specified address will be placed in the SCCP Called Party Address (CdPA), the routing indicator (RI) will be changed to RI=GT, and then 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 not input in BCD-string format, but in normal form.
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 are in the range 0 through 255.
gti	(Optional) Specifies a Global Title Indicator. (Only specified when cs7 variant is 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 value. (Only specified when the <i>gti</i> value is 4.)
<i>np</i>	Numbering plan value. Valid range is 0 through 15.
nai	(Optional) Specifies a nature of address indicator. (Only specified when the <i>gti</i> value is 4.)
<i>nai</i>	(Optional) Nature of address indicator. Valid range is 0 through 127.
pc	(Optional) Point code message will be routed using PC.
<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 that will support configuring a sccp-error on the block result.

Defaults

No default behavior or values.

Command Modes

CS7 mlr address table configuration

Command History

Release	Modification
12.2(21)SW	This command was introduced.
12.2(25)SW1	Added the ability to configure result gt for MLR address table addresses.

Examples**Example 1**

The following example specifies 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
```

Example 2

The following example specifies 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
```

Related Commands

Command	Description
cs7 mlr address-table	Defines a table of addresses that is 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 the command.

adjacent-sp-restart

no adjacent-sp-restart

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes CS7 linkset submode

Command History	Release	Modification
	12.2(4)MB	This command was introduced.

Examples The following example enables the adjacent-sp-restart process to 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.

allow-multi-message-dialogue

To specify that all messages including multi-message dialogues match the rule, 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

No default behavior or value

Command Modes

CS7 mlr ruleset-rule configuration

Command History

Release	Modification
12.2(25)SW	This command was introduced.

Usage Guidelines

If the **allow-multi-message-dialogue** command is configured, all messages match the rule. If the command is not specified, all messages excluding multi-message dialogues match the rule.

The **allow-multi-message-dialogue** command is allowed for default sms-mo rules, default sms-mt rules, and rules defined with the **all** operation.

Multi-Message dialogues include:

- 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 specifies the **multi-message-dialogue** command:

```
cs7 mlr ruleset ruleset1
rule 10 sms-mt default
allow-multi-message-dialogue
```

Related Commands

Command	Description
rule (cs7 mlr ruleset)	Specifies the rules for a routing trigger within a multi-layer ruleset table and enables CS7 MLR ruleset-rule configuration mode.

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 configuration mode. To remove the configuration, use the **no** form of this command.

asname *as-name* [*cost* | *wf*] [*ssn* *ssn*] {*gt* | *pcssn*}

no asname

Syntax Description

<i>as-name</i>	Application server name. This parameter allows the user to assign a global title translation to an M3UA or SUA AS, instead of a point code and SSN. It 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 (1-8) specifying the priority of the AS name within the application group.
<i>wf</i>	Weighing factor. Any items added to the group require a cost if the multiplicity is specified as cgpa .
gt	Set RI to route on GT.
pcssn	Set RI to route on point code and subsystem number.
ssn	Set subsystem number during translation process.
<i>ssn</i>	Subsystem number

Defaults

No default behavior or values.

Command Modes

CS7 gtt application group configuration

Command History

Release	Modification
12.2(4)MB5	This command was introduced.

Usage Guidelines

The **asname** command allows you to assign 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 the type **gtt** must be configured. Verification of the AS name is performed at execution time.

Examples

The following example configures 2 asnames. AS1 has a cost value of 4 and RI set to route on GT. AS2 has a cost value of 5 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 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*]

no asname *as-name* [**order** *order*] [**weight** *weight*]

Syntax Description

<i>as-name</i>	1 to 12 character name identifying an M3UA or SUA application server name.
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	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 non-zero weighted resources are unavailable. If multiple zero-weighted resources exist, then messages are equally distributed between them if all non-zero weighted resources fail. If not specified, a default weight of 1 is used.

Defaults

If not specified, a default weight of 1 is used.

Command Modes

CS7 mlr result configuration

Command History

Release	Modification
12.2(4)MB	This command was introduced.
12.2(25)SW4	The order keyword was added for the dest-sme-binding mode.

Usage Guidelines

If multiple zero-weighted resources exist, then messages are equally distributed between them if all non-zero 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).

Examples

The following example specifies 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 specifies 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 multi-layer 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 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).
weight	Specifies the weighted round-robin ASP distribution within an AS.
<i>weight</i>	The weight assigned to the ASP. Valid range is 0 through 10. The default weight is 1.

Defaults

No default behavior or values.

Command Modes

CS7 as configuration

Command History

Release	Modification
12.2(4)MB5	This command was introduced.
12.2(21)SW	The weight parameter was introduced.

Usage Guidelines

You can associate multiple ASPs to an AS by specifying multiple **asp** commands.

The ASP name must already be defined using the **cs7 asp** command before it can be associated with an AS.

The **no** form of this command will delete this ASP from the AS definition and will inactivate this 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 parameter 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 there are multiple active ASPs of weight 0, and no other active and uncongested ASPs, packets are evenly distributed to the ASPs of weight 0.

Examples

The following example defines 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)

Retransmissions occur when the sender does not receive an acknowledgement within some specified time period. To configure the maximum number of consecutive retransmissions for the association, 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 through 20. Default is the value specified under the local M3UA or SUA instance.
--------------------	--

Defaults

Default value of *max-retrans* is the value specified under the local M3UA or SUA instance

Command Modes

CS7 asp configuration

Command History

Release	Modification
12.2(4)MB5	This command was introduced.

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 multi-homed.

Examples

The following example sets 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)

Retransmissions occur when the sender does not receive an acknowledgement within some 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 through 20.
Defaults	10 retransmissions	
Command Modes	CS7 link configuration	
Command History	Release	Modification
	12.2(1)MB	This command was introduced.
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 multi-homed.	
Examples	<p>The following example sets the maximum number of retransmissions to 20:</p> <pre>cs7 linkset michael 10.1.1 link 0 sctp 172.18.44.147 7000 7000 assoc-retransmit 20</pre>	
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)

Retransmissions occur when the sender does not receive an acknowledgement within some 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 through 20.
---------------------------	--------------------	---

Defaults	10 retransmissions
-----------------	--------------------

Command Modes	CS7 m2pa profile configuration
----------------------	--------------------------------

Command History	Release	Modification
	12.2(25)SW3	This command was introduced.

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 multi-homed.
-------------------------	--

Examples	The following example defines a profile named m2parfc, specifies that the profile supports M2PA RFC, specifies the assoc-retransmit parameter in the profile, then applies the m2parfc profile to all the links in 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)

Retransmissions occur when the sender does not receive an acknowledgement within some 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 through 20.
Defaults	10 retransmissions	
Command Modes	CS7 m3ua configuration	
Command History	Release	Modification
	12.2(4)MB5	This command was introduced.
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 multi-homed.	
Examples	The following example sets the maximum number of retransmissions to 20: <pre>cs7 m3ua 2905 offload local-ip 4.4.4.4 assoc-retransmit 20</pre>	
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.

assoc-retransmit (cs7 mated-sg)

Retransmissions occur when the sender does not receive an acknowledgement within some 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 through 20.
--------------------	---

Defaults

The value of *max-retrans* defaults to the value specified under the local port instance.

Command Modes

CS7 mated-sg configuration

Command History

Release	Modification
12.2(4)MB5	This command was introduced.

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 multi-homed.

Examples

The following example sets 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)

Retransmissions occur when the sender does not receive an acknowledgement within some 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 through 20.
Defaults	10 retransmissions	
Command Modes	CS7 sgmp configuration	
Command History	Release	Modification
	12.2(4)MB5	This command was introduced.
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 multi-homed.	
Examples	The following example sets the maximum number of retransmissions to 20: <pre>cs7 sgmp 5000 local-ip 4.4.4.4 assoc-retransmit 20</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.

assoc-retransmit (cs7 sua)

Retransmissions occur when the sender does not receive an acknowledgement within some 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 through 20.	
Defaults	10 retransmissions	
Command Modes	CS7 sua configuration	
Command History	Release	Modification
	12.2(4)MB5	This command was introduced.
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 multi-homed.	
Examples	The following example sets 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 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 the command.

atm nni

no atm nni

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(4)MB2	This command was introduced.

Examples

The following example shows an ATM interface configured for NNI:

```
interface atm1/0/0
 no shutdown
 atm nni
 pvc atm_pvc1 0/5 qsaal
```

Related Commands

Command	Description
pvc	Specifies the PVC.

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

No default behavior or values

Command Modes

CS7 asp configuration

Command History

Release	Modification
12.2(4)MB5	This command was introduced.

Usage Guidelines

There are significant differences between the **block** and **shutdown** CS7 ASP submode commands:

The **shutdown** command terminates the SCTP association with this ASP. New SCTP associations will be rejected if the ASP is in shutdown mode.

The **block** command sends an unsolicited asp-inactive acknowledgement. However, the ITP will not terminate the SCTP association.

When the ASP retries, in the shutdown case, the association must be reestablished, asp-up sent and failed. For block, ASP-ACT may just be retried.

Examples

The following example blocks 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 broadcast, 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	Broadcast all route management messages.
tfa	Broadcast TFA.
tfp	Broadcast TFP.
txa-txr	Broadcast TFA/TCA and TFR/TCR.
txp	Broadcast TFP/TCP.

Defaults

The default for ANSI, ITU and China variants is broadcast all route management messages.

Command Modes

CS7 linkset configuration

Command History

Release	Modification
12.2(4)MB	This command was introduced.

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 given adjacent node, that node can become temporarily overloaded, because processing such a large number of management messages can be processor intensive. The **broadcast** command allows you to regulate the broadcast of route management messages and enables you to prevent this potential overload situation. 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 they attempt to route the next MSU to the concerned destination via the ITP, the ITP will send a response method TFP or TFR (if the destination status were to be inaccessible or restricted). In the case of response method TFP the MSU is dropped.

Examples

ANSI, ITU, China Variants

The following example enables the broadcast of all route management messages on linkset1:

```
cs7 linkset linkset1
 broadcast all
```

The following example disables the broadcast of all route management messages on linkset1:

```
cs7 linkset linkset1
 no broadcast all
```

ANSI Variant

The following example enables the broadcast of TFA/TCA and TFR/TCR messages on linkset1:

```
cs7 linkset linkset1
 broadcast txa-txr
```

ITU or China Variants

The following example enables 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, in milliseconds, that SCTP will wait for messages for bundling. Valid range is 5 through 1000 milliseconds. Default is the value specified under the M3UA or SUA instance.
---------------------------	-------------	--

Defaults	Packet defaults to the value specified under the local port instance.
-----------------	---

Command Modes	CS7 asp configuration
----------------------	-----------------------

Command History	Release	Modification
	12.2(4)MB5	This command was introduced.

Usage Guidelines	<p>Packets sent while bundling is enabled can experience a delay before transmission. The delay is the amount of time the implementation waits for messages to encourage bundling. When bundling messages, the resulting packet (including IP and SCTP headers) must be less than or equal to the current path MTU.</p> <p>During periods of congestion, the implementation bundles messages (when possible) even if bundling is disabled. During periods of congestion, abatement messages are bundled whenever possible, with no impact to performance.</p>
-------------------------	---

Examples	The following example sets 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, in milliseconds, to wait for messages for bundling. Valid range is 5 through 1000 milliseconds. Default is 5 milliseconds.
-------------	--

Defaults

Enabled.

The default maximum time to wait for messages for bundling is 5 milliseconds.

Command Modes

CS7 link configuration

Command History

Release	Modification
12.2(1)MB	This command was introduced, enabling bundling.
12.2(4)MB	Added bundling capability between MTP3 on the RSP and MTP2 on the linecard.

Usage Guidelines

Packets sent while bundling is enabled can experience a delay before transmission. The delay is the amount of time the implementation waits for messages to encourage bundling. When messages are bundled, the resulting packet must be less than or equal to the current path MTU.

During periods of congestion, the implementation bundles messages (when possible) even if bundling is disabled. During periods of congestion, abatement messages are bundled whenever possible, with no impact to performance.

Bundling for MTP2 packets is supported on the Cisco 7500 router only.

MTP2 parameters can also be specified in a CS7 profile.

Examples

The following example sets 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, in milliseconds, to wait for messages for bundling. Valid range is 5 through 1000 milliseconds. Default is 5 milliseconds.
-------------	--

Defaults

Enabled.

The default maximum time to wait for messages for bundling is 5 milliseconds.

Command Modes

CS7 m2pa profile configuration

Command History

Release	Modification
12.2(25)SW3	This command was introduced.

Usage Guidelines

Packets sent while bundling is enabled can experience a delay before transmission. The delay is the amount of time the implementation waits for messages to encourage bundling. When messages are bundled, the resulting packet must be less than or equal to the current path MTU.

During periods of congestion, the implementation bundles messages (when possible) even if bundling is disabled. During periods of congestion, abatement messages are bundled whenever possible, with no impact to performance.

Bundling for MTP2 packets is supported on the Cisco 7500 router only.

MTP2 parameters can also be specified in a CS7 profile.

Examples

The following example defines a profile named m2parfc, specifies that the profile supports M2PA RFC, specifies the **bundling** parameter in the profile, then applies the m2parfc profile to all the links in linkset named to_nyc:

```
cs7 profile m2parfc
  m2pa
    bundling 100
  .
  .
  .
cs7 linkset to_nyc
  profile m2parfc
```

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 if 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, in milliseconds, that SCTP will wait for messages for bundling. Valid range is 5 through 1000 milliseconds. Default is 5 milliseconds.
-------------	--

Defaults

Enabled.

The default maximum time that SCTP will wait for messages for bundling is 5 milliseconds.

Command Modes

CS7 m3ua configuration

Command History

Release	Modification
12.2(4)MB5	This command was introduced.

Usage Guidelines

Packets sent while bundling is enabled can experience a delay before transmission. The delay is the amount of time the implementation waits for messages to encourage bundling. When bundling messages, the resulting packet (including IP and SCTP headers) must be less than or equal to the current path MTU.

During periods of congestion, the implementation bundles messages (when possible) even if bundling is disabled. During periods of congestion, abatement messages are bundled whenever possible, with no impact to performance.

Examples

The following example sets 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, in milliseconds, that SCTP will wait for messages for bundling. Valid range is 5 through 1000 milliseconds. Default is the value specified under the local port instance.
-------------	---

Defaults

Packet defaults to the value specified under the SGMP instance.

Command Modes

CS7 mated-sg configuration

Command History

Release	Modification
12.2(4)MB5	This command was introduced.

Usage Guidelines

Packets sent while bundling is enabled can experience a delay before transmission. The delay is the amount of time the implementation waits for messages to encourage bundling. When bundling messages, the resulting packet (including IP and SCTP headers) must be less than or equal to the current path MTU.

During periods of congestion, the implementation bundles messages (when possible) even if bundling is disabled. During periods of congestion, abatement messages are bundled whenever possible, with no impact to performance.

Examples

The following example sets 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, in milliseconds, to wait for messages for bundling. Valid range is 5 through 1000 milliseconds. Default is 5 milliseconds.
-------------	--

Defaults

Enabled.

The default maximum time to wait for messages for bundling is 5 milliseconds.

Command Modes

CS7 profile configuration

Command History

Release	Modification
12.2(4)MB	This command was introduced.

Usage Guidelines

Packets sent while bundling is enabled can experience a delay before transmission. The delay is the amount of time the implementation waits for messages to encourage bundling. When messages are bundled, the resulting packet must be less than or equal to the current path MTU.

During periods of congestion, the implementation bundles messages (when possible) even if bundling is disabled. During periods of congestion, abatement messages are bundled whenever possible, with no impact to performance.

Bundling for MTP2 packets is supported on the Cisco 7500 router only.

Examples

The following example defines a profile named timers, configures the profile to support MTP2, configures the packet bundling, t1, and t2 settings, then applies the timers profile to all the links in linkset 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 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 if 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, in milliseconds, that SCTP will wait for messages for bundling. Valid range is 5 through 1000 milliseconds. Default is 5 milliseconds
-------------	---

Defaults

Enabled.

The default maximum time that SCTP will wait for messages for bundling is 5 milliseconds.

Command Modes

CS7 sgmp configuration

Command History

Release	Modification
12.2(4)MB5	This command was introduced.

Usage Guidelines

Packets sent while bundling is enabled can experience a delay before transmission. The delay is the amount of time the implementation waits for messages to encourage bundling. When bundling messages, the resulting packet (including IP and SCTP headers) must be less than or equal to the current path MTU.

During periods of congestion, the implementation bundles messages (when possible) even if bundling is disabled. During periods of congestion, abatement messages are bundled whenever possible, with no impact to performance.

Examples

The following example sets 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 if 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, in milliseconds, that SCTP will wait for messages for bundling. Valid range is 5 through 1000 milliseconds. Default is 5 milliseconds
---------------------------	-------------	---

Defaults	Enabled. The default maximum time that SCTP will wait for messages for bundling is 5 milliseconds.
-----------------	---

Command Modes	CS7 sua configuration
----------------------	-----------------------

Command History	Release	Modification
	12.2(4)MB5	This command was introduced.

Usage Guidelines	<p>Packets sent while bundling is enabled can experience a delay before transmission. The delay is the amount of time the implementation waits for messages to encourage bundling. When bundling messages, the resulting packet (including IP and SCTP headers) must be less than or equal to the current path MTU.</p> <p>During periods of congestion, the implementation bundles messages (when possible) even if bundling is disabled. During periods of congestion, abatement messages are bundled whenever possible, with no impact to performance.</p>
-------------------------	---

Examples	<p>The following example sets the bundling interval to 500 milliseconds:</p> <pre>cs7 sua 15000 local-ip 4.4.4.4 bundling 500</pre>
-----------------	---

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 in milliseconds. The valid range is 1000 through 10000 msec. The default is 4000 msec.
-------------	---

Defaults

4000 msec.

Command Modes

CS7 as configuration

Command History

Release	Modification
12.2(4)MB5	This command was introduced.

Examples

The following example sets the burst-recovery-timeout to 1000 msec:

```
cs7 as BLUE m3ua
  burst-recovery-timeout 1000
```

Related Commands

Command	Description
cs7 as	Defines an Application Server.

cdpa (cs7 mlr table 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 asname | gt gt [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 asname | gt gt [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 not input in BCD-String format, but in normal form.
<i>gt-addr-type</i>	<p>(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.</p> <p>tt <i>tt</i> [gti <i>gti</i>] [np <i>np</i> nai <i>nai</i>]</p> <p>tt Identifies the translation type specified within the address.</p> <p><i>tt</i> An integer value from 0 to 255.</p> <p>gti Identifies the global title indicator value for the specified address. This value is only specified when cs7 variant is ITU or China.</p> <p><i>gti</i> Integer value of 2 or 4.</p> <p>np Identifies the numbering plan of the specified address. Only specified when the gti parameter value is 4.</p> <p><i>np</i> Integer value from 0 to 15.</p> <p>nai Identifies the nature of specified address. Only specified when the gti parameter value is 4.</p> <p><i>nai</i> Integer value from 0 to 127.</p>
pc	Specifies that the trigger will be matched if it contains the specified point code. The PC within the SCCP CgPA will be inspected first. If the PC is not present, then the OPC is used.
<i>point-code</i>	The point code in variant-specific point-code format.
ssn	(Optional) Route based on PC and subsystem number.
<i>ssn</i>	Subsystem number in decimal. Valid range is 2 to 255.

block	This trigger-action specifies that messages matching this trigger should be dropped. The block parameter is ignored if combination triggers are defined within the CS7 MLR trigger mode.
continue	This trigger-action specifies that messages matching this trigger should be routed as received. This is the same behavior as if no primary trigger had been matched. The continue parameter is ignored if combination triggers are defined within the 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	Result trigger action specifies route the message based on the trigger alone. Result groups with dest-sme-binding mode are not valid trigger results.
pc	Route based on point code.
<i>pc</i>	Point code
ssn	(Optional) Specify subsystem number.
<i>ssn</i>	Subsystem number.
asname	Route based on AS name.
<i>asname</i>	AS name.
gt	Route based on Global Title.
<i>gta</i>	Global title address.
group	Route based on result group.
<i>group-name</i>	Result group name.

Defaults

No default behavior or value.

Command Modes

CS7 MLR trigger configuration

Command History

Release	Modification
12.2(4)MB	This command was introduced.
12.2(21)SW	The continue keyword was added.
12.2(25)SW3	The selector keyword was added.
12.2(25)SW4	The result trigger action was added.

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 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. Once 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 occurs, then the packet is not MLR routed. If no secondary triggers have been defined then MLR processing continues based on the primary trigger only.

If you configure a secondary address in the 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 CGPA 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.

The configurable **result** trigger action 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 simply redirected as indicated in the trigger result. Result groups with dest-sme-binding mode are not valid trigger results.

Examples

The following example creates a combination trigger based on the combination of the primary trigger (the CgPA) and the secondary trigger (the CdPA). The example specifies that ruleset-5 should be applied if the combination trigger is found:

```
cs7 mlr table sms-router
trigger cgpa gt 9991117770
cdpa gt 9991116 ruleset ruleset-5
```

The following example creates 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 creates a combination trigger based on the combination of the primary trigger (the CgPA) and the secondary trigger (the CdPA). If a messages matches the trigger, the message is redirected to the specified 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 multi-layer routing table.
default	Specifies the routing of packets on primary trigger when defined secondary triggers are not matched.
show cs7 mlr table	Displays the multi-layer SMS routing information.
trigger cgpa	Specifies a primary routing trigger that is located in the SCCP calling party address field of the incoming MSU.

cgpa (cs7 mlr modify-profile)

To modify the calling party address (CgPA) use the **cgpa** command within the cs7 mlr modify-profile submode. To disable cgpa modification, 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.	
	Note	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 CgPA with RI=SSN, then the GT modifications are simply ignored.	
prefix	The prefix keyword specifies that prefix modification will be performed on the address.	
<i>prefix-remove-num</i>	An integer in the range of 1 to 15 which defines the number of prefix digits to remove from the address. If no prefix digits are to be removed, then '*' should be specified. 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>	An 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 to be 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 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 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>	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. Only specified when the gti parameter 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>	The 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 Modes `cfg-cs7-mlr-modify` submode

Command History 12.2(18)IXC This command was introduced.

Examples

```
cs7 mlr modify-profile SRISM gsm-map sri-sm
orig-smsc prefix 2 351
cgpa gt prefix 2 351
```

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 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 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).

For prefix-based GT address translation, you can 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. If the resulting modified address exceeds the maximum allowed number of digits, then MLR will fail the modification and discard the packet by default. You can optionally configure the desired action for failed modifications using the modify-failure command within the MLR options submode.

**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 (cs7 mlr option)	Specifies the desired action when MLR packet modification fails.

cgpa (cs7 mlr table 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 asname | gt gta [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 asname | gt gta [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 not input in BCD-String format, but in normal form.
<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 only specified when cs7 variant is ITU or China. <i>gti</i> 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> 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.
pc	Specifies that the trigger will be matched if it contains the specified point code. The PC within the SCCP CdPA will be inspected first. If the PC is not present, then the DPC in the routing label is used.
<i>point-code</i>	The point code in variant-specific point-code format.
ssn	(Optional) Route based on PC and subsystem number.
<i>ssn</i>	Subsystem number in decimal. Valid range is 2 to 255.
block	This trigger-action specifies that messages matching this trigger should be dropped. The block parameter is ignored if combination triggers are defined within the CS7 MLR trigger mode.

continue	This trigger-action specifies that messages matching this trigger should be routed as received. This is the same behavior as if no primary trigger had been matched. The continue parameter is ignored if combination triggers are defined within the 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	Result trigger action specifies route the message based on the trigger alone. Result groups with dest-sme-binding mode are not valid trigger results.
pc	Route based on point code.
<i>pc</i>	Point code
ssn	(Optional) Route based on PC and subsystem number.
<i>ssn</i>	Subsystem number.
asname	Route based on AS name.
<i>asname</i>	AS name.
gt	Route based on Global Title.
<i>gta</i>	Global title address.
group	Route based on result group.
<i>group-name</i>	Result group name.

Defaults

No default behavior or value.

Command Modes

CS7 MLR trigger configuration

Command History

Release	Modification
12.2(4)MB	This command was introduced.
12.2(21)SW	The continue keyword was added.
12.2(25)SW3	The selector keyword was added.
12.2(25)SW4	The result trigger action was added.

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 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. Once 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 occurs, then the packet is not MLR routed. If no secondary triggers have been defined, then MLR processing continues based on the primary trigger only.

If you configure a secondary address in the 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.

The configurable **result** trigger action 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 simply redirected as indicated in the trigger result. Result groups with dest-sme-binding mode are not valid trigger results.

Examples

The following example creates 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 specifies that ruleset-5 should be applied if the combination trigger is found:

```
cs7 mlr table sms-router
trigger cdpa gt 9991117770
cgpa gt 9991116 ruleset ruleset-5
```

The following example creates 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 creates 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 the specified 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 multi-layer routing table.
default	Creates a trigger to be used if all other subtriggers are unmatched.
show cs7 mlr table	Displays the multi-layer SMS routing information.
trigger cdpa	Specifies a routing trigger that is located in the SCCP called party address field of the incoming MSU.

clear cs7 accounting

To clear the ITP accounting databases, use the **clear cs7 accounting** EXEC command.

clear cs7 [*instance-number*] **accounting** [**access-violations** | **gtt** | **unroutable**] [**checkpoint**]

Syntax Description

<i>instance-number</i>	Instance number.
access-violations	Clears Cisco ITP access-violations database.
checkpoint	Checkpointed data.
gtt	Clear SCCP GTT accounting database.
unroutable	Clear unroutable database.

Command Modes

EXEC

Command History

Release	Modification
12.2(1)MB	This command was introduced.
12.2(4)MB	The gtt keyword was added.
12.2(25)SW	The unroutable keyword was added.

Usage Guidelines

The **clear cs7 accounting** command resets counters. It is useful in debugging, to track new message activity.

This command can be issued either globally or on an instance.

Examples

The following example clears the ITP access violations database:

```
clear cs7 accounting access-violations
```

Related Commands

Command	Description
show cs7 accounting	Displays ITP 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) Clear all including all checkpoint tables.
	<i>instance-number</i>	Instance number.

Command Modes	EXEC
---------------	------

Command History	Release	Modification
	12.2(4)MB	This command was introduced.

Usage Guidelines	This command can be issued either globally or on an instance.
------------------	---

Examples	The following example clears 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	Clear all

Command Modes

EXEC

Command History

Release	Modification
12.2(4)MB5	This command was introduced.

Examples

The following example clears 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	Clear all

Command Modes	EXEC
----------------------	------

Command History	Release	Modification
	12.2(4)MB5	This command was introduced.

Examples	The following example clears all application server process statistics: clear cs7 asp statistics all
-----------------	---

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 all
```

Syntax Description

<i>instance-number</i>	Instance number.
all	Clear all dynamic routes.
<i>minutes</i>	Purge only if older than specified time, in minutes. Range is 0 to 20160 minutes.

Command Modes

EXEC

Command History

Release	Modification
12.2(4)MB5	This command was introduced.

Usage Guidelines

This command can be issued either globally or on an instance.

Examples

The following example clears all dynamic routes:

```
clear cs7 dynamic-route all
```

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.
Command Modes	EXEC	
Command History	Release	Modification
	12.2(4)MB	This command was introduced.
Usage Guidelines	This command can be issued either globally or on an instance.	
Examples	The following example clears all GTT measurements:	
	<pre>clear cs7 gtt-meas</pre>	
Related Commands	Command	Description
	show cs7 gtt measurements	Displays a summary of CS7 GTT/SCCP measurements.

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.
---------------------------	--

Command Modes	EXEC
----------------------	------

Command History	Release	Modification
	12.2(4)MB5	This command was introduced.

Examples	The following example clears all SG mated pair statistics: <code>clear cs7 mated-sg statistics</code>
-----------------	--

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 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.
------------------------	------------------

Command Modes

EXEC

Command History

Release	Modification
12.2(1)MB	This command was introduced.

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, since vital information will be lost.

This command can be issued either globally or on an instance.

Examples

The following example clears the MTP3 event history log:

```
clear cs7 mtp3 event history
```

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.
------------------------	------------------

Command Modes

EXEC

Command History

Release	Modification
12.2(4)MB5	This command was introduced.

Examples

The following example clears 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 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>	The name of the linkset.
<i>link</i>	The number of the link.

Command Modes

EXEC

Command History

Release	Modification
12.2(1)MB	This command was introduced.

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 desired to see statistics counted.

The following statistics are kept:

- MSU In
- MSU Out
- LSSU In
- LSSU Out
- ByteCnt In
- ByteCnt Out
- Drop

Statistics are displayed via the **show cs7 linkset statistics** command

Examples

The following example resets to zero all counters for all linksets, then resets 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 measurements, use the **clear cs7 tcap statistics** EXEC command.

clear cs7 [*instance-number*] **tcap statistics**

Syntax Description

<i>instance-number</i>	Instance number.
------------------------	------------------

Command Modes

EXEC

Command History

Release	Modification
12.2(4)MB5	This command was introduced.

Usage Guidelines

This command can be issued either globally or on an instance.

Examples

The following example clears all CS7 TCAP measurements:

```
clear cs7 tcap statistics
```

Related Commands

Command	Description
show cs7 tcap	Displays TCAP information.

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	Specifies that clocking for all nodes is derived from one designated source.
	line	Specifies that clocking is derived from the external source to which the port is connected.
	primary	Specifies the primary source of clock.
	secondary	Specifies the secondary source of clock.
	<i>priority</i>	Specifies the priority of the clock source. The valid range is 1 to 8.
	free-running	Specifies a free-running clock derived from the oscillator on the motherboard.
	internal	Specifies that clocking is derived from the controller's internal phase-locked loop (PLL).

Defaults	line
----------	------

Command Modes	Controller configuration
---------------	--------------------------

Command History	Release	Modification
	10.3	This command was introduced.
	11.1	This command was modified to include the T3 serial port adapter and PA-T3 serial port adapter.
	12.2(8)T	This command was modified to include free-running keyword.
	12.2(4)MB	This command was modified to include the bits keyword and the <i>priority</i> argument.

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 specifies BITS clock source as the primary clock:
----------	---

```
controller t1 4/0/7
clock source bits primary
```

■ clock source (controller)

Related Commands

Command	Description
framing	Selects the frame type for the T1 or E1 data line.
linecode	Selects the linecode type for the T1 or E1 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	Specifies that the interface will clock its transmitted data from a common clock source.
	internal	Specifies that the interface will clock its transmitted data from its internal clock.
	line	Specifies that the interface will clock its transmitted data from a clock recovered from the line's receive data stream. This is the default.
	<i>interface-number</i>	Specific physical link or port number of the common clock source. Valid range is 0 - 7.

Defaults	line
----------	------

Command Modes	Interface configuration
---------------	-------------------------

Command History	Release	Modification
	12.2(23)SW1	The common parameter was added to provide a common BITS clock to IMA interfaces in the ITP.

Usage Guidelines

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 crossover cabled to the SS7 port adapter.

As of IOS Release 12.2(23)SW1, this functionality is available for T1 IMA PAs only. E1 support will be available in a future release.

Examples

The following example provides 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.

```

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

```

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 the command.

cs7 accounting { **checkpoint-interval** *min* | **checkpoint-limit** *entries* | **global-gtt** | **global-mtp3** | **global-unrouteable** | **gtt-checkpoint-interval** *min* }

Syntax Description		
checkpoint-interval <i>min</i>		Specifies an accounting checkpoint interval, in minutes. The range is 1 through 3600 minutes. Default is 5 minutes.
checkpoint-limit <i>entries</i>		Specifies the maximum entries of 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-unrouteable		Enables unrouteable accounting on all linksets.
gtt checkpoint-interval <i>min</i>		Specifies the GTT accounting checkpoint interval, in minutes. The range is 1 through 3600 minutes. Default is 5 minutes.

Defaults

Default accounting checkpoint interval is 5 minutes.

Default GTT accounting checkpoint interval is 5 minutes.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)MB	This command was introduced.

Usage Guidelines

The global-gtt, global-mtp3, and global-unrouteable keywords have the same effect

Examples

The following example sets 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** } *tablename URL*

nocs7 address-table replace { **mlr** | **sms** } *tablename URL*

Syntax Description

mlr	Specifies table type mlr .
sms	Specifies table type sms .
<i>tablename</i>	Identifies the existing address table that is to be replaced.
<i>URL</i>	The user-assigned local or remote location representing the file name and path from which the file will be replaced.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(25)SW	This command was introduced.

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 replaces an SMS address table named addrtbl1 with the file at disk0:smsaddrtbl:

```
cs7 address-table replace sms addrtbl1 disk0:smsaddrtbl
```

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**}

no [**instance** *instance-number*] **cs7 as** *as-name* {**m3ua** | **sua**}

Syntax Description	
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.

Defaults No default behavior or values.

Command Modes Global configuration

Command History	Release	Modification
	12.2(4)MB5	This command was introduced.

Usage Guidelines

- You must configure the ASPs before you configure the AS.
- You must specify both a routing key and at least 1 ASP in the AS submode, or this 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 the CS7 AS submode. In CS7 AS submode, you can configure the routing-key, the ASP, the traffic-mode AS parameters and QoS class. You cannot modify the parameters of an active AS.
- When an AS is inactivated, the ASPs associated with this AS are also inactivated for this routing context by generating a NOTIFY with the routing context.

Examples

The following example configures an M3UA AS named BLUE:

```
cs7 as BLUE m3ua
```

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 multi-instance	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.
routing-key (CS7 AS)	Specifies the routing key for the AS.
show cs7 as	Displays AS and routing key information.
shutdown (cs7 as)	Disables an AS without deleting the configuration.
traffic-mode	Specifies the traffic mode of operation for the ASP within an 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>	The ASP name is a unique name used to identify 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 parameter is used for validation. The SCTP connection requests from the ASP must come in with this remote port number. If 2 ASPs are configured with the same remote IP address, then the remote port and local port is used to differentiate between the 2 ASPs. If a remote port of 0 is configured, the ASP will match on any remote port (providing remote-ip and local port 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) The m3ua keyword indicates that this is an M3UA ASP. This value must match the protocol of the specified local port.
sua	(Optional) The sua keyword indicates that this is an SUA ASP. This value must match the protocol of the specified local port.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)MB5	This command was introduced.

Usage Guidelines

The **cs7 asp** command allows you to define an ASP and enables the 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 be failed if the ASP is not associated with an AS. An ASP may be associated with multiple ASs.

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 will be 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** form of the **cs7 asp** command deletes this ASP definition from configuration. If an association is up with this ASP, you must first shutdown the ASP and remove the ASP from all CS7 AS definitions before this command can be deleted from the configuration.

In the CS7 ASP submode, you can disable the ASP by entering the **shutdown** or **block** commands. New SCTP associations will be rejected if the ASP is in shutdown mode.

You cannot delete an ASP that is currently configured in an AS. You must first remove this ASP from the AS configuration.

You must specify at least 1 remote-ip address in the ASP submode, or this incomplete ASP definition will be deleted.

This command is not instance related and cannot be specified with the **instance** keyword.

Examples

The following example configures 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 time-out 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)	Configure 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 capability-pc

To configure the capability point code for the 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*] **capability-pc** *zone.region.sp*

no cs7 [*instance instance*] **capability-pc** *zone.region.sp*

Syntax Description	
instance	(Optional) Configure 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 through 7. The default instance is instance 0.
<i>zone.region.sp</i>	The capability point code.

Defaults No default behavior or values

Command Modes Global configuration

Command History	Release	Modification
	12.2(4)MB	This command was introduced.
	12.2(25)SW1	ITP supports multiple capability points (Up to 200 per instance).

Usage Guidelines

The ITP supports configuration of up to 200 capability point codes per 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, a capability point code could be assigned to a mated pair of ITPs that share a GTT database for redundancy purposes. In this case all SCCP messages could be directed to a single “capable” point-code and either ITP could handle the processing.

Examples

The following example shows excerpts from two separate ITP configurations, with both ITPs 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
```

■ **cs7 capability-pc**

```
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 point-code	Assigns a local point code to an instance.
cs7 variant	Specifies the variant for an instance.
cs7 multi-instance	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 Code (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. Length of <i>line</i> can be from 1 to 11 alphanumeric characters.
--------------------	---

Defaults	No default behavior or values
----------	-------------------------------

Command Modes	Global configuration
---------------	----------------------

Command History	Release	Modification
	12.2(4)MB	This command was introduced.

Usage Guidelines	<p>The CLLI <i>line</i> value will be included on traps that apply to the SS7 resources on the ITP. The value will also be used by network management stations.</p> <p>Complete listings of geographical and geopolitical codes can be found in the BR 751-401-xxx series and BR 751-100-055, respectively.</p> <p>This command is not instance related and cannot be specified with the instance keyword.</p>
------------------	---

Examples	The following example defines a common language location code for the ITP:
----------	--

```
cs7 clli QSWYNJPIDS5
```

Related Commands	Command	Description
	show running config	Displays the contents of the currently running configuration file.

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 through 7. The default instance is instance 0.
<i>line</i>	Text string description of the ITP. Length of <i>line</i> can be from 1 to 254 alphanumeric characters.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)MB	This command was introduced.

Usage Guidelines

The **cs7 description** command is used to provide 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 are two examples of 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 allows you to assign 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) Assign a descriptive name to an ITP instance.
<i>instance-number</i>	Instance number. The valid range is 0 through 7. The default instance is instance 0.
<i>line</i>	Text string description or the ITP point code formatted as an ASCII string in dotted decimal format. Length of <i>line</i> can 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(4)MB	This command was introduced.

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 are two examples of configuring 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 Cisco 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 the 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) Specifies the particular instance with a valid range of 0 through 7. The default is 0.

Defaults The default behavior is in-sequence delivery of SSCP traffic.

Command Modes Global configuration

Command History	Release	Modification
	12.2(25)SW9	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, ITP overrides the in-sequence delivery of SCCP traffic.

Examples The following example two examples enable **cs7 distribute-sccp-sequenced**:

```
cs7 distribute-sccp-sequenced
```

or

```
cs7 instance 1 distribute-sccp-sequenced
```

Related Commands	Command	Description
	cs7 multi-instance	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 Cisco 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 the 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 through 7. The default instance is instance 0.

Defaults

The default behavior is to include distributed links in round-robin selection.

Command Modes

Global configuration

Command History

Release	Modification
12.2(1)MB	This command was introduced.
12.2(4)MB	The instance keyword was added.

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 example two examples enable **cs7 distribute-sccp-unsequenced**:

```
cs7 distribute-sccp-unsequenced
```

```
cs7 instance 1 distribute-sccp-unsequenced
```

Related Commands

Command	Description
cs7 multi-instance	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 the command.

cs7 [*instance instance-number*] **fast-restart**

no cs7 [*instance instance-number*] **fast-restart**

Syntax Description

instance	(Optional) Enable MTP3 fast restart on an instance.
<i>instance-number</i>	Instance Number. The valid range is 0 through 7. The default instance is instance 0.

Defaults

Fast restart is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(1)MB	This command was introduced.
12.2(4)MB	The instance keyword was added.

Usage Guidelines

When an SP restarts, it normally waits to receive a TRA from each of its adjacent nodes before it will mark the links available for passing user traffic. If TRAs are not received from each of the adjacent nodes, it will eventually time out (30 seconds default) and start passing user traffic.

The **cs7 fast-restart** command bypasses this so that the SP will not need to wait for TRAs from the adjacent nodes.

Examples

The following two examples enable fast restart:

```
cs7 fast-restart
```

```
cs7 instance 2 fast-restart
```

Related Commands

Command	Description
cs7 multi-instance	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 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** *tablename*

no **cs7** [*instance instance-number*] **gtt address-conversion** *tablename*

Syntax Description	instance	(Optional) Configure a global title address conversion table on an instance
	<i>instance-number</i>	Instance number. The valid range is 0 through 7. The default instance is instance 0.
	<i>tablename</i>	Global Title Address Conversion table name. The table name may be 1-12 characters in length.

Defaults No default behavior or values

Command Modes Global configuration

Command History	Release	Modification
	12.2(4)MB2	This command was introduced.

Usage Guidelines The address conversion tables are used to specify mappings such as E.212 - E.214 address conversion. Issuing the **cs7 gtt address-conversion** command enables CS7 GTT address conversion submode. After you have defined a GTT address conversion table, you can apply the table on a GTT selector basis.

Examples The following command specifies a global title address conversion table named conv1:

```
cs7 gtt address-conversion conv1
```

The following command specifies a global title address conversion table named conv1 for instance 1:

```
cs7 instance 2 gtt address-conversion conv1
```

Related Commands	Command	Description
	cs7 multi-instance	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, use the **cs7 gtt application-group** command in global configuration mode. To remove the configuration, use the **no** form of the command.

cs7 [*instance instance-number*] **gtt application-group** *name*

no cs7 [*instance instance-number*] **gtt application-group** *name*

Syntax Description	instance	(Optional) Configure a GTT application group on an instance.
	<i>instance-number</i>	Instance number. The valid range is 0 through 7. The default instance is instance 0.
	<i>name</i>	The name of the application-group that will be specified in the gta app-grp CS7 GTT selector submode command.

Defaults No default behavior or values

Command Modes Global configuration

Command History	Release	Modification
	12.2(4)MB	This command was introduced.

Usage Guidelines The application-group must be defined prior to defining the gta subcommands that use it.

Examples The following example configures an application group named group1:

```
cs7 gtt application-group group1
```

The following example configures an application group named group1 on instance 3:

```
cs7 instance 3 gtt application-group group1
```

Related Commands	Command	Description
	cs7 multi-instance	Enables multiple instances of a variant and network indicator combination.
	gta app-grp	Translates a GTA to a GTT application group.
	multiplicity	Specifies a method for selecting destination in the application group.
	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 the command. To delete the concerned point code list, remove all point codes from the list.

cs7 [*instance instance-number*] **gtt concern-pclist** *listname cpc*

no cs7 [*instance instance-number*] **gtt concern-pclist** *listname cpc*

Syntax Description

<i>cpc</i>	Concerned point code, in the form zone.region.sp.
instance	(Optional) Configure a GTT concerned point code list on an instance.
<i>instance-number</i>	Specifies the instance. The valid range is 0 through 7. The default instance is instance 0.
<i>name</i>	The name of the concerned point code list.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)MB	This command was introduced.

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 creates 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 creates 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 multi-instance	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

To specify the URL location from which, upon ITP reload, the GTT database will be loaded, use the **cs7 gtt load** command in global configuration mode.

cs7 [*instance instance-number*] **gtt load** *url* [**execute**]

Syntax Description	<i>url</i>	The path and filename for the gtt load file.
	execute	Keyword to execute the load immediately.
	instance	(Optional) Specifies the URL location from which, upon ITP reload, the GTT database for a specified instance will be loaded.
	<i>instance-number</i>	Instance Number. The valid range is 0 through 7. The default instance is instance 0.

Defaults No default behavior or values

Command Modes Global configuration

Command History	Release	Modification
	12.2(4)MB	This command was introduced.

Examples The following example specifies that when the ITP is reloaded, the GTT database will be loaded from a file named gttdata.txt in flash:

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

The following example specifies that when the ITP is reloaded, the GTT database for instance 4 will be loaded from a file named gttdata.txt in flash:

```
cs7 instance 4 gtt load flash:gttdata.txt
```

Related Commands	Command	Description
	cs7 multi-instance	Enables multiple instances of a variant and network indicator combination.
	cs7 save gtt-table	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 the 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) Configure a Global Title Mated Application (MAP) entry for an instance.
<i>instance-number</i>	Instance Number. The valid range is 0 through 7. The default instance is instance 0.
<i>ppc</i>	Primary SS7 point code, in the form zone.region.sp.
<i>pssn</i>	Primary subsystem number.
<i>flags</i>	One of the following flags: adj - Mark ppc/pssn as adjacent. csplist name - Specifies a concerned point code list name. rrc - Reroute if congested.
<i>mult</i>	The entry in the MAP table may be modified to work in 1 of 3 multiplicities or modes: solitary - Use a single PC, no alternate if PC and/or SSN is not available. share - Load share 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.
<i>bpc</i>	Backup point code, in the form zone.region.sp.
<i>bssn</i>	Backup subsystem number. Valid range is 2 through 255.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)MB	This command was introduced.

Usage Guidelines

A GTT 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 following rules apply:

- 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 per point-code is allowed.
- The PC can not be equal to the node's self 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 route the message.

There are three modes described in ITU-T Q.714 section 5.1: solitary, dominant, and shared.

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 will notify the SCCP routing control; and the traffic towards the **solitary** nodes will be 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 towards 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 will notify 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 will backup each other. If one of the nodes becomes inaccessible, the SCCP management will notify the routing control and the traffic will be 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 8 different destinations each having a relative cost, rather than supporting only a primary and secondary node.

Examples

The following example configures 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 configures a primary mated application with PC=1.20.1 and SSN=250. The backup is PC=2.20.2 SSN=20 operating in the dominant mode:

```
cs7 gtt map 1.20.1 250 dom 2.20.2 250
```

The following example configures a primary mated application with PC=1.30.1 and SSN=250. The backup is PC=2.30.2 SSN=250 operating in the 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 multi-instance	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	Override the current state of the point code and set it to available.
	instance	(Optional) Change the state of a point code in the map table for an instance
	<i>instance-number</i>	Instance Number. The valid range is 0 through 7. The default instance is instance 0.
	prohibited	Override the current state of the point code and set it to prohibited.
	<i>point-code</i>	Remote SP point code.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)MB	This command was introduced.

Usage Guidelines Use this command when it becomes necessary (e.g. for maintenance purposes) to prevent GTT translated messages from being sent to a point code in the map table.

Examples The following example sets 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 sets 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 multi-instance	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-ss** | **accept-ss**}
point-code *ssn*

Syntax Description	instance	(Optional) Change the state of a subsystem in the map table for an instance.
	<i>instance-number</i>	Instance Number. The valid range is 0 through 7. The default instance is instance 0.
	accept-ss	Process subsystem test messages received for the affected point code and subsystem.
	available	Override the current state of the subsystem and set it to available.
	ignore-ss	Ignore subsystem test messages received for the affected point code and subsystem.
	prohibited	Override the current state of the subsystem and set it to prohibited.
	<i>point-code</i>	Remote SP point code.
	<i>ssn</i>	Subsystem number.

Defaults No default behavior or values

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)MB	This command was introduced.

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.

The **cs7 gtt map ss** command allows the user to manually change the subsystem state to prohibited. Since the user is 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 sent the message to.

Examples The following example sets 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 sets 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 multi-instance	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) Replace the entire contents of the GTT database for an instance
<i>instance-number</i>	Instance Number. The valid range is 0 through 7. The default instance is instance 0.
<i>url</i>	URL of replacement contents.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)MB	This command was introduced.

Usage Guidelines

GTT database replacement is a non-disruptive as of IOS release 12.2(4)MB13.

Examples

The following example specifies that the GTT database will be replaced by a file named gttdata.txt in flash:

```
cs7 gtt replace-db flash:gttdata.txt
```

The following example specifies that the GTT database will be replaced by a file named gttdata.txt in flash for instance 1:

```
cs7 instance 1 gtt replace-db flash:gttdata.txt
```

Related Commands

Command	Description
cs7 multi-instance	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 the 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) Create and configure a GTT selector for an instance.
<i>instance-number</i>	Instance Number. The valid range is 0 through 7. The default instance is instance 0.
<i>selector</i>	Name of the GTT selector. Selector 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 are in the range 0 through 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).
<i>instance-number</i>	Specifies the instance. The valid range is 0 through 7. The default instance is instance 0.
np	Specifies a numbering plan value.
<i>np</i>	(Optional) Numbering plan value. Valid range is 0 through 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 through 127.

Defaults The default instance is 0.

Command Modes Global configuration

Command History	Release	Modification
	12.2(4)MB	This command was introduced.

Usage Guidelines

The following are the rules for creating 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.
- For ITU nodes, GTI must be 2 or 4.
- For ANSI nodes, GTI must be 2.

The command in the form **cs7 gtt selector** *selector* with no other arguments exits global configuration and enters CS7 GTT selector mode. CS7 GTT selector mode is used to modify attributes of a selector or to update Global Title Addresses (GTAs) of a selector.

Examples

The following example configures for instance 2 a selector named itp_gtt, with tt=0, gti=4, np=1, nai=3:

```
cs7 instance 2 gtt selector itp_gtt 0 4 1 3
```

The following example configures a selector named itp_gtt, with tt=0, gti=4, np=1, nai=3:

```
cs7 gtt selector itp_gtt 0 4 1 3
```

Related Commands

Command	Description
cs7 multi-instance	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 gws action-set name {allow | block [sccp-error error]}[logging {silent | file [verbose] |  
console [verbose] | file [verbose] console [verbose]}]
```

```
no cs7 gws action-set name
```

Syntax Description

<i>name</i>	Name of the action set. Valid action-set names may contain no more than 12 characters.
allow	Allow the message for further processing.
block	Block (reject) the message.
logging	(Optional) Enable logging.
silent	Specifies that messages are screened without any logging.
file	Specifies that the log is copied to a file.
verbose	(Optional) Specifies that the packet up to 40 bytes will be printed to the file or displayed on the console along with other parameters.
console	Specifies that the log is displayed on the console.
sccp-error	Option to return an UDTs with the configured error if SCCP packet is rejected and return-on-error option is set in the received UDT. This option is used only for incoming packets.

Defaults

The default logging type is **silent**.

Command Modes

Global configuration

Command History

Release	Modification
12.2(25)SW4	This command was introduced.
12.2(18)IXC	The keyword sccp-error was added.

Usage Guidelines

An action set cannot be deleted if it is referenced by other entries.

Action sets are independent of CS7 variants.

The user can configure block results with sccp-error in MLR rules and address table entries

Examples

The following example defines action sets allowed-ver and blocked-ver:

```
cs7 gws action-set allowed-ver allow
cs7 gws action-set blocked-ver block
```

Related Commands

Command	Description
show cs7 gws action-set	Displays ITP gateway screening action-set information.

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 through 7. The default instance is instance 0.
name	Specifies an AS name
<i>as-name</i>	AS name.
default	Default screening for all ASes.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(25)SW4	This command was introduced.

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 configures 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 configures 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 SI00
  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 through 7. The default instance is instance 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(25)SW4	This command was introduced.

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 configures a GWS linkset screening table for the linkset to_morehead1 and specifies 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 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 through 7. The default instance is instance 0.																																
<i>name</i>	Specifies the name of the table.																																
type	Specifies a gateway screening table type.																																
<i>table-type</i>	Gateway screening table type. Valid table 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(25)SW4	This command was introduced.

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 configures 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 host name 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 host-name** form of this command. To remove only one point-code from a name mapping use the **no cs7 host host-name point-code** form of the command.

cs7 host *host-name* [**additional**] {*point-code* [*point-code* ...]} | {*point-code:instance-number* [*point-code:instance-number*...]}

no cs7 host *host-name* [**additional**] {*point-code* [*point-code* ...]} | {*point-code:instance-number* [*point-code:instance-number*...]}

Syntax Description	additional	Append an additional point code.
	<i>host-name</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 No default behavior or value.

Command Modes Global configuration

Command History	Release	Modification
	12.2(4)MB	This command was introduced.

Usage Guidelines It is possible to map multiple point codes to the same name. This allows a node that is part of multiple instances to have the same name in all instances. However, a point-code can **not** be mapped to multiple names.

The optional keyword **additional** must be used when assigning an additional point-code to a name. If you do not specify **additional**, an existing mapping of point-codes to the name will be replaced with the new configuration.

When the multiple instance feature is enable, include the instance number.

To display name to point-code mapping use the **show hosts** command.

A name instead of a point-code is displayed if the point code represents a node (no clusters, networks or summarized routes) and a name for the point-code is configured. 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 point-code	Assigns a local point code to an instance.
cs7 variant	Specifies the variant for an instance.
cs7 multi-instance	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 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.

Command Modes

User EXEC

Command History

Release	Modification
12.2(1)MB	This command was introduced.

Usage Guidelines

Inhibit is used when it becomes necessary (e.g. for maintenance purposes) to make or keep a signaling link unavailable to user-generated signaling traffic. Inhibiting a link is allowed only if the inhibiting action does not cause any previously accessible destinations to become inaccessible at either end of the signaling link.

Inhibit is a signaling traffic management action, and does not cause any link status changes at Level 2. In particular, a signaling link that was active and in service prior to being inhibited will remain so, and will thus be able to transmit and receive maintenance and test messages.

Examples

The following command inhibits link 0 on the linkset named tony:

```
cs7 inhibit tony 0
```

Related Commands

Command	Description
shutdown (cs7 link)	Disables a link or linkset.
cs7 uninhibit	Puts the link or linkset back in service.

cs7 instance pc-conversion

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. 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>	The instance number of the real point code. The valid range is 0 through 7.
<i>pc</i>	The CS7 point code. This point code must already exist in the instance's routing table.
alias-pc	Map the alias point code to the real point code.
<i>alias-instance</i>	The instance number of the alias point code. The valid range is 0 through 7.
<i>alias-pc</i>	The alias point code. The alias point code must not already exist in the alias instance's routing table.

Defaults

No default behavior or value.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)MB	This command was introduced.

Usage Guidelines

Prior to IOS Release 12.2(20)SW, point code conversion was limited to instances with the same variant. That limitation now pertains to default conversions only. However, conversion from ANSI or ITU to China or TTC variant is not supported. In the case of conversion between ITU and either ANSI or China variants, the MSU size will change as a result of the different point code size. If the conversion causes the MSU size to grow beyond the maximum MSU size of 273 bytes, the MSU is discarded.

Examples

The following example maps 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 measurement.
show cs7 pc-conversion	Displays the status of the Instance Translation.

cs7 instance pc-conversion default

Default conversion sends any MSUs with unknown point codes in one instance to another instance. Also, any PCs in the MSU that require conversion but do not have an alias point code assigned will be 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 cs7 instance *dest-instance* **pc-conversion default** *orig-instance*

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.

Defaults

No default behavior or value.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)MB12	This command was introduced.

Usage Guidelines

This command accomplishes the following:

- Enters a summary route for mask length 0 in *orig-instance* going over the virtual linkset to *dest-instance*. This means that any MSUs routed in *orig-instance* that do not match other routes, will be sent to *dest-instance*.
- Enters a default conversion for point codes between instance *orig-instance* and *dest-instance*. This means that 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.

Default conversion can only be configured in one direction between two instances. If you configure default conversion from instance 0 to instance 1, then you must configure specific conversion from instance 1 to instance 0 for destinations in instance 0 to allow traffic to be routed from instance 1 to instance 0.

We recommend that you also configure **cs7 instance summary-routing-exception** if you configure default routing from one instance to another. 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, then when 4.4.4 becomes unavailable, the ITP will send MSUs destined for 4.4.4 to instance 1. If summary-routing-exception is configured for instance 0, then when 4.4.4 becomes unavailable the ITP will send TFPs for 4.4.4 and will **not** try to route MSUs destined for 4.4.4 to instance 1.

Examples

The following example sends MSUs with unknown point code in instance 0 to instance 1:

```
cs7 instance 1 pc-conversion default 0
```

Related Commands

Command	Description
cs7 instance pc-conversion	Enables the conversion of packets between instances.
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 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 through 7. The default instance is instance 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 ITPs primary or secondary point code. The default is the primary point code.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(1)MB	This command was introduced.
12.2(4)MB	The optional parameter <i>local-pc</i> was added to enable multiple linksets to an adjacent node.

Usage Guidelines

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



Note

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

The optional multiple linkset feature enables you can configure two linksets to an adjacent node, each having 16 links, for a total of 32 links. To do so, use the optional parameter *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. (The default is primary *pc*.)

When a linkset is created using the **cs7 linkset** command, a route table entry is automatically created for destination *adj-pc*. Since this is the direct linkset to this destination it is assigned the highest priority, 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 will be 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 CS7 linkset submode you have access to commands that allow you to further configure linksets.

Examples

The following example configures 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 configures 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 configures 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 multi-instance	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 [*name*] *local-port-number* **offload** *slotbay*

no cs7 local-peer [*name*] *local-port-number* **offload** *slotbay*

Syntax Description

<i>name</i>	Name of group peer on which the local peer physically resides. The <i>name</i> parameter is only valid (and required) if the ITP Group feature has been configured.
<i>local-port-number</i>	Port number of the local peer. Range is 1024 to 49151.
offload	Configure local peer for M2PA/SCTP offload onto a linecard.
<i>slot</i>	Linecard slot number. Valid range is 0 to 12.
<i>bay</i>	Linecard bay number where Port Adapter is located. Valid range is 0 to 1.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(1)MB	This command was introduced.
12.2(4)MB	The offload keyword was added to enable M2PA/SCTP offload.
12.2(4)MB8	The range of ports that can be configured was changed from 4096-32767 to 1024-49151.
12.2(23)SW	The <i>name</i> parameter was added.

Usage Guidelines

The **cs7 local-peer** command offloads the M2PA/SCTP protocol onto the specified linecard, enabling management of peer links on the linecard and freeing the RP CPU for MTP3 management and routing.

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 CS7 local peer submode, you can configure a local IP address for an instance.

Examples

The following example specifies M2PA/SCTP offload onto the linecard in slot 2 bay 0:

```
cs7 local-peer 7000 offload 2 0
```

Related Commands	Command	Description
	local-ip (CS7 local peer)	Assigns an IP address to the local peer.
	show cs7 m2pa	Displays ITP M2PA statistics.

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 through 7. The default instance is instance 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(25)SW5	This command was introduced.

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 this 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 multi-instance	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** *size*}

no cs7 log *type*

Syntax Description	
<i>type</i>	Specifies the type of log. Valid <i>types</i> are: gtt Log related to Global Title Translation errors. gws-nontest Enhanced Gateway Screening logging in non-test 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 log is stored. Valid <i>destinations</i> 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 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 will overwrite existing entries, starting from the first entry.

Defaults Logging is off by default. The default log size is 0.

Command Modes Global configuration

Command History	Release	Modification
	12.2(25)SW	This command was introduced.
	12.2(25)SW4	The gws-test and gws-nontest types were added.

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 archives a GWS log every hour and sends 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 specifies the maximum number of entries in the circular log. When the current number of entries exceeds 10000, the first entry will be overwritten.

```
cs7 log gws-test size 10000
```

The following example specifies the checkpoint DIRECTORY. The filename will be created automatically and will contain 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 by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(25)SW	This command was introduced.

Examples

The following example archives the GTT log every hour and sends 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 ASs or ASPs) use the **no** form of this command.

cs7 m3ua *local-port* **offload** *slotbay*

no cs7 m3ua *local-port*

Syntax Description

<i>local-port</i>	The 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.)
offload	Configures local peer for M2PA/SCTP offload onto a linecard.
<i>slot</i>	Linecard slot number.
<i>bay</i>	Linecard bay number.

Defaults

There is no default configuration. The M3UA well-known port is 2905.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)MB5	This command was introduced.
12.2(4)MB13	The offload keyword was added, enabling the xUA SCTP Offload feature.

Usage Guidelines

M3UA uses SCTP to communicate with Application Server Processes (ASPs). The **offload** keyword enables the ITP to offload M3UA SCTP message processing to the linecard.

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.

Issuing the **cs7 m3ua** command enables the 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 specifies a local port number of 2000 for M3UA:

```
cs7 m3ua 2000 offload 2 0
local-ip 10.10.10.7
```

The following example offloads two different instances of M3UA processing to the linecard in slot 5 bay 0 and another instance to the linecard 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 4 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 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 No default behavior or values.

Command Modes Global configuration

Command History	Release	Modification
	12.2(4)MB9	This command was introduced.

Usage Guidelines By default, the ITP sends response-mode UPU 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 sends UPU in the following additional cases. (Note that the destination M3UA AS PC must still be available.)

- If the M3UA AS goes inactive or down, send UPU 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 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 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 goes inactive, send UPU to the OPC in the AS routing key.

Extended UPU is disallowed if any M3UA AS has a CIC range configured. Conversely, CIC range configuration is disallowed 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 enables M3UA extended-upu operation:

```
cs7 m3ua extended-upu
```

cs7 mated-sg

The Signaling Gateway Mate Protocol (SGMP) is used to establish an association to the mated SG with an equivalent SG configuration. 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* [**passive**]

no cs7 mated-sg *name remote-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 parameter is used for validation. The SCTP connection requests from the mate must come in with this remote port number.
passive		(Optional) Keyword to specify no attempt to initiate the connection to the mate.

Defaults No default behavior or values.

Command Modes Global configuration

Command History	Release	Modification
	12.2(4)MB5	This command was introduced.

Usage Guidelines

The **cs7 mated-sg** command allows you to define the mate SG and enables the 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. The user 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 specifies a mated SG named mate2 at remote port 5000 with the passive keyword:

```
cs7 mated-sg mate2 5000 passive
```

Related Commands	Command	Description
	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 of 1000 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>	The maximum number of dynamic routes that can be created. The range is 100 to 2000.
--------------------	---------------	---

Defaults	1000 dynamic routes.
----------	----------------------

Command Modes	Global configuration
---------------	----------------------

Command History	Release	Modification
	12.2(4)MB	This command was introduced.

Usage Guidelines	This command is not instance related and cannot be specified with the instance keyword.
------------------	--

Examples	The following example specifies 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 that is to be used 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 the 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 through 7. The default instance is instance 0.
	<i>table-name</i>	Identifies a name to be associated with this multi-layer result table. The name must be unique among all multi-layer routing tables. The name is specified as a character string with a maximum of 12 characters.

Defaults No default behavior or value.

Command Modes Global configuration

Command History	Release	Modification
	12.2(21)SW	This command was introduced.

Usage Guidelines The MLR address table is a table of 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 in only 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 defines 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 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.

cs7 mlr modify-profile *profile-name operation-name*

no cs7 mlr modify-profile *profile-name operation-name*

Syntax Description

modify-profile	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>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.
<i>protocol</i>	Specifies an application layer protocol filter.

Usage Guidelines

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-sm-sc) and the calling party address (CgPA) for SRI-SM messages.

The modify profile is assigned to a rule using the modify-profile rule parameter. If a 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.

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 which are MLR routed.

cs7 mlr options

Use the **cs7 mlr options** command to specify MLR global options. To remove the definition, use the **no** form of the 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 through 7. The default instance is instance 0.

Defaults	None
-----------------	------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.2(18)IXB	This command was introduced.

Usage Guidelines	The cs7 mlr options command enables CS7 MLR options configuration mode.
-------------------------	--

Examples	The following example enables global options and specifies that when a packet is MLR routed, the Message Transfer Part (MTP) destination point code (dpc) is inserted 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 MLR routed.
	preserve-opc (cs7 mlr ruleset)	Preserves the original originating point code (OPC) when a MLR is selected in this instance
	modify-profile (cs7 mlr ruleset rule)	Specifies SCCP and MAP addresses to modify in messages which are MLR routed.

cs7 mlr result

To name a multi-layer 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 multi-layer information.

cs7 [*instance instance-number*] **mlr result** *name* [**protocol** {**gsm-map** | **ansi41**}] [**mode** {**wrr** | **dest-sme-binding**}]

no cs7 [*instance instance-number*] **mlr 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 instance is not specified, then the table may only be used in the default network instance 0.
<i>instance-number</i>	Instance number. The valid range is 0 through 7. The default instance is instance 0.
<i>name</i>	Identifies a name to be associated with this multi-layer result table. The name must be unique among all multi-layer routing tables. The name is specified as a character string with a maximum of 12 characters.
protocol	This optional protocol is only used by SMS-MO Proxy (DSMR). It is included in MLR result group configuration for the case in which a DSMR result references an MLR result group. It is not used by MLR.
gsm-map	Specifies that the gsm-map protocol is used by SMS-MO Proxy (DSMR) for the results in this result-group.
ansi41	Indicates that the ansi-41/is-41 protocol is used by SMS-MO Proxy (DSMR) for the results in this result-group.
mode	Specifies the algorithm used by this result group. If mode is not configured, then the mode defaults to WRR.
wrr	Specifies that the weighted round robin algorithm is used by this result group to select a result.
dest-sme-binding	Specifies that a dynamic B-address binding algorithm is used by this result group to select a result. The dest-sme-binding mode uses a weighted distribution algorithm which binds a set of B-addresses to the same available result.

Defaults No default behavior or value.

Command Modes Global configuration

Command History

Release	Modification
12.2(4)MB	This command was introduced.
12.2(21)SW	The instance keyword was added.
12.2(25)SW4	The keywords protocol , gsm-map , ansi41 , mode , wrr , and dest-sme-binding were added.

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 as always available. Ensure that the proper GT configuration is in place and available for GT routing.

MLR 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. Congested resources are used only if no available, non-congested destinations exist.

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 ITP enhancement was introduced with Cisco IOS Release 12.2(25)SW4 to simplify configuration since 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 results within an SMS result group, so DMSR can reference only MLR groups that contain no asname results.

Examples

The following example identifies a multi-layer 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 identifies a multi-layer 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.
	result (cs7 mlr ruleset rule)	Specifies the processing that will be performed on a packet matching the specified trigger and rule.
	show cs7 mlr dest-sme-binding	Display the result that will be selected from an SMS result group for the specified dest-sme address.
	show cs7 mlr result	Specifies a multi-layer result group.

cs7 mlr ruleset

To specify sets of rules that will be used to process traffic matching triggers defined in a multi-layer routing table, use the **cs7 mlr ruleset** command in global configuration mode. To remove the **cs7 mlr ruleset** command, provided that no defined MLR triggers are using the ruleset, use the **no** form of the command.

cs7 [*instance instance-number*] **mlr ruleset** *name* [**protocol** {**gsm-map** | **ansi-41**}]

no cs7[*instance instance-number*] **mlr ruleset** *name* [**protocol** {**gsm-map** | **ansi-41**}]

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 in the default network instance 0.
<i>instance-number</i>	An integer value in the range 0 to 7.
<i>name</i>	Identifies a name to be associated with this multi-layer rule set table. The name must be unique among all multi-layer rule set 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) Specifies that GSM MAP ¹ is the application layer protocol to be used within the ruleset. For networks with mixed application layer protocols, the protocol should not be specified to allow all protocol operations on the rule statement.
ansi-41	Specifies that ANSI-41 ² or IS-41 is the application layer protocol to be used within the ruleset. For networks with mixed application layer protocols, the protocol should not be specified to allow all protocol operations on the rule statement.
<ol style="list-style-type: none"> 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	No default behavior or value.
-----------------	-------------------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.2(4)MB	This command was introduced.
	12.2(21)SW	The instance , gsm-map , and ansi-41 keywords were added.

Usage Guidelines

This command enables the CS7 MLR ruleset configuration submode. The **cs7 mlr ruleset** command allows for the configuration of rules that customize the routing of messages. The **cs7 mlr ruleset** command when entered, will put the user in **cfg-cs7-mlr-set** configuration submode. In this submode, the **rule** command is valid.

Examples

The following example creates 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
cdpa	Creates a combination trigger based on the combination of the calling party and the called party
cgpa	Specifies a combination trigger based on the combination of the calling party and the called party
rule (cs7 mlr ruleset)	Specifies the rules for a routing trigger within a multi-layer 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 Multi-layer 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 Multi-layer 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 multi-layer SMS routing table and enable CS7 MLR table mode, use the **cs7 mlr table** command in global configuration mode. To disable the Multi-layer SMS routing feature use the **no** form of the command.

cs7 [*instance instance-number*] **mlr table** *name*

no cs7 [*instance instance-number*] **mlr table** *name*

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 instance is not specified, then the table may only be used in the default network instance 0.
	<i>instance-number</i>	Instance number. An integer value in the range 0 to 7.
	<i>name</i>	Identifies a name to be associated with this multi-layer routing table. The name must be unique among all multi-layer routing tables. The name is specified as a character string with a maximum of 12 characters.

Defaults No default behavior or value.

Command Modes Global configuration

Command History	Release	Modification
	12.2(4)MB	This command was introduced.
	12.2(21)SW	The instance keyword was added.

Usage Guidelines This command enables the CS7 MLR table mode.
In the current release, only a single multi-layer routing table is allowed.

Examples The following example specifies 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 specifies a CS7 MLR routing table named SMS-TABLE and specified that the MLR table is valid in instance 2:

```
cs7 instance 2 mlr table SMS-TABLE
```

Related Commands	Command	Description
	cs7 multi-instance	Enables multiple instances of a variant and network indicator combination.
	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
	trigger default	Specifies a routing trigger that matches all packets in 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, in seconds, 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(25)SW7</td><td>This command was introduced.</td></tr></table>		Release	Modification	12.2(25)SW7	This command was introduced.						
Release	Modification											
12.2(25)SW7	This command was introduced.											
Usage Guidelines	Use the cs7 msu-rates notification-interval command to prevent excessive generation of notifications.											
Examples	<p>The following example specifies a notification interval of 60 seconds:</p> <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, in seconds, over which MSU rates are calculated</td></tr><tr><td>cs7 msu-rates threshold-default</td><td>Configures the global MSU rate thresholds 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, in seconds, over which MSU rates are calculated	cs7 msu-rates threshold-default	Configures the global MSU rate thresholds 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, in seconds, over which MSU rates are calculated											
cs7 msu-rates threshold-default	Configures the global MSU rate thresholds 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>	The sample interval in seconds. 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(25)SW7	This command was introduced.

Examples	The following example specifies 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, in seconds, used to prevent excessive generation of notifications.
	cs7 msu-rates threshold-default	Configures the global MSU rate thresholds 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>	The 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. There is no default value.
	<i>warning</i>	The threshold value, in MSUs per second, that indicates a rate of traffic which may impact device. This value must be greater than the <i>acceptable</i> threshold value and less than the <i>overloaded</i> threshold value. Range is from 100 to 999999. There is no default value.
	<i>overloaded</i>	The threshold value, in MSUs per second, that indicates a rate of traffic which impacts operation of device. This value must be greater than both the acceptable and warning threshold values. Range is from 100 to 999999. There is no default value.

Defaults	No default behavior or values. This command established the default MSU rate threshold values for all processors on the platform.
-----------------	---

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.2(25)SW7	This command was introduced.

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 to set values for acceptable, warning, and threshold for specific processors in the ITP platform.
-------------------------	---

Examples

The examples in this section are intended only to describe the command parameters. They do not represent recommended configurations.

In the example below, for a Cisco 7513 ITP platform, the first line defines global thresholds for acceptable, warning, and overloaded MSU rates for all VIPs in the ITP platform. Lines 4 and 5 set the threshold values for the RSPs.

```
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, 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-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) Specifies the slot that contains the processor. This keyword only applies to those ITP platforms that support multiple processors.
	<i>bay</i>	(Optional) Specifies the bay that contains the processor. This keyword only applies to those ITP platforms that support multiple processors.
	<i>acceptable</i>	The threshold value in MSUs per second, which 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. There is no default value.
	<i>warning</i>	The threshold value in MSUs per second, which defines, for the specified processor, a rate of traffic that may impact the device. This value must be greater than the <i>acceptable</i> threshold value and less than the <i>overloaded</i> threshold value. Range is from 100 to 999999. There is no default value.
	<i>overloaded</i>	The threshold value in MSUs per second, which defines, for the specified processor, a rate of traffic that impacts operation of device. This value must be greater than both the acceptable and warning threshold values. Range is from 100 to 999999. There is no default value.

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(25)SW7	This command was introduced.

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 in 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 example below, for a Cisco 7513 ITP platform, the first line defines global thresholds for acceptable, warning, and overloaded MSU rates for all VIPs in the ITP platform. Lines 4 and 5 set the threshold values for the RSPs.

```
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, 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 thresholds ranges and defaults for all processors in the ITP platform.
show cs7 msu-rates	Displays information about configured SS7 MSU rates.

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) Specify the maximum number of events to store in memory for an instance.
	instance-number	Instance number. The valid range is 0 through 7. The default instance is instance 0.
	number	Maximum number of events to log in history. Valid numbers are in the range 0 to 1024. Setting the number to 0 removes all saved events and discontinues the logging of events. The default number of events logged if this command is not configured, or if the no form of the command is issued, is 512.

Defaults	512 events are logged by default.
-----------------	-----------------------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.2(1)MB	This command was introduced.

Usage Guidelines	Since 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 sets the maximum number event to be logged at 1024:
-----------------	---

```
cs7 mtp3 event history 1024
```

The following example sets the maximum number event to be logged to 1024 for instance 2:

```
cs7 instance 2 mtp3 event history 1024
```

Related Commands

Command	Description
cs7 multi-instance	Enables multiple instances of a variant and network indicator combination.
show cs7 mtp3 event-history	Displays logged events exchanged among the 3 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}
```

```
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}
```



Note

Ranges are ANSI, ITU, or TTC defined. MTP3 timer values for China Variant are the same as ITU. When used, the MTP3 timer values for TTC match ITU.

Syntax Description

instance	(Optional) Configure 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 through 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 through 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 through 90000 milliseconds. (ANSI, ITU) Default is 60000 milliseconds.
t01 msec	(ANSI, ITU, TTC) Delay to avoid message mis-sequencing. (ANSI, ITU, TTC) Range of <i>msec</i> is 500 through 1200 milliseconds. (ANSI, ITU, TTC) Default is 800 milliseconds.
t02 msec	(ANSI, ITU, TTC) Wait for changeover acknowledgment. (ANSI, ITU, TTC) Range of <i>msec</i> is 700 through 2000 milliseconds. (ANSI, ITU, TTC) Default is 1400 milliseconds.
t03 msec	(ANSI, ITU, TTC) Delay to avoid mis-sequencing in changeback. (ANSI, ITU, TTC) Range of <i>msec</i> is 500 through 1200 milliseconds. (ANSI, ITU, TTC) Default is 800 milliseconds.
t04 msec	(ANSI, ITU, TTC) Wait for changeback acknowledgment (first attempt). (ANSI, ITU, TTC) Range of <i>msec</i> is 500 through 1200 milliseconds. (ANSI, ITU, TTC) Default is 800 milliseconds.
t05 msec	(ANSI, ITU) Wait for changeback acknowledgment (second attempt). (ANSI, ITU) Range of <i>msec</i> is 500 through 1200 milliseconds. (ANSI, ITU) Default is 800 milliseconds.

t06 msec	(ANSI, ITU, TTC) Delay to avoid message mis-sequencing on controlled rerouting. (ANSI, ITU, TTC) Range of <i>msec</i> is 500 through 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 through 1200 milliseconds. (ANSI, ITU, TTC) Default is 1000 milliseconds.
t10 msec	(ANSI, ITU, TTC) Waiting to repeat signaling-route-set-test message. (ANSI, ITU, TTC) Range of <i>msec</i> is 30,000 through 60,000 milliseconds. (ANSI, ITU, TTC) Default is 45,000 milliseconds.
t11 msec	(ANSI, ITU) Transfer-restricted timer. (ANSI, ITU) Range of <i>msec</i> is 30,000 through 90,000 milliseconds. (ANSI, ITU) Default is 60,000 milliseconds.
t12 msec	(ANSI, ITU) Wait for uninhibited acknowledgment. (ANSI, ITU) Range of <i>msec</i> is 800 through 1500 milliseconds. (ANSI, ITU) Default is 1150 milliseconds.
t13 msec	(ANSI, ITU) Wait for force uninhibited. (ANSI, ITU) Range of <i>msec</i> is 800 through 1500 milliseconds. (ANSI, ITU) Default is 1150 milliseconds.
t14 msec	(ANSI, ITU) Wait for inhibition acknowledgment. (ANSI, ITU) Range of <i>msec</i> is 2000 through 3000 milliseconds. (ANSI, ITU) Default is 2500 milliseconds.
t15 msec	(ANSI) Waiting to repeat signaling route set congestion test. (ITU, TTC) Waiting to start route set congestion test. (ANSI, ITU, TTC) Range of <i>msec</i> is 2000 through 3000 milliseconds. (ANSI, ITU, TTC) Default is 2500 milliseconds.
t16 msec	(ANSI, ITU, TTC) Waiting for route set congestion update. (ANSI, ITU, TTC) Range of <i>msec</i> is 1400 through 2000 milliseconds. (ANSI, ITU, TTC) Default is 1700 milliseconds.
t17 msec	(ANSI, ITU) Delay to avoid oscillation of alignment failure and link restart. (ANSI, ITU) Range of <i>msec</i> is 800 through 1500 milliseconds. (ANSI, ITU) Default is 1150 milliseconds.
t18 msec	(ANSI) Repeat TFR once by response method. (ANSI) Range of <i>msec</i> is 2000 through 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 through 31000 milliseconds. (ITU) Default is 30000 milliseconds.
t19 msec	(ANSI) Failed link craft referral timer. (ANSI) Range of <i>msec</i> is 480000 through 600000 milliseconds. (ANSI) Default is 540000. (ITU) Supervision timer during MTP restart. (ITU) Range of <i>msec</i> is 67000 through 69000 milliseconds. (ITU) Default is 68000 milliseconds.

t20 <i>msec</i>	<p>(ANSI) Waiting to repeat local inhibit test. (ANSI) Range of <i>msec</i> is 90000 through 120000 milliseconds. (ANSI) Default is 105000 milliseconds.</p> <p>(ITU) MTP restart timer at the signaling point whose MTP restarts. (ITU) Range of <i>msec</i> is 1000 through 61000 milliseconds. (ITU) Default is 60000 milliseconds.</p>
t21 <i>msec</i>	<p>(ANSI) Waiting to repeat remote inhibit test. (ANSI) Range of <i>msec</i> is 90000 through 120000 milliseconds. (ANSI) Default is 105000 milliseconds.</p> <p>(ITU) MTP restart timer at signaling point adjacent to one whose MTP restarts. (ITU) Range of <i>msec</i> is 63000 through 65000 milliseconds. (ITU) Default is 64000 milliseconds.</p>
t22 <i>msec</i>	<p>(ANSI) Timer at restarting SP waiting for signaling links to become available all traffic restart allowed messages. (ANSI) Range of <i>msec</i> is 36000 through 60000 milliseconds. (ANSI) Default is 30000 milliseconds.</p> <p>(ITU) Local inhibit test timer. (ITU) Range of <i>msec</i> is 180000 through 360000 milliseconds. (ITU) Default is 300000 milliseconds.</p>
t23 <i>msec</i>	<p>(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 through 60000 milliseconds. (ANSI) Default is 30000 milliseconds.</p> <p>(ITU) Remote inhibit test timer. (ITU) Range of <i>msec</i> is 180000 through 360000 milliseconds. (ITU) Default is 300000 milliseconds.</p>
t24 <i>msec</i>	<p>(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 through 60000 milliseconds. (ANSI) Default is 30000 milliseconds.</p> <p>(ITU) Stabilizing timer after removal of local processor outage, used in LPO latching to RPO. (ITU) The only valid value for <i>msec</i> is 500 milliseconds. (ITU) Default is 500 milliseconds.</p>
t25 <i>msec</i>	<p>(ANSI) Timer at SP adjacent to restarting SP, waiting for traffic restart allowed message. (ANSI) Range of <i>msec</i> is 30000 through 35000 milliseconds. (ANSI) Default is 30000 milliseconds.</p>
t26 <i>msec</i>	<p>(ANSI) Timer at restarting SP waiting to repeat traffic restart waiting message. (ANSI) Range of <i>msec</i> is 12000 through 15000 milliseconds. (ANSI) Default is 12000 milliseconds.</p>
t28 <i>msec</i>	<p>(ANSI) Timer at SP adjacent to restarting SP waiting for traffic restart waiting message. (ANSI) Range of <i>msec</i> is 3000 through 35000 milliseconds. (ANSI) Default is 30000 milliseconds.</p>

t29 msec	(ANSI) Timer started when TRA sent in response to unexpected TRA or TRW. (ANSI) Range of <i>msec</i> is 60000 through 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 through 35000 milliseconds. (ANSI) Default is 33000 milliseconds.
t32 msec	(ANSI) Link oscillation timer - Procedure A. Range of <i>msec</i> is 60000 through 120000 milliseconds. Default is 60000 milliseconds.
tc msec	(TTC) Congestion test timer. Range of <i>msec</i> is 3000 through 30000. Default is 3000 milliseconds.

Defaults

Defaults listed in Syntax Description.

Command Modes

Global configuration

Command History

Release	Modification
12.2(1)MB	This command was introduced.
12.3(20)SW	The MTP3 timer values were updated to include TTC. The TTC tc timer was added.

Usage Guidelines

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.

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 will override any global values.

All 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.

Examples

The following example sets the ITP MTP3 T6 timer to 1000 milliseconds:

```
cs7 mtp3 timer t6 1000
```

The following example sets the ITP MTP3 T6 timer to 1000 milliseconds:

```
cs7 mtp3 timer t6 1000
```

Related Commands	Command	Description
	cs7 multi-instance	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 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 [*instance instance-number*] **mtp3 tuning buffered-packet-threshold** *bufferedPaks*
rx-congestion-threshold *queuedPaks*

no cs7 [*instance instance-number*]**mtp3 tuning**

Syntax Description	
instance	(Optional) Specifies MTP3 performance tuning parameters
<i>instance-number</i>	Instance number. An integer value in the range 0 to 7.
buffered-packet-threshold <i>bufferedPaks</i>	Threshold number of packets buffered at MTP3 for changeover/changeback after which packets begin to be dropped. The range is 1000 to 80000 buffered packets per ITP. The default is 20000 buffered packets per ITP.
rx-congestion-threshold <i>queuedPaks</i>	Threshold 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 is 75%.

Defaults

The default **buffered-packet-threshold** is 20000 buffered packets per ITP.

The default **rx-congestion-threshold** is 75% of the maximum number packets on the MTP3 link's interface input queue.

Command Modes

Global configuration

Command History

Release	Modification
12.2(1)MB	This command was introduced.

Examples

The following example sets the buffered-packet-threshold to 1000 and the rx-congestion-threshold to 50%:

```
cs7 mtp3 tuning buffered-packets-threshold 1000 rx-congestion-threshold 50
```

The following example sets the buffered-packet-threshold to 1000 and the rx-congestion-threshold to 50% for instance 2:

```
cs7 instance 2mtp3 tuning buffered-packets-threshold 1000 rx-congestion-threshold 50
```

Related Commands	Command	Description
	cs7 mtp3 timer	Configures MTP3 timers.
	cs7 multi-instance	Enables multiple instances of a variant and network indicator combination.
	show cs7 mtp3 timers	Displays the values of the MTP3 timers.

cs7 multi-instance

To enable multiple instances of a variant and network indicator combination, use the **cs7 multi-instance** command in global configuration mode.

cs7 multi-instance

no cs7 multi-instance

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or value.

Command Modes Global configuration

Command History	Release	Modification
	12.2(4)MB	This command was introduced.

Usage Guidelines Use the **cs7 multi-instance** command to enable multiple variants and network indicator combinations to run concurrently on one ITP. Up to 8 instances can be configured.

The multiple instance feature cannot be enabled until the default instance is first assigned a variant.

Examples The following example enables the configuration of multiple variant and network indicator “instances.”

```
cs7 multi-instance
```

Related Commands	Command	Description
	cs7	Customizes the setting of the national use field within SCCP management calling and called party addresses
	local-sccp-addr-ind	
	cs7 variant	Indicates which of the SS7 variations the ITP is running on an instance.

cs7 national-options

To configure the 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) Configure the 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 congestions 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

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(1)MB	This command was introduced.
12.2(20)SW	The route-set-congestion-test keyword was added.
12.2(25)SW1	The combined-linkset-loadsharing keyword was added.

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

Previous to 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 exist 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, the **combined-linkset-loadsharing** keyword was added.

There is currently no command to display national options, other than **show running config**.

Refer to Q.704 section 11.2.4 for multiple-congestion, and Q.704 section 13.4 for TFR.

Examples

The following example configures the national options to send transfer restricted messages:

```
cs7 national-options TFR
```

Related Commands

Command	Description
cs7 multi-instance	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) Configure 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	For international use only

Defaults

National network.

Command Modes

Global configuration

Command History

Release	Modification
12.2(1)MB	This command was introduced.

Examples

The following example configures the network indicator to international:

```
cs7 network-indicator international
```

The following example configures the network indicator to international on instance 3:

```
cs7 instance 3 network-indicator international
```

Related Commands

Command	Description
cs7 multi-instance	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 instance network-name** command in global configuration mode. To remove, use the **no** form of the 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.
	<i>instance-number</i>	Instance number. An integer value in the range 0 to 7.
	<i>network-name</i>	Specifies the network name. Valid names are text string up to 19 characters long.

Defaults	No default behavior or value.
-----------------	-------------------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.2(4)MB	This command was introduced.

Usage Guidelines	The network-name is used to allow network management to group signalling points by network. Network-name is not required for instance zero. For all other instances it must be specified after the variant and prior to all other commands for the instance,
-------------------------	--

Examples	The following example specifies the network name hr :
-----------------	--

```
cs7 network-name hr
```

The following example specifies the network name **hr** for instance 2:

```
cs7 instance 2 network-name hr
```

Related Commands	Command	Description
	cs7 multi-instance	Enables multiple instances of a variant and network indicator combination.

cs7 nso

To enable ITP Non-Stop 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

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(23)SW	This command was introduced.

Usage Guidelines

Issuing the **no cs7 nso** command results in a reload of the standby RSP, if it is present. This occurs because the ITP protocols on the standby RSP must revert back to the state required for RPR+ operation, which is the default for ITP if the redundancy mode is SSO and NSO is not configured.

Examples

The following example enables NSO:

```
cs7 nso
```

Related Commands

Command	Description
show cs7 nso	Displays NSO information.

cs7 paklog

To configure the ITP Packet Logging facility parameter, 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>	Keyword and value indicating the Destination IP port of the remote syslog receiving port. Valid range is port number 1 to 65535.
severity <i>severity</i>	(Optional) Keyword and value specifying 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) Keyword and value specifying 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) Keyword and value specifying 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) Keyword and value specifying 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(4)MB	This command was introduced.

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 Systems, Inc. does not provide monitoring tools specifically for receiving and decoding messages sent by the facility. The user must obtain a suitable tool for receiving syslog messages.

Under normal conditions, use of the ITP Packet Logging facility will 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 specifies a CS7 access list to permit packets that are 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 10.4.0.90 dest-port 5514 src-port 10000
!  
access-list 2700 instance 0 permit all
```

Related Commands

Command	Description
access-list	Defines a Cisco ITP access list.
debug cs7 mtp3 paklog	Sends selected message signaling units (MSU) to an appropriate monitoring tool.

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) Assign 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>	The local point code for this router. The ANSI point code range is 0.0.0 through 255.255.255. The ITU point code range is 0.0.0 through 7.255.7

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)MB	This command was introduced.

Usage Guidelines

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

You must remove all M3UA, SUA, and linkset configuration before you can remove the local point code.

Examples

The following example sets the local point to 10.44.254:

```
cs7 point-code 10.44.254
```

The following example sets the local point code for instance 1 to 10.44.254:

```
cs7 instance 1 point-code 10.44.254
```

Related Commands

Command	Description
cs7 multi-instance	Enables multiple instances of a variant and network indicator combination.
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** | **dot**}

no cs7 [**instance** *instance-number*] **point-code delimiter** {**dash** | **default** | **dot**}

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 of dot (.).
dot	Specifies a dot (.) as the point code delimiter.

Defaults

The default point code delimiter is a dot (.).

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)MB	This command was introduced.

Usage Guidelines

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.

Examples

The following example sets the local point code delimiter to dash:

```
cs7 point-code delimiter dash
```

The following example sets the local point code delimiter to dash for instance 2:

```
cs7 instance 2 point-code delimiter dash
```

Related Commands

Command	Description
cs7 multi-instance	Enables multiple instances of a variant and network indicator combination.
cs7 point-code	Assigns a local point code to the router.

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 instance point-code format** command in global configuration mode. To return to either standard's default, use the **default** keyword.

cs7 [*instance instance-number*] **point-code format** { *1-24* [*1-23* [*1-22*]] } [**description** *string*] [**default**]

no cs7 [*instance instance-number*] **point-code format** { *1-24* [*1-23* [*1-22*]] } [**description** *string*] **default**

Syntax Description

instance	(Optional) Modify the point code format on an instance.
<i>instance-number</i>	Instance number. An integer value in the range 0 to 7.
<i>1-24</i>	Number of bits used for the first component of the point code.
<i>1-23</i>	Number of bits used for the second component of the point code.
<i>1-22</i>	Number of bits used for the third component of the point code.
description	Text description follows.
<i>string</i>	Text description.
default	Use the default format.

Defaults

The ANSI standard for point code representation is 24 bits partitioned into 3 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 3 segments for network, cluster, and member, with a default representation of 3.8.3.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)MB	This command was introduced.

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 prior removal of links and linksets.

Examples

The following example sets the format for the ITU standard to 2.6.6:

```
cs7 point-code format 2 6 6 description network cluster member
```

The following example sets 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 multi-instance	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 the command.

cs7 profile *name*

no cs7 profile *name*

Syntax Description

<i>name</i>	Profile name.
-------------	---------------

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)MB	This command was introduced.

Usage Guidelines

The **cs7 profile** command enable CS7 profile configuration mode.
This command is not instance related and cannot be specified with the **instance** keyword.

Examples

The following example defines a profile named **m2parfc**, specifies that the profile supports M2PA RFC, configures **peer-timer** settings and **hold-transport** settings in the profile, then applies the **m2parfc** profile to all the links in 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 defines a profile named **timers**, configures the profile to support MTP2, configures the **t1** and **t2** settings in the **timers** profile, then applies the **timers** profile to all the links in linkset named **to_nyc**:

```
cs7 profile timers
  mtp2
  timer t1 15000
  timer t2 9000

cs7 linkset to_nyc
  profile timers
```

The following example defines a profile named SAAL, configures the profile to support HSL, specifies the packet bundling interval and SSCF NNI timers, then applies the profile to all the links in linkset 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, 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

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(25)ISW	This command was introduced.

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 is intended to help avoid the possibility of inadvertently shutting down the wrong linkset/link.

Examples

The following example configures the CLI prompt to display the current linkset:

```
cs7 prompt enhanced
```

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 CS7 Quality of Service class, use the **cs7 qos class** command in global configuration mode. To remove the configuration, use the **no** form of the command.

cs7 [**instance** *instance-number*] **qos class** *class*

no cs7 [**instance** *instance-number*] **qos class** *class*

Syntax Description

instance	(Optional) Specifies QoS class for an instance.
<i>instance-number</i>	Instance number. An integer value in the range 0 to 7.
<i>class</i>	Quality of Service class identification number. Valid numbers are in the range 0 through 7.
<i>instance-number</i>	Specifies the instance. The valid range is 0 through 7. The default instance is instance 0.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)MB	This command was introduced.

Usage Guidelines

A QoS class must be defined prior to being used by peer links and by the QoS packet classification methods input linkset, service indicator and access list.

Examples

The following example configures a QoS class of 4:

```
cs7 qos class 4
```

The following example configures a QoS class of 4 to instance 2:

```
cs7 instance 2 qos class 4
```

Related Commands

Command	Description
cs7 multi-instance	Enables multiple instances of a variant and network indicator combination.
gta qos-class	Sets the QoS class for the Global Title Address.
match access-group	Enables access list packet classification.
match any (CS7 Linkset)	Enables input linkset packet classification.
match si (cs7 linkset)	Enables service indicator packet classification.

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 the command.

cs7 [*instance instance-number*] **remote-congestion-msgs**

no cs7 [*instance instance-number*] **remote-congestion-msgs**

Syntax Description	instance	(Optional) Specifies QoS class for an instance.
	<i>instance-number</i>	Instance number. An integer value in the range 0 to 7.
Defaults	Allow remote congestion status messages.	
Command Modes	Global configuration	
Command History	Release	Modification
	12.2(4)MB	This command was introduced.
Examples	The following example enables remote congestion status console messages: cs7 remote-congestion-msgs	
	The following example enables remote congestion status console messages on instance 1: cs7 instance 1remote-congestion-msgs	
Related Commands	Command	Description
	cs7 multi-instance	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 instance route-mgmt-sls** command in global configuration mode. To return to the default selection method (round-robin), use the **no** form of the command.

cs7 [*instance instance-number*] **route-mgmt-sls** {**destination** | **round-robin** | **value num**}

no cs7 [*instance instance-number*] **route-mgmt-sls**

Syntax Description	
instance	(Optional) Change the way route management signaling link selector (SLS) values are assigned on an instance
<i>instance-number</i>	Instance number. An integer value in the range 0 to 7.
destination	Assigns route management SLS values based upon the concerned point code destination.
<i>instance-number</i>	Specifies the instance. The valid range is 0 through 7. The default instance is instance 0.
round-robin	Assigns route management SLS values using round-robin method. Route management messages will be distributed evenly over the available links in the linkset.
value	Assigns route management SLS values to a static value. Route management messages will be distributed over the same link within a linkset.
<i>num</i>	Value in the range 0 - 255 (ANSI) and 1-15 (ITU).

Defaults The default is to assign route management SLS values using round-robin.

Command Modes Global configuration

Command History	Release	Modification
	12.2(4)MB	This command was introduced.

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 link set. When the SLS is assigned using the round-robin method, the route management messages are distributed over the available links in the linkset. This results in the most efficient use of the available links.

There are some SS7 nodes that 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 num** form of the command. Configuring the **cs7 instance route-mgmt-sls** command to use a specific value will cause route management messages to use the same link within a linkset. This is not necessarily the most efficient use of the available links in a linkset but it will ensure 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 upon the concerned point code destination address in the route management message. This 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 will cause route management messages to have an SLS value of zero:

```
cs7 route-mgmt-sls value 0
```

The following command will cause route management messages that originate at instance 2 to have an SLS value of zero:

```
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 sls-shift	Shifts which SLS bits are used for link and linkset selection.

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 by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)MB	This command was introduced.

Usage Guidelines

A route table for an instance is identified by its route table name. A route table name system is configured by default and used to keep routes to all adjacent signaling points. Additional routes can be added to the system 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 creates a route table:

```
cs7 route-table system
```

The following example creates a route table for instance 1:

```
cs7 instance 1 route-table system
```

Related Commands

Command	Description
cs7 multi-instance	Enables multiple instances of a variant and network indicator combination.
update route (route-table)	Updates a route.

cs7 save address-table

To save an address table to a specified location and file, use the **cs7 save address-table** command in privileged EXEC mode. To remove the line from the configuration, use the **no** form of this command.

cs7 save address-table {mlr | sms} *tablename* *URL*

no cs7 save address-table {mlr | sms} *tablename* *URL*

Syntax Description	mlr	Specifies the type of table is mlr .
	sms	Specifies the type of table is sms .
	<i>tablename</i>	Identifies the existing address table that is to be replaced.
	<i>URL</i>	The user-assigned local or remote location representing the file name and path from which the file will be replaced.

Defaults	No default behavior or values
----------	-------------------------------

Command Modes	Privileged EXEC
---------------	-----------------

Command History	Release	Modification
	12.2(25)SW	This command was introduced.

Usage Guidelines	SMS 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 off address entries that can be stored there. In this case, the file storage option is recommended.
------------------	--

Examples	The following command saves an SMS address table named addrtbl1 to disk0:smsaddrtbl: <pre>cs7 save address-table sms addrtbl1 disk0:smsaddrtbl</pre>
----------	---

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 file is to be saved.
------------	-------------------------------------

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)MB	This command was introduced.

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 saves a the GTT table to a file named gttdata.txt in flash:

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

Related Commands

Command	Description
cs7 gtt load	Specifies the location from which the GTT database will be reloaded when the ITP router is rebooted.

cs7 save log

To save a log to a file, use the **cs7 save log** command in privileged EXEC mode.

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 Non-Test 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
	nvrn: URL to saved table
	rcp: URL to saved table
	system: URL to saved table
	tftp: URL to saved table

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(25)SW	This command was introduced.

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 detaches the current log from the active log process and saves 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 detaches the current log from the active log process and saves 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 route-table

To save the CS7 route table to a file, use the **cs7 save route-table** privileged EXEC command.

cs7 save route-table *rtname url*

Syntax Description	<i>rtname</i>	Route table name.
	<i>url</i>	Location where file is to be saved.

Defaults	No default behavior or values
----------	-------------------------------

Command Modes	Privileged EXEC
---------------	-----------------

Command History	Release	Modification
	12.2(4)MB	This command was introduced.

Usage Guidelines	Use this privileged EXEC command to 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**

All **update route** or **remove route** route-table 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 therefore are included in the saved file.

It is recommended 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).

Examples	The following example saves a route table named testtable to flash:
----------	---

```
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 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 *tablename*

no cs7 sccp gti-conversion *tablename*

Syntax Description	<i>tablename</i>	SCCP GTI Conversion table name. The table name may be 1-12 characters in length.
---------------------------	------------------	--

Defaults	No default behavior or values
-----------------	-------------------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.2(20)SW	This command was introduced.

Usage Guidelines	Issuing the cs7 sccp gti-conversion command enables the CS7 SCCP GTI Conversion submode.
-------------------------	---

Examples	The following command specifies an SCCP GTI conversion table named gti-conv1:
-----------------	---

```
cs7 sccp gti-conversion conv1
```

Related Commands	Command	Description
	show cs7 sccp gti-conversion	Displays CS7 GTI conversion table.
	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 the input instance for which conversion is desired.
<i>instance</i>	Input instance number.
out-instance	Specifies the output-instance for which conversion is desired.
<i>instance</i>	Output instance number.

Defaults

If no conversion methods are assigned, the GTT in the MSUs will not be changed.

Command Modes

Global configuration

Command History

Release	Modification
12.2(20)SW	This command was introduced.

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. 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.

You can also set message-handling options and specify a national indicator.

Examples

The following example configures an SCCP instance conversion entry and sets gti-conversion, subsystem mapping, and address-conversion tables from instance0 to instance1:

```
cs7 sccp instance-conversion in-instance 0 out-instance 1
  set gti-conversion gtitable
  set ssn-conversion ssntable
  set address-conversion gtaddressstable
```

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.
	set message-handling	Specifies the message handling options.
	set national-indicator	Specifies the SCCP national indicator to be used.
	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 *tablename* **in-ssn** *in-ssn* **out-ssn** *out-ssn*

no cs7 sccp ssn-conversion *tablename* **in-ssn** *in-ssn* **out-ssn** *out-ssn*

Syntax Description	<i>tablename</i>	Subsystem table name. The table name may be 1-12 characters in length.
	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 No default behavior or values

Command Modes Global configuration

Command History	Release	Modification
	12.2(20)SW	This command was introduced.

Usage Guidelines 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, not the subsystem from the SSN conversion table.

Examples The following command creates 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.
	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 secondary-pc

To configure the secondary point code, use the **cs7 secondary-pc** command in global configuration mode. To remove the configuration, use the **no** form of the command.

cs7 [**instance** *instance-number*]**secondary-pc** *zone.region.sp*

no [**instance** *instance-number*]**secondary-pc** *zone.region.sp*

Syntax Description

instance	(Optional) Configure the secondary point code on an instance.
<i>instance-number</i>	Instance number. An integer value in the range 0 to 7.
<i>zone.region.sp</i>	Secondary point code.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)MB	This command was introduced.

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 primary point code configured using the **cs7 point-code** command and one with the point code configured using this command.

Examples

The following example configures 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 multi-instance	Enables multiple instances of a variant and network indicator combination.
cs7 linkset	Specifies a linkset.

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.

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(4)MB5	This command was introduced.

Examples	The following example specifies that 64 events will be saved in history: <code>cs7 sg-event-history 64</code>
----------	--

cs7 sgmp

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). 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 there is no mated SG configured) use the **no** form of this command.

cs7 sgmp *local_port*

no cs7 sgmp *local_port*

Syntax Description

<i>local_port</i>	The local port number. 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.
-------------------	--

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)MB5	This command was introduced.

Usage Guidelines

Issuing the **cs7 sgmp** command enables CS7 SGMP submode.

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.

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 upon expiration of an AS recovery timer.

This command is not instance related and cannot be specified with the **instance** keyword.

Examples

The following example specifies the local port number 5000 for SGMP:

```
cs7 sgmp 5000
```

Related Commands

Command	Description
cs7 mated-sg	Specifies the mated SG.
local-ip (CS7 SGMP)	Configures up to 4 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 **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	Shift SLS bits on an instance.
<i>instance-number</i>	Instance number. An integer value in the range 0 to 7.
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 0, the equivalent of the **no sls-shift** command.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)MB5	This command was introduced.

Usage Guidelines

This command is for MTP3 users (SUA/M3UA) that do not have an inbound linkset. The command works the same 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.

It is necessary to be able 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 won't balance evenly.

Examples

The following example specifies that the most significant bit (3) is to be used for linkset selection:

```
cs7 sls-shift 3
```

Related Commands

Command	Description
cs7 linkset	Specifies a linkset.
cs7 multi-instance	Enables multiple instances of a variant and network indicator combination.
cs7 route-mgmt-sls	Changes the way route management SLS values are assigned.

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	<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
	12.2(21)SW	This command was introduced.

Examples	In the following example, the maximum number of destination state changes allowed per window is set to 500: <pre>cs7 snmp dest-max-window 500</pre>
-----------------	--

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(21)SW	This command was introduced.

Examples	In the following example, the maximum number of route management state changes allowed per window is set 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 *local-port* **offload** *slotbay*

no **cs7 sua** *local-port*

Syntax Description

<i>local-port</i>	This value 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 is 14001.
offload	Enables the ITP to perform SUA SCTP message processing on the linecard.
<i>slot</i>	Linecard slot number.
<i>bay</i>	Linecard bay number.

Defaults

No default behavior or values. The SUA well-known port number is 14001.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)MB5	This command was introduced.
12.2(4)MB13	The offload keyword was added, enabling the xUA SCTP Offload feature.

Usage Guidelines

SUA uses SCTP to communicate with Application Server Processes (ASPs).

If offloaded, a specific SUA instance can run on only one linecard. But different offloaded SUA instances can run on the same linecard or on different linecards.

If you offload M3UA or SUA to a linecard, that linecard cannot also be used for M2PA offload.

The **local-ip** *ip-address* must be an IP address that was already configured on the linecard to which you are offloading this SUA instance. When offload is enabled, only a single IP route per destination is allowed.

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 specifies a local port number of 5000 for SUA:

```
cs7 sua 5000 offload 5 0
  local-ip 10.10.10.4
```

The following example offloads two different instances of SUA SCTP message processing to the linecard in slot 5 bay 0 and another instance to the linecard 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 4 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(23)SW1	This command was introduced.

Usage Guidelines

The **cs7 sua-allow-xudt-request** command allows the SUA ASP additional control in determining whether an SCCP UDT or XUDT will be generated upon receiving a CLDT message. When the command is specified, SUA will request the SCCP layer to generate an XUDT message if the ASP has provided either the IMPORTANCE or HOP_COUNTER parameters within the CLDT message.

Examples

The following command enables the SUA to request the SCCP layer to generate an XUDT message if the ASP has provided either the IMPORTANCE or HOP_COUNTER parameters 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 MSU) 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-summary*] **summary-routing-exception**

no cs7 [*instance instance-summary*] **summary-routing-exception**

Syntax Description

instance	(Optional) Turn 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(4)MB	This command was introduced.

Usage Guidelines

The **cs7 summary-routing-exception** command lets you control whether or not to use the summary route or ANSI cluster route when the full point code route is not available. If the command is enabled, then the summary route will **not** be used. The MSU will be dropped and a TFP sent.

This feature is useful for customers who want most destinations that are covered by a summary route to be routed on a certain group of linksets, but want one or a few destinations within that summary to be routed on different linksets completely independently of the summary routes.

The feature only affects routing of MSU for a destination for which there is a configured set of full point code routes.

Examples

The following example turns off the use of summary routes:

```
cs7 summary-routing-exception
```

Related Commands

Command	Description
cs7 multi-instance	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 re-establish the default timer value of 60 minutes, use the **no** form of this command.

cs7 tcap tid-timer *minutes*

no cs7 cs7 tcap tid-timer

Syntax Description	<i>minutes</i>	Time in minutes before TCAP may cancel transaction. Valid range is 0 to 1440 minutes. Default is 60 minutes.
--------------------	----------------	--

Defaults	The minimum expiration time for TCAP transactions is 60 minutes.
----------	--

Command Modes	Global configuration
---------------	----------------------

Command History	Release	Modification
	12.2(25)SW	This command was introduced.

Examples	<p>The following example sets the minimum expiration time for TCAP transactions to 120 minutes:</p> <pre>cs7 tcap tid-timer 120</pre>
----------	---

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 the command.

cs7 tcap variant {ansi | itu}

no cs7 tcap variant {ansi | itu}

Syntax Description

ansi	Specifies that the 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	Specifies that the 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, then ITU/ETSI is the default variant used.

Command Modes

Global configuration

Command History

Release	Modification
12.2(25)SW3	This command was introduced.

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 enables the ANSI T1.114 variant:

```
cs7 tcap variant ansi
```

Related Commands

Command	Description
cs7 tcap tid-timer	Specifies 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 1 TFC for every dropped message signal unit (MSU), use the **cs7 tfc-pacing-ratio** command in global configuration mode. To re-establish the ITP default TFC pacing ratio (8 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) Adjust 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	The default TFC pacing ratio is 8 MSUs dropped for outbound link congestion for each TFC generated.	
Command Modes	Global configuration	
Command History	Release	Modification
	12.2(4)MB	This command was introduced.
Usage Guidelines	The cs7 tfc-pacing-ratio command controls the ratio of TFC MSUs that are sent in response to received MSUs that are dropped due to outbound link congestion. The ANSI standard is a 1 to 1 ratio. The ITP default configuration sets a ratio of 1 TFC per 8 dropped MSUs to prevent congestion in the reverse direction.	
Examples	The following example sends TFCs in a 1 to 1 ratios (TFC MSUs sent in response to MSUs dropped due to outbound congestion):	
	<pre>cs7 tfc-pacing-ratio 1</pre>	
Related Commands	Command	Description
	cs7 multi-instance	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.

Command Modes

User EXEC

Command History

Release	Modification
12.2(1)MB	This command was introduced.

Usage Guidelines

The **cs7 inhibit** command prevents you from taking the last link in a linkset out of service. If you were to use the **shutdown** command to shutdown 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 commands allows you to add linksets or to reduce your bandwidth in the linksets by taking links out of service.

Examples

The following command uninhibits link 0 on the linkset named tony:

```
cs7 uninhibit tony 0
```

Related Commands

Command	Description
shutdown (cs7 link)	Disables a link or linkset.
cs7 inhibit	Inhibits a link.

cs7 upgrade analysis

To display the available links configured in each linecard slot, a list of the destinations that might become inaccessible when the linecard is upgraded, and step-by-step description of the software upgrade process, use the cs7 upgrade analysis command in Privileged EXEC mode.

cs7 upgrade analysis

Syntax Description This command has no arguments or keywords.

Defaults No default behaviors 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 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
       2         7         7

Total number of affected destinations = 0
```

UPGRADE ANALYSIS FOR SLOT 2

1. Linkset Name : miramalo
 Available links (SLC) : 1, 2

Expected utilization of links on other slots (percent):

Link	Rcvd	Sent
0	7	7
3	7	7

Total number of affected destinations = 0

% Link status is dynamic and the destination status may vary at the actual time of card upgrade

Summary of Software Upgrade Steps:

Step 1: Copy new image onto the disk

```
Enter 'delete slavedisk0:old-image'
Enter 'copy tftp://new-image slavedisk0:new-image'
Enter 'verify /md5 slavedisk0:new-image CCO_posted_hash'
Enter 'configure terminal'
Enter 'boot system disk0:'
Enter 'end'
Enter 'copy running-config startup-config'
Enter 'show boot | inc BOOT '
  Verify that one location is listed and that standby variable matches
  the primary, example:
    BOOT variable = disk0:,12;
    and
    Standby BOOT variable = disk0:,12;
```

Step 2: Reset the Standby Supervisor

```
Enter 'hw-module module <standby sup> reset'
  Once slot <standby slot> is up, verify the Supervisors are in
  SSO mode to continue with upgrade.
Enter 'show redundancy states'
Enter 'redundancy force-switchover'
Verify the Supervisors are in RPR mode to continue with upgrade
Enter 'show redundancy states'
  Wait for the message 'Standby supervisor is up. Line cards can be upgraded now.'
  on the new active SUP.
```

Step 3: Upgrade the Linecards sequentially

```
Enter 'cs7 upgrade module 1'
  Once slot 1 is up
Enter 'cs7 upgrade module 2'
  Once slot 2 is up
Enter 'cs7 upgrade module 3'
.
.
.
```

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 linecard.

cs7 upgrade module

To upgrade the software on a linecard, use the following command in Privileged EXEC mode:

cs7 upgrade module *slot bay*

Syntax Description	<i>slot</i>	Specifies the slot where the linecard is installed.
	<i>bay</i>	Specifies the bay where the linecard is installed.

Defaults	No default behaviors or values.
----------	---------------------------------

Command Modes	Privileged EXEC
---------------	-----------------

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.

Examples	The following example upgrades the software on the linecard 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 the command.

cs7 util-abate *percent*

no util-abate *percent*

Syntax Description	<i>percent</i>	Integer range utilization threshold in percent. The range is 0 to 40 percent. The default is 0.
---------------------------	----------------	---

Defaults	The default is 0.
-----------------	-------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.2(4)MB4	This command was introduced.

Usage Guidelines	<p>The abate delta is an integer used to reduce the number of cItpSpLinkRcvdUtilChange and cItpSpLinkSentUtilChange notifications generated when a link's utilization fluctuates around the specified threshold. The abate delta is used to lower 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 the rising notifications will be generate at 45 percent and the falling notification will be generated at 35 percent.</p>
-------------------------	---

This command is not instance related and cannot be specified with the **instance** keyword.

Examples	The following example sets the utilization threshold to 30 percent:
-----------------	---

```
cs7 util-abate 30
```

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-receive	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 the command

cs7 util-plan-capacity *bps*

no cs7 util-plan-capacity *bps*

Syntax Description	<i>bps</i>	The default planned capacity in bps. The range is 56000 to 2147483647 bps.
---------------------------	------------	--

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.2(4)MB4	This command was introduced.

Usage Guidelines	The default planned capacity value that is configured will be used as a default for an SCTP-based link in place of the interface speed.
	This command is not instance related and cannot be specified with the instance keyword.

Examples	The following example sets 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-receive	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 the command

cs7 util-sample-interval *seconds*

no cs7 util-sample-interval *seconds*

Syntax Description	<i>seconds</i>	Integer range utilization threshold, in seconds. 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(4)MB4	This command was introduced.

Usage Guidelines	<p>The cs7 util-sample-interval command specifies the duration of the sample interval in seconds. Shorter intervals allow the 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. However, longer interval requires more time to detect link utilization problems.</p>
-------------------------	---

This command is not instance related and cannot be specified with the **instance** keyword.

Examples	The following example sets 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-receive	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 the command.

cs7 util-threshold *percent*

no cs7 util-threshold *percent*

Syntax Description	<i>percent</i>	Utilization threshold in percent. 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(4)MB4	This command was introduced.

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 percent of the utilization. The cItpSpLinkRcvdUtilChange and cItpSpLinkSentUtilChange 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 submode commands.

This command is not instance related and cannot be specified with the **instance** keyword.

Examples	The following example sets 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 the command.

cs7 [**instance** *instance-number*] **variant** {**ansi** | **china** | **itu** | **ttc**}

no cs7 [**instance** *instance-number*] **variant** {**ansi** | **china** | **itu** | **ttc**}

Syntax Description

instance	(Optional) Indicate 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

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(1)MB	This command was introduced.
12.2(4)MB5	The CHINA SS7 protocol variant was added.
12.2(20)SW	The TTC SS7 protocol variant was added.

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=20ms)
 - TF timer for sending FISU (default=20ms)
 - TO timer for sending SIO (default=20ms)
 - TS timer for sending SIOS (default=20ms)

- Outstanding number of MSUs transmittable without confirmation: MTP2/TTC uses TTC default 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 configuration that is ITP-specific. Remove the following ITP configuration statements in the following order:

- links
- linksets
- route-table
- access list
- encapsulation on serial links. (This removes all MTP2 timers.)
- AS route
- AS
- ASPs
- M3UA and SUA
- point code
- variant

Examples

The following example indicates that the ANSI variant of SS7 is being used:

```
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 base M3UA/SUA congestion on AS congestion level, use the **cs7 xua-as-based-congestion** command in global configuration mode. To remove the statement from the configuration, use the **no** form of the command.

cs7 xua-as-based-congestion

no cs7 xua-as-based-congestion

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)MB5	This command was introduced.

Examples

The following example specifies that M3UA/SUA congestion will be based on AS congestion level:

```
cs7 xua-as-based-congestion
```

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	No default behaviors or values.
-----------------	---------------------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.2(4)MB	This command was introduced.

Examples	The following example enables M3UA/SUA SSNM filtering: <code>cs7 xua-ssnm-filtering</code>
-----------------	---

cs7 xua-tfc-allowed

To allow TFCs and SCONs for M3UA/SUA congestion, use the **cs7 xua-tfc-allowed** command in global configuration mode. 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	No default behaviors or values.
-----------------	---------------------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.2(4)MB	This command was introduced.

Examples	The following example allows TFCs and SCONs for M3UA/SUA congestion: cs7 xua-tfc-allowed
-----------------	---

cumulative-sack (CS7 ASP)

To configure the cumulative selective acknowledgment time-out 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 time-out value, in milliseconds. Range is 100 through 500 milliseconds. The default is the value specified under the local port instance.
-------------	---

Defaults

The default acknowledgment time-out value is the value specified under the local port instance.

Command Modes

CS7 asp configuration

Command History

Release	Modification
12.2(4)MB5	This command was introduced.

Examples

The following example sets the cumulative selective acknowledgment time-out value to 300:

```
cs7 asp ASP1 14001 15000 sua
  remote-ip 1.1.1.1
  cumulative-sack 300
```

Related Commands

Command	Description
cs7 asp	Specifies an Application Server Process and enables CS7 ASP submode.
show cs7 asp detail	Displays ASP detail information.

cumulative-sack (CS7 Link)

To configure the cumulative selective acknowledgment time-out 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 time-out value, in milliseconds. Range is 100 through 500 milliseconds. The default is 200 milliseconds.
--------------------	-------------	--

Defaults	200 milliseconds.
----------	-------------------

Command Modes	CS7 link configuration
---------------	------------------------

Command History	Release	Modification
	12.2(1)MB	This command was introduced.

Examples	The following example sets the cumulative selective acknowledgment time-out 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 time-out 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 time-out value, in milliseconds. Range is 100 through 500 milliseconds. The default is 200 milliseconds.
-------------	---

Defaults

200 milliseconds.

Command Modes

CS7 m2pa profile configuration

Command History

Release	Modification
12.2(25)SW3	This command was introduced.

Examples

The following example defines a profile named m2parfc, specifies that the profile supports M2PA RFC, specifies the **cumulative-sack** parameter in the profile, then applies the m2parfc profile to all the links in 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 time-out 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 time-out value, in milliseconds. Range is 100 through 500 milliseconds. The default is 200 milliseconds.
-------------	--

Defaults

200 milliseconds.

Command Modes

CS7 m3ua configuration

Command History

Release	Modification
12.2(4)MB5	This command was introduced.

Examples

The following example sets the cumulative selective acknowledgment time-out 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 time-out 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 time-out value, in milliseconds. Range is 100 through 500 milliseconds. The default is the value specified under the local SGMP port instance.
-------------	--

Defaults

The default selective acknowledgment time-out value is the value specified under the local SGMP port instance.

Command Modes

CS7 mated-sg configuration

Command History

Release	Modification
12.2(4)MB5	This command was introduced.

Examples

The following example sets the cumulative selective acknowledgment time-out value to 300:

```
cs7 mated-sg mate2 5000 passive
 cumulative-sack 300
```

Related Commands

Command	Description
cs7 mated-sg	Configures a connection to a mated SG.
show cs7 mated-sg detail	Displays mated SG detail information.

cumulative-sack (CS7 SGMP)

To configure the cumulative selective acknowledgment time-out 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 time-out value, in milliseconds. Range is 100 through 500 milliseconds. The default is 200 milliseconds.
--------------------	-------------	--

Defaults	200 milliseconds.
----------	-------------------

Command Modes	CS7 sgmp configuration
---------------	------------------------

Command History	Release	Modification
	12.2(4)MB5	This command was introduced.

Examples	The following example sets the cumulative selective acknowledgment time-out value to 300: cs7 sgmp 5000 cumulative-sack 300
----------	---

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 time-out 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 time-out value, in milliseconds. Range is 100 through 500 milliseconds. The default is 200 milliseconds.
-------------	---

Defaults

200 milliseconds.

Command Modes

CS7 sua configuration

Command History

Release	Modification
12.2(4)MB5	This command was introduced.

Examples

The following example sets the cumulative selective acknowledgment time-out 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.

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 asname | gt gta [gt-addr-type] | group groupname } }
```

```
no default { block | continue | ruleset ruleset-name | result { pc pc [ssn ssn] | asname asname | gt gta [gt-addr-type] | group groupname } }
```

Syntax Description

block	This trigger-action specifies that messages matching this trigger should be dropped. The block parameter is ignored if combination triggers are defined within the CS7 MLR trigger mode.
continue	This trigger-action specifies that messages matching this trigger should be routed as received. This is the same behavior as if no primary trigger had been matched. The continue parameter is ignored if combination triggers are defined within the 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) This trigger action 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 simply redirected as indicated in the trigger result. Note: Result groups with dest-sme-binding mode are not valid trigger results.
pc	Route based on point code.
<i>pc</i>	Point code
ssn	(Optional) Route based on PC and subsystem number.
<i>ssn</i>	Subsystem number.
asname	Route based on AS name.
<i>asname</i>	AS name.
gt	Route based on Global Title.
<i>gta</i>	Global title address.
group	Route based on result group.
<i>group-name</i>	Result group name.

Defaults

No default behavior or value.

Command Modes

CS7 mlr trigger configuration

Command History

Release	Modification
12.2(4)MB	This command was introduced.
12.2(21)SW	The continue keyword was added.

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 the secondary trigger.

If you configure a secondary address in the 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 is used to handle routing of packets on 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 will be routed according to standard SCCP or MTP3 procedures.

Examples

In the following example, there are 3 secondary triggers defined 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 multi-layer routing table.
show cs7 mlr table	Displays multi-layer 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	Specifies that the default result will be to screen by action set.
<i>action-set-name</i>	Action set name. Valid names may not exceed 12 alpha numeric characters.
table	Specifies that the default result will be to screen by table.
<i>table-name</i>	Table name. Valid names may not exceed 12 alpha numeric characters.

Defaults

No default behavior or values.

Command Modes

CS7 GWS table configuration

Command History

Release	Modification
12.2(25)SW4	This command was introduced.

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 defines the allowed dpc table and specifies the default result as an action:

```
cs7 instance 6 gws table OPC6 type opc action allowed
default result action ALLOW
```

The following example defines the allowed cgpa-pc-ssn table and specifies 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	Display 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.

cs7 description *line*

no cs7 description *line*

Syntax Description

<i>line</i>	Text string description of the link. Length of <i>line</i> can be from one to 254 alphanumeric characters.
-------------	--

Defaults

No default behavior or values

Command Modes

CS7 link configuration

Command History

Release	Modification
12.2(4)MB	This command was introduced.

Examples

The following example provides 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.
show running config	Displays the contents of the currently running configuration file.

description (cs7 linkset)

To specify a description of the linkset to be used by the administrator or the network management stations, use the **cs7 description** command in cs7 linkset configuration mode. To remove the text string, use the **no** form of this command.

cs7 description *line*

no cs7 description *line*

Syntax Description

<i>line</i>	Text string description of the linkset. Length of <i>line</i> can be from one to 254 alphanumeric characters.
-------------	---

Defaults

No default behavior or values

Command Modes

CS7 linkset configuration

Command History

Release	Modification
12.2(4)MB	This command was introduced.

Examples

The following example provides 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** CS7 MLR ruleset-rule configuration mode command. 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

No default behavior or value

Command Modes

CS7 mlr ruleset-rule configuration

Command History

Release	Modification
12.2(21)SW	This command was introduced.

Examples

The following example specifies an address of the destination port number of 1234:

```
cs7 mlr ruleset ruleset1
 rule 10 sms-mt
  dest-port 1234
```

Related Commands

Command	Description
rule (cs7 mlr ruleset)	Specifies the rules for a routing trigger within a multi-layer 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	
*	Match all address values.
<i>dest-addr</i>	<p>When the rule operation is sms-mo, the <i>dest-addr</i> is an address string of 1 to 20 hexadecimal characters.</p> <p>When the rule operation is sri-sm, <i>dest-addr</i> is an address string of 1 to 16 hexadecimal characters.</p> <p>The string is not input in BCD-String format, but in normal form. The string always carries an implicit '*' at the end of the string, allowing only the prefix of a range of addresses to be specified.</p>
<i>dest-sme-addr-type</i>	<p>(Optional) Parameters that identify attributes of the SME address being used to match a rule. The address is composed of the following keywords:</p> <ul style="list-style-type: none"> • [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 only be matched if 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	(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

No default behavior or values.

Command Modes CS7 MLR ruleset-rule configuration

Command History	Release	Modification
	12.2(4)MB	This command was introduced.
	12.2(21)SW	The imsi and min keywords were added.
	12.2(25)SW	The min-digits and max-digits options were added.
	12.2(25)SW3	The keyword/argument ton <i>ton</i> replaced the keyword/argument noa <i>noa</i> .

Usage Guidelines MLR/SMS rule-matching implementations prior to ITP release 12.2(25)SW3

In ITP releases prior to 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 keyword **ton** replaces the keyword **noa**. 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** 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 28 **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
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 specifies an address of the destination SME:

```
cs7 mlr ruleset ruleset1
rule 10 sms-mo
dest-sme 1234
```

Related Commands

Command	Description
match-unknown-ton-np	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 multi-layer ruleset table and enables CS7 MLR ruleset-rule configuration mode.

dest-sme-table (cs7 mlr ruleset rule)

To configure an MLR table of destination SME addresses, use the **dest-sme-table** cs7 mlr ruleset-rule configuration command. To remove the specification, use the **no** form of this command.

dest-sme-table *tablename* [*dest-sme-addr-type*]

no dest-sme-table

Syntax Description	
<i>tablename</i>	IMSI address table name. Valid range is up to 16 hexadecimal digits.
<i>dest-sme-addr-type</i>	<p>(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:</p> <ul style="list-style-type: none"> • [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.

Defaults	No default behavior or value
-----------------	------------------------------

Command Modes	CS7 MLR ruleset-rule configuration
----------------------	------------------------------------

Command History	Release	Modification
	12.2(21)SW	This command was introduced.
	12.2(25)SW	The noa , np , min , and imsi parameters were added.
	12.2(25)SW3	The keyword/argument ton ton replaced the keyword/argument noa noa .

Usage Guidelines**MLR/SMS rule-matching implementations prior to ITP release 12.2(25)SW3**

In ITP releases prior to 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 keyword **ton** replaces the keyword **noa**. 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 specifies 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	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 multi-layer ruleset table and enables CS7 MLR ruleset-rule configuration mode.

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	
*	Match 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 <i>addr-type</i> is composed of the following keywords: <ul style="list-style-type: none"> [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 No default behavior or values.

Command Modes CS7 MLR ruleset-rule configuration

Command History	Release	Modification
	12.2(4)MB	This command was introduced.
	12.2(21)SW	The exact keyword was added.
	12.2(25)SW3	The keyword/argument ton <i>ton</i> replaced the keyword/argument noa <i>noa</i> .

Usage Guidelines**MLR/SMS rule-matching implementations prior to ITP release 12.2(25)SW3**

In ITP releases prior to 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 keyword **ton** replaces the keyword **noa**. 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 will already contain the destination SMSC address, and need not be specified on the rule.

Examples

The following example specifies the destination service center address:

```
cs7 mlr ruleset ruleset1
rule 20 sms-mo
dest-smsc 1234
```

Related Commands

Command	Description
match-unknown-ton-np	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 multi-layer ruleset table and enables CS7 MLR ruleset-rule configuration mode.

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 of <i>line</i> can 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(4)MB	This command was introduced.

Examples

The following example configures 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.

display-name *line*

no display-name *line*

Syntax Description

<i>line</i>	Text string description for the linkset. Length of <i>line</i> can 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(4)MB	This command was introduced.

Examples

The following example configures 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.

■ display-name (cs7 linkset)



ITP Command Set: E - R

This section documents new or modified commands. All other commands used with this feature are documented in the Cisco IOS Command Reference publications.

- [encapsulation hs-mtp2, page 608](#)
- [encapsulation mtp2, page 609](#)
- [false-congestion, page 610](#)
- [fast-cwnd-rate \(cs7 asp\), page 611](#)
- [fast-cwnd-rate \(cs7 link\), page 612](#)
- [fast-cwnd-rate \(cs7 m2pa profile\), page 613](#)
- [fast-cwnd-rate \(cs7 m3ua\), page 615](#)
- [fast-cwnd-rate \(cs7 mated-sg\), page 616](#)
- [fast-cwnd-rate \(cs7 sgmp\), page 617](#)
- [fast-cwnd-rate \(cs7 sua\), page 618](#)
- [gt \(cs7 mlr result\), page 619](#)
- [gta app-grp, page 621](#)
- [gta asname, page 622](#)
- [gta pcssn, page 624](#)
- [gta -prefix, page 626](#)
- [gta qos-class, page 628](#)
- [gta-start, page 630](#)
- [gtt-accounting, page 631](#)
- [hold-transport \(cs7 link\), page 632](#)
- [hold-transport \(cs7 m2pa profile\), page 633](#)
- [hs-mtp2, page 634](#)
- [hs-mtp2-timer \(cs7 link\)](#)
- [hsl, page 637](#)
- [idle-cwnd-rate \(cs7 asp\), page 638](#)
- [idle-cwnd-rate \(cs7 link\), page 639](#)
- [idle-cwnd-rate \(cs7 mated-sg\), page 640](#)

- [idle-cwnd-rate \(cs7 m2pa profile\), page 641](#)
- [idle-cwnd-rate \(cs7 m3ua\), page 643](#)
- [idle-cwnd-rate \(cs7 sgmp\), page 644](#)
- [idle-cwnd-rate \(cs7 sua\), page 645](#)
- [inbound \(config-gws-as\), page 646](#)
- [inbound \(config-gws-ls\), page 648](#)
- [init-cwnd-size \(cs7 asp\), page 650](#)
- [init-cwnd-size \(cs7 link\), page 651](#)
- [init-cwnd-size \(cs7 m2pa profile\), page 652](#)
- [init-cwnd-size \(cs7 m3ua\), page 654](#)
- [init-cwnd-size \(cs7 mated-sg\), page 655](#)
- [init-cwnd-size \(cs7 sgmp\), page 656](#)
- [init-cwnd-size \(cs7 sua\), page 657](#)
- [init-ip-dscp, page 658](#)
- [init-ip-precedence, page 659](#)
- [init-retransmit \(cs7 link\), page 660](#)
- [init-retransmit \(cs7 m2pa profile\), page 661](#)
- [init-retransmit \(cs7 m3ua\), page 662](#)
- [init-retransmit \(cs7 sgmp\), page 663](#)
- [init-retransmit \(CS7 SUA\), page 664](#)
- [init-timeout \(CS7 Link\), page 665](#)
- [init-timeout \(cs7 m2pa profile\), page 666](#)
- [init-timeout \(CS7 M3UA\), page 667](#)
- [init-timeout \(CS7 SGMP\), page 668](#)
- [init-timeout \(CS7 SUA\), page 669](#)
- [insert-dpc-in-cdpa, page 670](#)
- [ip-dscp \(cs7 m2pa profile\), page 672](#)
- [ip-precedence \(CS7 Link\), page 673](#)
- [ip-precedence \(cs7 m2pa profile\), page 674](#)
- [isup-msg-type, page 675](#)
- [keepalive \(CS7 ASP\), page 677](#)
- [keepalive \(CS7 Link\), page 678](#)
- [keepalive \(cs7 m2pa profile\), page 679](#)
- [keepalive \(CS7 M3UA\), page 680](#)
- [keepalive \(CS7 Mated-SG\), page 681](#)
- [keepalive \(CS7 SGMP\), page 682](#)
- [keepalive \(CS7 SUA\), page 683](#)
- [linestate debounce, page 684](#)

- [link \(CS7 linkset\), page 685](#)
- [link-test, page 688](#)
- [link-timer, page 689](#)
- [load \(cs7 route table\), page 692](#)
- [local-ip \(CS7 local peer\), page 694](#)
- [local-ip \(CS7 M3UA\), page 695](#)
- [local-ip \(CS7 SGMP\), page 696](#)
- [local-ip \(CS7 SUA\), page 697](#)
- [m2pa, page 698](#)
- [match access-group, page 700](#)
- [match any \(CS7 ASP\), page 701](#)
- [match any \(CS7 Linkset\), page 702](#)
- [match si \(cs7 asp\)\), page 703](#)
- [match si \(cs7 linkset\), page 704](#)
- [match-unknown-ton-np \(cs7 mlr ruleset rule\), page 705](#)
- [max-inbound-streams \(CS7 M3UA\), page 708](#)
- [max-inbound-streams \(CS7 SGMP\), page 709](#)
- [max-inbound-streams \(CS7 SUA\), page 710](#)
- [modify-failure \(cs7 mlr option\), page 711](#)
- [modify-profile \(cs7 mlr ruleset rule\), page 712](#)
- [mtp2, page 713](#)
- [mtp2-timer, page 714](#)
- [mtp2-timer ttc enable, page 716](#)
- [multi-message-dialogue \(cs7 mlr ruleset rule\), page 717](#)
- [multiplicity, page 719](#)
- [nai, page 720](#)
- [network-appearance, page 721](#)
- [new-name, page 722](#)
- [np, page 723](#)
- [orig-imsi \(cs7 mlr ruleset rule\), page 724](#)
- [orig-imsi-table \(cs7 mlr ruleset rule\), page 725](#)
- [orig-sme \(cs7 mlr ruleset rule\), page 727](#)
- [orig-sme-table \(cs7 mlr ruleset rule\), page 730](#)
- [orig-smsc \(cs7 mlr ruleset rule\), page 732](#)
- [orig-smsc \(cs7 mlr modify-profile\), page 734](#)
- [outbound \(config-gws-as\), page 736](#)
- [outbound \(config-gws-ls\), page 738](#)
- [path-retransmit \(CS7 ASP\), page 740](#)

- [path-retransmit \(CS7 Link\), page 741](#)
- [path-retransmit \(cs7 m2pa profile\), page 742](#)
- [path-retransmit \(CS7 M3UA\), page 743](#)
- [path-retransmit \(CS7 Mated-SG\), page 744](#)
- [path-retransmit \(CS7 SGMP\), page 745](#)
- [path-retransmit \(CS7 SUA\), page 746](#)
- [pc \(cs7 gtt application group\), page 747](#)
- [pc \(cs7 mlr result\), page 748](#)
- [pc-range, page 750](#)
- [pc-range ssn, page 751](#)
- [peer-timer \(cs7 link\), page 752](#)
- [peer-timer \(cs7 m2pa profile\), page 754](#)
- [pid \(cs7 mlr ruleset rule\), page 756](#)
- [ping cs7, page 757](#)
- [plan-capacity-rcvd, page 759](#)
- [plan-capacity-send, page 760](#)
- [post-gtt-address-conversion, page 761](#)
- [pre-gtt-address-conversion, page 762](#)
- [preserve-opc \(cs7 mlr ruleset\), page 763](#)
- [preserve-opc \(cs7 mlr options\), page 764](#)
- [preventive-txp, page 765](#)
- [qos-access-group, page 766](#)
- [qos-class \(CS7 AS\), page 767](#)
- [qos-class \(CS7 ASP\), page 768](#)
- [qos-class \(CS7 gtt selector\), page 769](#)
- [qos-class \(CS7 link\), page 770](#)
- [qos-class \(cs7 m2pa profile\), page 771](#)
- [qos-class \(CS7 Mated-SG\), page 772](#)
- [qos-ip-dscp, page 773](#)
- [qos-ip-precedence, page 774](#)
- [receive-window \(CS7 local peer\), page 775](#)
- [receive-window \(CS7 M3UA\), page 777](#)
- [receive-window \(CS7 SGMP\), page 778](#)
- [receive-window \(CS7 SUA\), page 779](#)
- [recovery-timeout, page 780](#)
- [remote-ip \(CS7 ASP\), page 781](#)
- [remote-ip \(CS7 Mated-SG\), page 782](#)
- [remove route \(route table\), page 783](#)

- [result \(cs7 mlr ruleset rule\)](#), page 784
- [retransmit-cwnd-rate \(CS7 ASP\)](#), page 786
- [retransmit-cwnd-rate \(CS7 Link\)](#), page 788
- [retransmit-cwnd-rate \(cs7 m2pa profile\)](#), page 790
- [retransmit-cwnd-rate \(CS7 M3UA\)](#), page 792
- [retransmit-cwnd-rate \(CS7 Mated-SG\)](#), page 794
- [retransmit-cwnd-rate \(CS7 SGMP\)](#), page 796
- [retransmit-cwnd-rate \(CS7 SUA\)](#), page 798
- [retransmit-timeout \(CS7 ASP\)](#), page 800
- [retransmit-timeout \(CS7 Link\)](#), page 802
- [retransmit-cwnd-rate \(cs7 m2pa profile\)](#), page 790
- [retransmit-timeout \(CS7 M3UA\)](#), page 806
- [retransmit-timeout \(CS7 Mated-SG\)](#), page 808
- [retransmit-timeout \(CS7 SGMP\)](#), page 810
- [retransmit-timeout \(CS7 SUA\)](#), page 812
- [rotate-sls](#), page 814
- [routing-key \(CS7 AS\)](#), page 815
- [rule \(cs7 mlr ruleset\)](#), page 819

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 the 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(25)SW5	This command was introduced.

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	<p>The following example configures serial interface 4/1/0:0 to use high speed MTP2 encapsulation:</p> <pre>interface serial4/1/0:0 no ip address encapsulation hs-mtp2</pre>
-----------------	---

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 the 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(1)MB	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 configures 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.

false-congestion

To configure the false congestion detection level for linkset, use the **false-detection** 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.
--------------	---

Command Modes

CS7 linkset configuration

Command History

Release	Modification
12.2(4)MB7	This command was introduced.

Examples

The following example sets 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 will be decreased due a fast retransmission. Range is 0 to 100 percent. The default is 50 percent.
---------------------------	----------------	---

Defaults	The default is 50 percent.
-----------------	----------------------------

Command Modes	CS7 asp configuration
----------------------	-----------------------

Command History	Release	Modification
	12.2(19)SW	This command was introduced.

Usage Guidelines	The fast-cwnd-rate parameter allows the administrator to configure a rate at which the SCTP congestion window will be decreased due to a fast retransmission on the SCTP association.
-------------------------	---



Note

It is extremely important to note that the behavior of the SCTP congestion control algorithms are not compliant with RFC 2960 when this parameter is changed to values other than the default. This parameter should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples	The following examples 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 will be decreased due a fast retransmission. Range is 0 to 100 percent. The default is 50 percent.
----------------	---

Defaults

The default is 50 percent.

Command Modes

CS7 link configuration

Command History

Release	Modification
12.2(19)SW	This command was introduced.

Usage Guidelines

The fast-cwnd-rate parameter allows the administrator to configure a rate at which the SCTP congestion window will be decreased due to a fast retransmission on the SCTP association.



Note

It is extremely important to note that the behavior of the SCTP congestion control algorithms are not compliant with RFC 2960 when this parameter is changed to values other than the default. This parameter should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples

The following example 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 will be decreased due 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 will be decreased due a fast retransmission. Range is 0 to 100 percent. The default is 50 percent.
---------------------------	----------------	---

Defaults	The default is 50 percent.
-----------------	----------------------------

Command Modes	CS7 m2pa profile configuration
----------------------	--------------------------------

Command History	Release	Modification
	12.2(19)SW	This command was introduced.

Usage Guidelines	The fast-cwnd-rate parameter allows the administrator to configure a rate at which the SCTP congestion window will be decreased due to a fast retransmission on the SCTP association.
-------------------------	---




Note

It is extremely important to note that the behavior of the SCTP congestion control algorithms are not compliant with RFC 2960 when this parameter is changed to values other than the default. This parameter should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples	The following example defines a profile named m2parfc, specifies that the profile supports M2PA RFC, specifies the fast-cwnd parameter in the profile, then applies the m2parfc profile to all the links in 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 will be decreased due a fast retransmission. Range is 0 to 100 percent. The default is 50 percent.
---------------------------	----------------	---

Defaults	The default is 50 percent.
-----------------	----------------------------

Command Modes	CS7 m3ua configuration
----------------------	------------------------

Command History	Release	Modification
	12.2(19)SW	This command was introduced.

Usage Guidelines	The fast-cwnd-rate parameter allows the administrator to configure a rate at which the SCTP congestion window will be decreased due to a fast retransmission on the SCTP association.
-------------------------	---



Note

It is extremely important to note that the behavior of the SCTP congestion control algorithms are not compliant with RFC 2960 when this parameter is changed to values other than the default. This parameter should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples	The following example 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 will be decreased due 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 will be decreased due a fast retransmission. Range is 0 to 100 percent. The default is 50 percent.
----------------	---

Defaults

The default is 50 percent.

Command Modes

CS7 mated-sg configuration

Command History

Release	Modification
12.2(19)SW	This command was introduced.

Usage Guidelines

The fast-cwnd-rate parameter allows the administrator to configure a rate at which the SCTP congestion window will be decreased due to a fast retransmission on the SCTP association.



Note

It is extremely important to note that the behavior of the SCTP congestion control algorithms are not compliant with RFC 2960 when this parameter is changed to values other than the default. This parameter should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples

The following example 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 will be decreased due a fast retransmission. Range is 0 to 100 percent. The default is 50 percent.

fast-cwnd-rate (cs7 sgmp)

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 sgmp 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 will be decreased due a fast retransmission. Range is 0 to 100 percent. The default is 50 percent.
---------------------------	----------------	---

Defaults	The default is 50 percent.
-----------------	----------------------------

Command Modes	CS7 sgmp configuration
----------------------	------------------------

Command History	Release	Modification
	12.2(19)SW	This command was introduced.

Usage Guidelines	The fast-cwnd-rate parameter allows the administrator to configure a rate at which the SCTP congestion window will be decreased due to a fast retransmission on the SCTP association.
-------------------------	---



Note

It is extremely important to note that the behavior of the SCTP congestion control algorithms are not compliant with RFC 2960 when this parameter is changed to values other than the default. This parameter should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples	The following example set the fast congestion window rate to 60 percent.
-----------------	--

```
cs7 sgmp 5000
 local-ip 4.4.4.4
 fast-cwnd-rate 60
```

Related Commands	Command	Description
	retransmit-cwnd-rate (CS7 SGMP)	Rate at which the size of the SCTP congestion window will be decreased due 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 will be decreased due a fast retransmission. Range is 0 to 100 percent. The default is 50 percent.
----------------	---

Defaults

The default is 50 percent.

Command Modes

CS7 sua configuration

Command History

Release	Modification
12.2(19)SW	This command was introduced.

Usage Guidelines

The fast-cwnd-rate parameter allows the administrator to configure a rate at which the SCTP congestion window will be decreased due to a fast retransmission on the SCTP association.



Note

It is extremely important to note that the behavior of the SCTP congestion control algorithms are not compliant with RFC 2960 when this parameter is changed to values other than the default. This parameter should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples

The following example 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 will be decreased due 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 the 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 through 255.
gti	(Optional) Identifies the global title indicator for the specified address. This value is only specified 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. Only configured when the gti parameter value is 4.
<i>np</i>	Integer in the range 0 through 15.
nai	(Optional) Identifies the nature of the specified address. Configured only when the gti parameter value is 4.
<i>nai</i>	Integer in the range 0 through 127.
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) Specify 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 non-zero weighted resources are unavailable. If multiple zero-weighted resources exist, then messages are equally distributed between them if all non-zero weighted resources fail. If not specified, a default weight of 1 is used.

Defaults Weight value default is 1.

Command Modes CS7 MLR result configuration

Command History

Release	Modification
12.2(25)SW3	This command was introduced.
12.2(25)SW4	The order keyword was added. The <i>weight</i> interval for dest-sme-binding was added.

Usage Guidelines

For the purposes of availability, the **gt** result will always be considered available and uncongested. The network global title translation function then assumes all further load balancing, congestion, and distribution decisions for the message. This is true for wrr mode and dest-sme-binding mode.

Examples

The following example configures an SMS result group named POSTPAY, with tt=0, gti=4, np=1, nai=4 and weight=1:

```
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 the command.

gta *gta app-grp app-grp*

no *gta gta*

Syntax Description

<i>gta</i>	Global Title Address. Valid values are hexadecimal numbers in the range of 1 to 15 characters.
app-grp	Result type specifying that GTA translates to a GTT Application Group.
<i>app-grp</i>	Name of application group.

Defaults

No default behavior or values

Command Modes

CS7 gtt selector configuration

Command History

Release	Modification
12.2(4)MB	This command 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 translates gta 919363 to the application group named group1:

```
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.
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 the command.

```
gta gta asname asname {gt | pcssn} {ntt ntt | ssn ssn}}
```

```
no gta gta
```

Syntax Description

<i>gta</i>	Global Title Address. Valid values are hexadecimal numbers in the range of 1 to 15 characters.
asname	Result type specifying that GTA translates to an M3UA or SUA application server name.
<i>asname</i>	Name of M3UA or SUA Application Server.
gt	Set routing indicator (RI) to Route on Global Title
pcssn	Set 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 through 255,
ssn	Specifies a subsystem number.
<i>ssn</i>	Subsystem number, in the range 2 through 255.

Defaults

No default behavior or values

Command Modes

CS7 gtt selector configuration

Command History

Release	Modification
12.2(4)MB5	This command was introduced.

Usage Guidelines

The **gta asname** command allows you to assign a global title translation to an M3UA or SUA AS, instead of a point code and SSN. By specifying the asname here, backup systems solely reside underneath the specified AS via the **cs7 as** command.

Examples

The following example configures 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
```

Related Commands

Command	Description
cs7 as	Specifies an Application Server and enables the CS7 AS submode.
cs7 gtt selector	Specifies a GTT selector.
cs7 m3ua	Specifies the local port number for SUA 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.

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 the command.

```
gta gta pcssn pc {gt | pcssn} {ntt ntt | ssn ssn}
```

```
no gta gta
```

Syntax Description

<i>gta</i>	Global Title Address. Valid values are hexadecimal numbers in the range of 1 to 15 characters.
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	Set routing indicator (RI) to Route on Global Title
pcssn	Set 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 through 255,
ssn	Specifies a subsystem number.
<i>ssn</i>	Subsystem number, in the range 2 through 255.

Defaults

No default behavior or values

Command Modes

CS7 gtt selector configuration

Command History

Release	Modification
12.2(4)MB	This command was introduced.

Usage Guidelines

You must configure at least one subsystem for the point code, or else the command will fail.

Examples

The following example adds GTA entry 1111 translating to point code 1.2.3 and sets the routing indicator to route on global title.

```
gta 1111 pcssn 1.2.3 gt
```

The following example modifies GTA entry 1111 translating to point code 1.2.3 and sets the routing indicator to route on point code and subsystem number.

```
gta 1111 pcssn 1.2.3 pcssn
```


The following example deletes GTA entry 1111.

```
no gta 1111
```

Related Commands

Command	Description
cs7 gtt concern-pclist	Configures a GTT concerned point code list.
cs7 gtt selector	Specifies a GTT selector.
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
min-digits	Screens against the minimum digits of the global title address.
<i>min-digits</i>	Minimum digits.
max-digits	Screens against the maximum digits of the global title address.
<i>max-digits</i>	Maximum 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 alpha numeric characters.
table	Specifies that the next step is a table.
<i>table-name</i>	Name of the next step table.

Command Default

No default behavior or values.

Command Modes

CS7 GWS table configuration

Command History

Release	Modification
12,2(25)SW4	This command was introduced.

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 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 the command.

```
gta gta qos-class class {[app-grp app-grp] | [pcssn pc {gt ntt ntt} | [pcssn {ntt ntt} | {ssn ssn}]]}
```

```
no gta gta qos-class
```

Syntax Description

<i>gta</i>	Global Title Address. Valid values are hexadecimal numbers in the range of 1 to 15 characters.
<i>qos-class</i>	QoS class. Valid range is 0 through 7.
app-grp	GTA translated to a GTT application group.
<i>app-grp</i>	Name of application group.
pcssn	GTA translated to a point code and optional subsystem number.
<i>pc</i>	Point code in the form zone.region.sp.
gt	Set the routing indicator to “route on global title.”
ntt	Specifies a new translation type.
<i>ntt</i>	New translation type. Valid range is 0 through 255.
pcssn	Set the routing indicator to “route on point code and subsystem number.”
<i>ssn</i>	Specifies a subsystem number.
<i>ssn</i>	Subsystem number. Valid range is 2 through 255.

Defaults

No default behavior or values

Command Modes

CS7 gtt selector configuration

Command History

Release	Modification
12.2(4)MB	This command was introduced.

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 configures a QoS class 3 for the GTA 1324:

```
cs7 gtt selector c7gsp 3 2
gta 1324 qos-class 3 2 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 1-15 hexadecimal digits.
gta-end	Specifies an end GTA.
<i>end-gta</i>	Ending GTA, in the range 1-15 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 alpha numeric characters.
table	Specifies that the next step is a table.
<i>table-name</i>	Name of the next step table.

Command Default

No default behavior or values.

Command Modes

CS7 GWS digit screening table configuration

Command History

Release	Modification
12.2(25)SW4	This command was introduced.

Usage Guidelines

The **gta-start** command is valid in the following table types: cdpa-gta-range, cgpa-gta-range.

Examples

The following example specifies 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

To enable GTT accounting on this linkset, use the **gtt-accounting** command in cs7 linkset configuration mode. To disable GTT accounting on this linkset, use the **no** form of this command.

gtt-accounting

no gtt-accounting

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Defaults	Disabled
-----------------	----------

Command Modes	CS7 linkset configuration
----------------------	---------------------------

Command History	Release	Modification
	12.2(4)MB	This command was introduced.

Examples	<p>The following example enables GTT accounting on the linkset named to_doc:</p> <pre>cs7 linkset to_doc gtt-accounting</pre>
-----------------	---

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 shutdown, 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(25)SW3	This command was introduced.

Examples

The following example specifies 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 shutdown, 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(25)SW3	This command was introduced.

Examples

The following example defines a profile named m2parfc, specifies that the profile supports M2PA RFC, specifies the **hold-transport** parameter in the profile, then applies the m2parfc profile to all the links in 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

Disabled

Command Modes

CS7 profile submode

Command History

Release	Modification
12.2(25)SW5	This command was introduced.

Examples

The following example defines a profile named TIMERS, configures the profile to support high speed MTP2, configures the t1 and t2 settings in the timers profile, then applies the timers profile to all the links in linkset 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 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 the 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 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

Command History	Release	Modification
	12.2(25)SW5	This command was introduced.

Usage Guidelines High speed MTP2 parameters can also be specified in CS7 profile configuration mode.

Examples The following example specifies 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	Define a profile of MTP2 parameters that you can apply to all 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, 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	Disabled
-----------------	----------

Command Modes	CS7 profile configuration
----------------------	---------------------------

Command History	Release	Modification
	12.2(4)MB	This command was introduced.

Examples	The following example defines a profile named SAAL, configures the profile to support HSL, specifies the packet bundling interval and SSCF NNI timers, then applies the profile to all the links in linkset 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 links in a linkset.
	variant jt1	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 will be decreased due to the association being idle. Range is 0 to 100 percent. The default is 50 percent.
----------------	---

Defaults

The default is 50 percent.

Command Modes

CS7 asp configuration

Command History

Release	Modification
12.2(19)SW	This command was introduced.

Usage Guidelines

The idle-cwnd-rate parameter allows the administrator to configure a rate at which the SCTP congestion window will be decreased due to the SCTP association being idle. The SCTP congestion window will not decrease below the initial congestion window size regardless of the rate and the length of idle time.



Note

It is extremely important to note that the behavior of the SCTP congestion control algorithms are not compliant with RFC 2960 when this parameter is changed to values other than the default. This parameter should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples

The following example 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)	Configure 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 will be decreased due to the association being idle. Range is 0 to 100 percent. The default is 50 percent.
----------------	---

Defaults

The default is 50 percent.

Command Modes

CS7 link configuration

Command History

Release	Modification
12.2(19)SW	This command was introduced.

Usage Guidelines

The idle-cwnd-rate parameter allows the administrator to configure a rate at which the SCTP congestion window will be decreased due to the SCTP association being idle. The SCTP congestion window will not decrease below the initial congestion window size regardless of the rate and the length of idle time.



Note

It is extremely important to note that the behavior of the SCTP congestion control algorithms are not compliant with RFC 2960 when this parameter is changed to values other than the default. This parameter should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples

The following example 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)	Configure 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 will be decreased due to the association being idle. Range is 0 to 100 percent. The default is 50 percent.
----------------	---

Defaults

The default is 50 percent.

Command Modes

CS7 mated-sg configuration

Command History

Release	Modification
12.2(19)SW	This command was introduced.

Usage Guidelines

The idle-cwnd-rate parameter allows the administrator to configure a rate at which the SCTP congestion window will be decreased due to the SCTP association being idle. The SCTP congestion window will not decrease below the initial congestion window size regardless of the rate and the length of idle time.



Note

It is extremely important to note that the behavior of the SCTP congestion control algorithms are not compliant with RFC 2960 when this parameter is changed to values other than the default. This parameter should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples

The following example 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)	Configure 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	<i>percent</i>	Rate at which the size of the SCTP congestion window will be decreased due to the association being idle. Range is 0 to 100 percent. The default is 50 percent.
---------------------------	----------------	---

Defaults	The default is 50 percent.
-----------------	----------------------------

Command Modes	CS7 m2pa profile configuration
----------------------	--------------------------------

Command History	Release	Modification
	12.2(19)SW	This command was introduced.

Usage Guidelines	The idle-cwnd-rate parameter allows the administrator to configure a rate at which the SCTP congestion window will be decreased due to the SCTP association being idle. The SCTP congestion window will not decrease below the initial congestion window size regardless of the rate and the length of idle time.
-------------------------	---




Note

It is extremely important to note that the behavior of the SCTP congestion control algorithms are not compliant with RFC 2960 when this parameter is changed to values other than the default. This parameter should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples	The following example defines a profile named m2parfc, specifies that the profile supports M2PA RFC, specifies the idle-cwnd parameter in the profile, then applies the m2parfc profile to all the links in 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 will be decreased due to the association being idle. Range is 0 to 100 percent. The default is 50 percent.
---------------------------	----------------	---

Defaults	The default is 50 percent.
-----------------	----------------------------

Command Modes	CS7 m3ua configuration
----------------------	------------------------

Command History	Release	Modification
	12.2(19)SW	This command was introduced.

Usage Guidelines	The idle-cwnd-rate parameter allows the administrator to configure a rate at which the SCTP congestion window will be decreased due to the SCTP association being idle. The SCTP congestion window will not decrease below the initial congestion window size regardless of the rate and the length of idle time.
-------------------------	---



Note

It is extremely important to note that the behavior of the SCTP congestion control algorithms are not compliant with RFC 2960 when this parameter is changed to values other than the default. This parameter should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples	The following example set the idle congestion window rate to 60 percent.
-----------------	--

```
cs7 m3ua 2905 offload 2 0
local-ip 4.4.4.4
idle-cwnd-rate 60
```

Related Commands	Command	Description
	init-cwnd-size (cs7 m3ua)	Configure the SCTP initial congestion window size.

idle-cwnd-rate (cs7 sgmp)

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 sgmp 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 will be decreased due to the association being idle. Range is 0 to 100 percent. The default is 50 percent.
----------------	---

Defaults

The default is 50 percent.

Command Modes

CS7 sgmp configuration

Command History

Release	Modification
12.2(19)SW	This command was introduced.

Usage Guidelines

The idle-cwnd-rate parameter allows the administrator to configure a rate at which the SCTP congestion window will be decreased due to the SCTP association being idle. The SCTP congestion window will not decrease below the initial congestion window size regardless of the rate and the length of idle time.



Note

It is extremely important to note that the behavior of the SCTP congestion control algorithms are not compliant with RFC 2960 when this parameter is changed to values other than the default. This parameter should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples

The following example set the idle congestion window rate to 60 percent.

```
cs7 sgmp 5000
 local-ip 4.4.4.4
 idle-cwnd-rate 60
```

Related Commands

Command	Description
init-cwnd-size (cs7 sgmp)	Configure 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 will be decreased due to the association being idle. Range is 0 to 100 percent. The default is 50 percent.
----------------	---

Defaults

The default is 50 percent.

Command Modes

CS7 sua configuration

Command History

Release	Modification
12.2(19)SW	This command was introduced.

Usage Guidelines

The idle-cwnd-rate parameter allows the administrator to configure a rate at which the SCTP congestion window will be decreased due to the SCTP association being idle. The SCTP congestion window will not decrease below the initial congestion window size regardless of the rate and the length of idle time.



Note

It is extremely important to note that the behavior of the SCTP congestion control algorithms are not compliant with RFC 2960 when this parameter is changed to values other than the default. This parameter should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples

The following example 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)	Configure 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** | **both** } [**test**] { **silent** | **file** [**verbose**] | **console** [**verbose**] | **file** [**verbose**] **console** [**verbose**]}] **result** { **action** *action-set-name* | **table** *tablename* }

no inbound

Syntax Description

logging	(Optional) Enables logging.
type	Specifies logging type.
allow	Messages allowed for further processing.
block	Messages blocked.
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</i>	Action set name. Valid names may not exceed 12 alpha numeric characters.
table	Specifies that the next step is a table.
<i>table-name</i>	Name of the next step table.

Defaults

Default logging is silent

Command Modes

GWS AS configuration

Command History

Release	Modification
12.2(25)SW4	This command was introduced.

Examples

The following example configures inbound and outbound default screening for all ASes.

```
cs7 instance 0 gws as default
inbound logging type block file console verbose result table SIOO
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** | **both** } { **silent** | **file** [**verbose**] | **console** [**verbose**] | **file** [**verbose**] **console** [**verbose**]}] **result** { **action** *action-set-name* | **table** *tablename* }

no inbound

Syntax Description	
logging	(Optional) Enables logging.
type	Specifies logging type.
allow	Messages allowed for further processing.
block	Messages blocked.
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</i>	Action set name. Valid names may not exceed 12 alpha numeric characters.
table	Specifies that the next step is a table.
<i>table-name</i>	Name of the next step table.

Defaults Default logging is silent

Command Modes GWS linkset configuration

Command History	Release	Modification
	12.2(25)SW4	This command was introduced.

Examples The following example configures 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 2 times the smallest MTU of the SCTP interfaces (in bytes).
--------------------	---

Defaults

The default *window-size* is 2 times the smallest MTU of the SCTP interfaces (in bytes).

Command Modes

CS7 asp configuration

Command History

Release	Modification
12.2(19)SW	This command was introduced.

Usage Guidelines

The **init-cwnd-size** command allows the administrator to configure an initial congestion window size for an SCTP association.

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



Note

It is extremely important to note that the behavior of the SCTP congestion control algorithms are not compliant with RFC 2960 when this parameter is changed to values other than the default. This parameter should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples

The following example 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)	Configure 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 2 times the smallest MTU of the SCTP interfaces (in bytes).
--------------------	---

Defaults

The default *window-size* is 2 times the smallest MTU of the SCTP interfaces (in bytes).

Command Modes

CS7 link configuration

Command History

Release	Modification
12.2(19)SW	This command was introduced.

Usage Guidelines

The **init-cwnd-size** command allows the administrator to configure an initial congestion window size for an SCTP association.



Note

It is extremely important to note that the behavior of the SCTP congestion control algorithms are not compliant with RFC 2960 when this parameter is changed to values other than the default. This parameter should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples

The following example 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)	Configure 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 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 2 times the smallest MTU of the SCTP interfaces (in bytes).
--------------------	---

Defaults

The default *window-size* is 2 times the smallest MTU of the SCTP interfaces (in bytes).

Command Modes

CS7 m2pa profile configuration

Command History

Release	Modification
12.2(25)SW3	This command was introduced.

Usage Guidelines

The **init-cwnd-size** command allows the administrator to configure an initial congestion window size for an SCTP association.



Note

It is extremely important to note that the behavior of the SCTP congestion control algorithms are not compliant with RFC 2960 when this parameter is changed to values other than the default. This parameter should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples

The following example defines a profile named m2parfc, specifies that the profile supports M2PA RFC, specifies the **init-cwnd-size** parameter in the profile, then applies the m2parfc profile to all the links in 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 2 times the smallest MTU of the SCTP interfaces (in bytes).
--------------------	---

Defaults

The default *window-size* is 2 times the smallest MTU of the SCTP interfaces (in bytes).

Command Modes

CS7 m3ua configuration

Command History

Release	Modification
12.2(19)SW	This command was introduced.

Usage Guidelines

The **init-cwnd-size** command allows the administrator to configure an initial congestion window size for an SCTP association.



Note

It is extremely important to note that the behavior of the SCTP congestion control algorithms are not compliant with RFC 2960 when this parameter is changed to values other than the default. This parameter should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples

The following example 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)	Configure 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 2 times the smallest MTU of the SCTP interfaces (in bytes).
--------------------	---

Defaults

The default *window-size* is 2 times the smallest MTU of the SCTP interfaces (in bytes).

Command Modes

CS7 mated-sg configuration

Command History

Release	Modification
12.2(19)SW	This command was introduced.

Usage Guidelines

The **init-cwnd-size** command allows the administrator to configure an initial congestion window size for an SCTP association.



Note

It is extremely important to note that the behavior of the SCTP congestion control algorithms are not compliant with RFC 2960 when this parameter is changed to values other than the default. This parameter should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples

The following example 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)	Configure the local receive window size.

init-cwnd-size (cs7 sgmp)

To configure the SCTP initial congestion window size, use the `init-cwnd-size` command in `cs7 sgmp` 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 2 times the smallest MTU of the SCTP interfaces (in bytes).
--------------------	---

Defaults

The default *window-size* is 2 times the smallest MTU of the SCTP interfaces (in bytes).

Command Modes

CS7 sgmp configuration

Command History

Release	Modification
12.2(19)SW	This command was introduced.

Usage Guidelines

The **init-cwnd-size** command allows the administrator to configure an initial congestion window size for an SCTP association.



Note

It is extremely important to note that the behavior of the SCTP congestion control algorithms are not compliant with RFC 2960 when this parameter is changed to values other than the default. This parameter should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples

The following example set the initial congestion window size to 5000 bytes.

```
cs7 sgmp 5000
 local-ip 4.4.4.4
  init-cwnd-size 5000
```

Related Commands

Command	Description
receive-window (CS7 SGMP)	Configure 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 2 times the smallest MTU of the SCTP interfaces (in bytes).
--------------------	---

Defaults

The default *window-size* is 2 times the smallest MTU of the SCTP interfaces (in bytes).

Command Modes

CS7 sua configuration

Command History

Release	Modification
12.2(19)SW	This command was introduced.

Usage Guidelines

The **init-cwnd-size** command allows the administrator to configure an initial congestion window size for an SCTP association.



Note

It is extremely important to note that the behavior of the SCTP congestion control algorithms are not compliant with RFC 2960 when this parameter is changed to values other than the default. This parameter should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples

The following example set the initial congestion window size to 5000 bytes.

```
cs7 sua 15000 offload 2 0
local-ip 4.4.4.4
init-cwnd-size 5000
```

Related Commands

Command	Description
receive-window (CS7 SUA)	Configure the local receive window size.

init-ip-dscp

To set the Differential 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, use the **no** form of this command.

init-ip-dscp *dscp*

no init-ip-dscp *dscp*

Syntax Description	<i>dscp</i>	IP DSCP setting, in decimal notation. Valid range is 0 through 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	0
-----------------	---

Command Modes	CS7 local-peer configuration
----------------------	------------------------------

Command History	Release	Modification
	12.2(4)MB4	This command was introduced.

Examples	The following example sets the IP type of service to DSCP 56 for the peer link initialization packets:
	<pre>cs7 local-peer 4096 init-ip-dscp 56</pre>

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	
<i>ip-tos</i>	IP precedence setting, in decimal notation. Range is 0 through 7. The default is 0.

Defaults

The IP TOS default is 0.

Command Modes

CS7 local-peer configuration

Command History

Release	Modification
12.2(4)MB4	This command was introduced.

Examples

The following example sets 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 Differential 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 initialization packet retries. The range is 2 through 20. The default is 8 retries.
--------------------	---

Defaults

8 retries.

Command Modes

CS7 link configuration

Command History

Release	Modification
12.2(1)MB	This command was introduced.

Examples

The following example sets 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 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 initialization packet retries. The range is 2 through 20. The default is 8 retries.
--------------------	--------------------	---

Defaults	8 retries.
----------	------------

Command Modes	CS7 m2pa profile configuration
---------------	--------------------------------

Command History	Release	Modification
	12.2(25)SW3	This command was introduced.

Examples

The following example defines a profile named m2parfc, specifies that the profile supports M2PA RFC, specifies the **init-retransmit** parameter in the profile, then applies the m2parfc profile to all the links in 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 initialization packet retries. The range is 2 through 20. The default is 8 retries.	
Defaults	8 retries.	
Command Modes	CS7 m3ua configuration	
Command History	Release	Modification
	12.2(4)MB5	This command was introduced.
Examples	The following example sets the number of retransmissions for peer initialization messages to 10: cs7 m3ua 2905 offload 2 0 local-ip 4.4.4.4 init-retransmit 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.

init-retransmit (cs7 sgmp)

To configure the number of retransmissions for peer initialization packets for this local port, use the **init-retransmit** command in CS7 SGMP 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 initialization packet retries. The range is 2 through 20. The default is 8 retries.
---------------------------	--------------------	---

Defaults	8 retries.
-----------------	------------

Command Modes	CS7 sgmp configuration
----------------------	------------------------

Command History	Release	Modification
	12.2(4)MB5	This command was introduced.

Examples	The following example sets the number of retransmissions for peer initialization messages to 10: cs7 sgmp 5000 init-retransmit 10
-----------------	---

Related Commands	Command	Description
	cs7 sgmp	Specifies the local port number for SGMP and enters CS7 SGMP submode.
	show cs7 sgmp	Displays SGMP 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 initialization packet retries. The range is 2 through 20. The default is 8 retries.	
Defaults	8 retries.	
Command Modes	CS7 SUA submode	
Command History	Release	Modification
	12.2(4)MB5	This command was introduced.
Examples	<p>The following example sets the number of retransmissions for peer initialization messages to 10:</p> <pre>cs7 sua 15000 offload 2 0 local-ip 4.4.4.4 init-retransmit 10</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.

init-timeout (CS7 Link)

To configure the time-out 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(1)MB	This command was introduced.

Examples The following example sets 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 time-out 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 m2pa profile submode
---------------	--------------------------

Command History	Release	Modification
	12.2(25)SW3	This command was introduced.

Examples The following example defines a profile named m2parfc, specifies that the profile supports M2PA RFC, specifies the **init-timeout** parameter in the profile, then applies the m2parfc profile to all the links in linkset named to_nyc:

```
cs7 profile m2parfc
  m2pa
    init-timeout 2000
  .
.
cs7 linkset to_nyc
  profile m2parfc
```

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 time-out 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	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>12.2(4)MB5</td><td>This command was introduced.</td></tr></table>		Release	Modification	12.2(4)MB5	This command was introduced.		
Release	Modification							
12.2(4)MB5	This command was introduced.							
Examples	<p>The following example sets the timeout value for retransmission of association setup messages to 2000 milliseconds:</p> <pre>cs7 m3ua 2905 offload 2 0 local-ip 4.4.4.4 init- timeout 2000</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 enter M3UA submode.</td></tr><tr><td>show cs7 m3ua</td><td>Displays M2PA statistics.</td></tr></table>		Command	Description	cs7 m3ua	Specifies the local port number for M3UA and enter M3UA submode.	show cs7 m3ua	Displays M2PA statistics.
Command	Description							
cs7 m3ua	Specifies the local port number for M3UA and enter M3UA submode.							
show cs7 m3ua	Displays M2PA statistics.							

init-timeout (CS7 SGMP)

To configure the maximum interval for the init packet retransmission time-out value, use the **init-timeout** CS7 SGMP 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 SGMP submode

Command History

Release	Modification
12.2(4)MB5	This command was introduced.

Examples

The following example sets the timeout value for retransmission of association setup messages to 2000 milliseconds:

```
cs7 sgm 5000
  init- timeout 2000
```

Related Commands

Command	Description
cs7 sgm	Specifies the local port number for SGMP and enter CS7 SGMP submode.
show cs7 sgm	Displays SGMP statistics.

init-timeout (CS7 SUA)

To configure the maximum interval for the init packet retransmission time-out 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(4)MB5	This command was introduced.
Examples	<p>The following example sets the timeout value for retransmission of association setup messages to 2000 milliseconds:</p> <pre>cs7 sua 15000 offload 2 0 local-ip 4.4.4.4 init- timeout 2000</pre>	
Related Commands	Command	Description
	cs7 sua	Specifies the local port number for SUA and enter CS7 SUA submode.
	show cs7 sua	Displays SUA statistics.

insert-dpc-in-cdpa

To enable a global Multi-Layer Routing (MLR) option to insert a destination point code (dpc) into the called party (cdpa) point code (pc) for packets that are MLR routed, 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 MLR options configuration
----------------------	-------------------------------

Command History	Release	Modification
	12.2(18)IXB	This command was introduced.

Usage Guidelines	<p>The insert-dpc-in-cdpa command is a cdpa modification enhancement. When this option is configured and a packet is MLR routed, 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.</p>
-------------------------	---

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 MLR routed without the updated Signaling Connection Control part (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	<p>The following example enables global options and specifies that when a packet is MLR routed, the MTP dpc is inserted into the cdPa pc if the cdPa is null.</p>
-----------------	---

```
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 Differential Services Code Point (DSCP) bits in the IP header TOS byte, use the **ip-dscp** CS7 link submode command. To set the DSCP setting to the default, use the **no** form of this command.

ip-dscp *ip-tos*

no ip-dscp *ip-tos*

Syntax Description

<i>ip-tos</i>	IP DSCP setting, in decimal notation. Range is 5000 through 63. The default 0.
---------------	--

Defaults

The IP TOS default is 0.

Command Modes

CS7 m2pa profilesubmode

Command History

Release	Modification
12.2(25)SW3	This command was introduced.

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 defines a profile named m2parfc, specifies that the profile supports M2PA RFC, specifies the **ip-dscp** parameter in the profile, then applies the m2parfc profile to all the links in 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 through 7. The default is zero.
---------------	--

Defaults

Zero.

Command Modes

CS7 link submode

Command History

Release	Modification
12.2(1)MB	This command was introduced.

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 sets 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), page 672	Specifies a Differential 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 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 through 7. The default is zero.
---------------	--

Defaults

Zero.

Command Modes

CS7 m2pa profile submode

Command History

Release	Modification
12.2(25)SW3	This command was introduced.

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 defines a profile named m2parfc, specifies that the profile supports M2PA RFC, specifies the **ip-precedence** parameter in the profile, then applies the m2parfc profile to all the links in 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** *tablename*}

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 next step action-set. Valid names may not exceed 12 alpha numeric characters.
table	Specifies that the next step is a table.
<i>table-name</i>	Name of the next step table.

Command Default

No default behavior or values.

Command Modes

CS7 GWS ISUP Message Table configuration

Command History

Release	Modification
12.2(25)SW4	This command was introduced.

Usage Guidelines

[Table 28](#) lists ISUP message types.

Table 29 *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
RLC	RSC	SUS	SGM (ITU only)

Table 29 **ISUP Message Types (continued)**

SAM (ITU only)	SDN (ITU only)	UBA	UBL
UCIC	UPA (ITU only)	UPT (ITU only)	USR

Examples

The following example specifies three ISUP message types and the next step for each.

```
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 through 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(4)MB5	This command was introduced.

Examples

The following example sets 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 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, 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 through 30000 milliseconds. The default keepalive 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(1)MB	This command was introduced.

Examples	The following example sets 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 link 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 through 30000 milliseconds. The default keepalive 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(1)MB	This command was introduced.

Examples

The following example defines a profile named m2parfc, specifies that the profile supports M2PA RFC, specifies the **keepalive** parameter in the profile, then applies the m2parfc profile to all the links in 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, 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 through 30000 milliseconds. The default keepalive 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(4)MB5	This command was introduced.

Examples	The following example sets the keepalive value to 1000 milliseconds:
----------	--

```
cs7 m3ua 2905 offload 2 0
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, 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 through 30000 milliseconds. The default keepalive interval is 30000 milliseconds.
-------------	---

Defaults

Keepalive is enabled.

The keepalive interval defaults to the interval specified under the local port instance.

Command Modes

CS7 Mated-SG submode

Command History

Release	Modification
12.2(4)MB5	This command was introduced.

Examples

The following example sets the keepalive value to 1000 milliseconds:

```
cs7 mated-sg BLUE 2905
remote-ip 5.5.5.5
keepalive 1000
```

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 SGMP)

To specify a keepalive interval to be used when a new SCTP association is started with the local port, use the **keepalive** CS7 link 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 through 30000 milliseconds. The default keepalive interval is 30000 milliseconds.
-------------	---

Defaults

Keepalive is enabled.

The default keepalive interval is 30000 milliseconds.

Command Modes

CS7 SGMP submode

Command History

Release	Modification
12.2(4)MB5	This command was introduced.

Examples

The following example sets the keepalive value to 1000 milliseconds:

```
cs7 sgmp 5000
local-ip 4.4.4.4
keepalive 1000
```

Related Commands

Command	Description
cs7 sgmp	Specifies the local port number for SGMP and enters CS7 SGMP submode.
show cs7 sgmp	Displays SGMP 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 link 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 through 30000 milliseconds. The default keepalive 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(4)MB5	This command was introduced.

Examples

The following example sets the keepalive value to 1000 milliseconds:

```
cs7 sua 15000 offload 2 0
local-ip 4.4.4.4
keepalive 1000
```

Related Commands

Command	Description
cs7 sua	Specifies the local port number for SUA and enters CS7 SUA submode.
show cs7 sua	Displays SUA statistics.

linestate debounce

To suppress rapid linestate transitions that may occur due to brief interruption of the framing on an E1, 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

No default behavior or values

Command Modes

Controller configuration

Command History

Release	Modification
12.2(18)IXB	This command was introduced.

Usage Guidelines

Enabling linestate debounce changes the behavior for an individual E1 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 enables 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** CS7 linkset submode command. To remove a link from a linkset, use the **no** form of this command. It is required that a link be in shutdown state before it can be removed from a linkset.

To configure a link to an ITP SS7 device, use the **link** CS7 linkset submode command.

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 0-15. 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 group peer on which the link physically resides. The <i>name</i> parameter is only valid (and required) 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. (examples: 3/0, 1/1/0).
sctp	Stream Control Transmission Protocol
<i>remote-ip-addr</i>	Remote IP address. This is one of the four IP address configured as a 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>	The remote port number. This is the local port number that was configured on the remote ITP.
<i>local-port-num</i>	The 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 dot (.) 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 end point using the pre-RFC M2PA protocol (draft2) communicates with the ITP, then the 12.2(25)SW3 software will switch to the M2PA draft2 protocol.

Command Modes

CS7 linkset submode

Command History

Release	Modification
12.2(1)MB	This command was introduced.
12.2(23)SW	The <i>name</i> parameter was added.
12.2(25)SW3	The draft2 keyword was added.
12.2(18)IXC	The <i>subinterface</i> argument was added for ATM HSL links.

Usage Guidelines

SLC must be the same at both ends of the signaling link to align.

When you issue the **link** command you enter CS7 link submode. In CS7 link submode you have access to commands that allow you to further configure links.

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 end point. If an end point using the M2PA draft2 protocol communicates with the ITP, then the 12.2(25)SW3 software will switch to the M2PA draft2 protocol. If an end point using the M2PA RFC protocol communicates with the ITP, then the 12.2(25)SW3 software uses the M2PA RFC protocol. This 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 end point to use the M2PA draft2 protocol. If the end point does not communicate using M2PA draft2 protocol then the M2PA link will not come up.

Examples

The following example configures 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 assigns link 0 to the ITP linkset named white and assigns 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 assigns link 0 to the ITP linkset named white and assigns 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.

link-test

Link test is performed by sending an SLTM message and verifying the acknowledgement (SLTA) from the adjacent node. Link test is performed on serial and peer links. To enable link-test, use the **link-test** CS7 link submode command. To disable link test, use the **no** form of this command.

link-test

no link-test

Syntax Description

This command has no arguments or keywords.

Defaults

Link-test is enabled by default and tests the links every 30 seconds.

A link test is automatically run when the link first comes into service.

Command Modes

CS7 link submode command

Command History

Release	Modification
12.2(1)MB	This command was introduced.

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 will be sent. If an SLTA is not received for the second SLTM, then the link restoration and activation procedure is initiated.

The command **no link-test** disables the link test. The command **link-test** re-enables link test.

Examples

The following example disables link test:

```
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 | 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 ANSI or ITU defined.

Syntax Description

retry msec	(ANSI, ITU) Link activation retry timer. (ANSI, ITU) Range of msec is 60000 through 90000 milliseconds. Default is 60000 milliseconds.
slt-t1 msec	(ANSI, ITU) Link test acknowledgment timer. (ANSI, ITU) ITU Range of msec is 4000 through 12000 milliseconds. Default is 8000 milliseconds.
slt-t2 msec	(ANSI, ITU) Interval timer for sending test messages. (ANSI, ITU) Range of msec is 30000 through 90000 milliseconds. (ANSI, ITU) Default is 60000 milliseconds.
t01 msec	(ANSI, ITU) Delay to avoid message mis-sequencing. (ANSI, ITU) Range of msec is 500 through 1200 milliseconds. (ANSI, ITU) Default is 800 milliseconds.
t02 msec	(ANSI, ITU) Wait for changeover acknowledgment. (ANSI, ITU) Range of msec is 700 through 2000 milliseconds. (ANSI, ITU) Default is 1400 milliseconds.
t03 msec	(ANSI, ITU) Delay to avoid mis-sequencing in changeback. (ANSI, ITU) Range of msec is 500 through 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 through 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 through 1200 milliseconds. (ANSI, ITU) Default is 800 milliseconds.
t12 msec	(ANSI, ITU) Wait for uninhibited acknowledgment. (ANSI, ITU) Range of msec is 800 through 1500 milliseconds. (ANSI, ITU) Default is 1150 milliseconds.
t13 msec	(ANSI, ITU) Wait for force uninhibited. (ANSI, ITU) Range of msec is 800 through 1500 milliseconds. (ANSI, ITU) Default is 1150 milliseconds.
t14 msec	(ANSI, ITU) Wait for inhibition acknowledgment. (ANSI, ITU) Range of msec is 2000 through 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 through 1500 milliseconds. (ANSI, ITU) Default is 1150 milliseconds.
t19 msec	(ANSI) Failed link craft referral timer. (ANSI) Range of <i>msec</i> is 480000 through 600000 milliseconds. (ANSI) Default is 540000.
t20 msec	(ANSI) Waiting to repeat local inhibit test. (ANSI) Range of <i>msec</i> is 90000 through 120000 milliseconds. (ANSI) Default is 105000 milliseconds.
t21 msec	(ANSI) Waiting to repeat remote inhibit test. (ANSI) Range of <i>msec</i> is 90000 through 120000 milliseconds. (ANSI) Default is 105000 milliseconds.
t22 msec	(ITU) Local inhibit test timer. (ITU) Range of <i>msec</i> is 180000 through 360000 milliseconds. (ITU) Default is 300000 milliseconds.
t23 msec	(ITU) Remote inhibit test timer. (ITU) Range of <i>msec</i> is 180000 through 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 through 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 through 35000 milliseconds. (ANSI) Default is 30000 milliseconds.
t32 msec	(ANSI) Link oscillation timer - Procedure A. Range of <i>msec</i> is 60000 through 120000 milliseconds. Default is 60000 milliseconds.

Defaults

See defaults listed in Syntax Description.

Command Modes

CS7 link submode

Command History

Release	Modification
12.2(1)MB	This command was introduced.

Usage Guidelines

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.

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 will override any global values.

All 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.

Examples

The following example sets 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 links 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 tablet load route table contents from flash, use the **load** command in route table configuration mode. To remove the **load** command from the configuration, use the **no** version 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 No default behavior or values.

Command Modes Route table configuration

Command History	Release	Modification
	12.2(1)MB	This command was introduced.
	12.2(4)MB	Command revised.

Usage Guidelines The **load** command will enter the (new) routing table immediately. When reloading the router, the **load** command will be executed before any update route.

Removing the **load** command from the configuration will not empty the routing table, but no table will be loaded when the next router reload occurs.

Use this command to load an MTP3 route-table upon ITP startup. At startup the ITP will load 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 re-applied.

Examples The following example loads 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 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

No default behavior or values.

Command Modes

CS7 local peer

Command History

Release	Modification
12.2(1)MB	This command was introduced.

Usage Guidelines

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.

When configuring multiple IP addresses for SCTP multi-homing, at least one of the configured IP addresses must be associated with the slot and bay specified on the instance.

Examples

The following example assigns IP address 172.18.44.254 to the local peer at port 7000:

```
cs7 local-peer 7000 offload 2 0
 local-ip 172.18.44.254
```

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	No default behavior or values.
----------	--------------------------------

Command Modes	CS7 M3UA
---------------	----------

Command History	Release	Modification
	12.2(4)MB5	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 multi-homing by specifying additional local-ip commands. The local port will receive packets from only an IP address that was configured.
------------------	---

When configuring multiple IP addresses for SCTP multi-homing, at least one of the configured IP addresses must be associated with the slot and bay specified on the instance.

The local-ip associated with an instance can only be added on the first visit to the instance submode, or when the instance submode is shutdown. The local-ip associated with an instance can only be removed when the instance is shutdown.

Examples	The following example assigns IP address 4.4.4.4 to the local peer at port 2905:
----------	--

```
cs7 m3ua 2905 offload 2 0
  local-ip 4.4.4.4
```

Related Commands	Command	Description
	cs7 m3ua	Specifies the local port number for M3UA and enter M3UA submode.

local-ip (CS7 SGMP)

To configure a local IP address for an instance, use the **local-ip** CS7 SGMP 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	No default behavior or values.
----------	--------------------------------

Command Modes	CS7 SGMP
---------------	----------

Command History	Release	Modification
	12.2(4)MB5	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 multi-homing by specifying additional local-ip commands. The local port will receive packets from only an IP address that was configured.
------------------	---

The local-ip associated with an instance can only be added on the first visit to the instance submode, or when the instance submode is shutdown. The local-ip associated with an instance can only be removed when the instance is shutdown.

Examples	The following example assigns IP address 4.4.4.4 to the local peer at port 5000:
----------	--

```
cs7 sgmp 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	No default behavior or values.
----------	--------------------------------

Command Modes	CS7 SUA
---------------	---------

Command History	Release	Modification
	12.2(4)MB5	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 multi-homing by specifying additional local-ip commands. The local port will receive packets from only an IP address that was configured.
------------------	---

When configuring multiple IP addresses for SCTP multi-homing, at least one of the configured IP addresses must be associated with the slot and bay specified on the instance.

The local-ip associated with an instance can only be added on the first visit to the instance submode, or when the instance submode is shutdown. The local-ip associated with an instance can only be removed when the instance is shutdown.

Examples	The following example assigns IP address 4.4.4.4 to the local peer at port 15000:
----------	---

```
cs7 sua 15000 offload 2 0
  local-ip 4.4.4.4
```

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 the command.

m2pa

no m2pa

Syntax Description

This command has no arguments or keywords.

Defaults

No default

Command Modes

CS7 profile configuration

Command History

Release	Modification
12.2(25)SW3	This command was introduced.

Examples

The following example defines a profile named m2parfc, specifies that the profile supports M2PA RFC, specifies the **hold-transport** parameter in the profile, then applies the m2parfc profile to all the links in 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 Differential 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	
retransmit-timeout	
tx-queue-depth (cs7 link)	Configures the MTP2 transmit queue depth.

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 the command.

match access-group

no match access-group

Syntax Description This command has no arguments or keywords.

Command Modes CS7 linkset submode

Command History	Release	Modification
	12.2(4)MB	This command was introduced.

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 enables access lists 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 the 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 through 7.
	<i>instance-number</i>	Required if multiple instances is configured. The valid range is 0 through 7. The default instance is instance 0.

Command Modes	CS7 ASP submode
---------------	-----------------

Command History	Release	Modification
	12.2(4)MB5	This command was introduced.

Examples The following example assigns 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 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 the 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 through 7.
Command Modes	CS7 linkset submode	
Command History	Release	Modification
	12.2(4)MB	This command was introduced.
Usage Guidelines	This command should be used on input linksets with legacy SS7 links.	
Examples	The following example configures input linkset packet classification and assigns QoS class 4 to the incoming packets:	
	<pre>cs7 linkset to-washington 3.3.3 match any qos-class 4</pre>	
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 the 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 through 15.
qos-class	Specifies a QoS class.
<i>class</i>	QoS class ID. Valid range is 1 through 7.
<i>instance-number</i>	Required if multiple instances is configured. The valid range is 0 through 7. The default instance is instance 0.

Command Modes

CS7 ASP configuration

Command History

Release	Modification
12.2(4)MB5	This command was introduced.

Examples

The following example assigns 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 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 the 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 through 15.
qos-class	Specifies a QoS class.
<i>class</i>	QoS class ID. Valid range is 1 through 7.

Command Modes

CS7 linkset configuration

Command History

Release	Modification
12.2(4)MB	This command was introduced.

Usage Guidelines

This command should be used on input linksets with legacy SS7 links.

Examples

The following example configures 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)

Use the **match-unknown-ton-np** command in CS7 MLR ruleset rule configuration mode to specify 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. 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	No default behavior or values
-----------------	-------------------------------

Command Modes	CS7 MLR ruleset rule configuration
----------------------	------------------------------------

Command History	Release	Modification
	12.2(25)SW3	This command was introduced.

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. One effect of the **match-unknown-ton-np** command is to preserve the pre-12.2(25)SW3 noa/np matching rules, with regard to unknown noa/np values.

In ITP releases prior to release 12.2(25)SW3 there was not a configuration to match a rule parameter of type noa 0 (unknown noa) to **only** those messages that have an unknown noa value in the corresponding parameter. With release 12.2 (25)SW3 that type of match is configurable. These usage guidelines describe 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 prior to ITP release 12.2(25)SW3

In ITP releases prior to 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 keyword **ton** replaces the keyword **noa**. 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/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 since the pre-12.2(25)SW3 MLR action is to match that rule to incoming messages containing unknown ton and np 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 Short Message Entity (SME) within an MLR operation.
	orig-sme-table (cs7 mlr ruleset rule)	Specifies a table of origin SME addresses that will be used to find the desired routing destination.
	rule (cs7 mlr ruleset rule)	Specifies a rule and the order in which is searched, within a multi-layer ruleset table.

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 the local port. The range is 2 to 25. The default is 17 streams.							
Defaults	17 streams							
Command Modes	CS7 M3UA							
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>12.2(4)MB5</td><td>This command was introduced.</td></tr></table>		Release	Modification	12.2(4)MB5	This command was introduced.		
Release	Modification							
12.2(4)MB5	This command was introduced.							
Examples	<p>The following command specifies that a maximum of 10 streams is allowed on the local port:</p> <pre>cs7 m3ua 2905 offload 2 0 local-ip 4.4.4.4 max-inbound-streams 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.							

max-inbound-streams (CS7 SGMP)

To configure the maximum number of inbound streams allowed for the local port, use the **max-inbound-streams** CS7 SGMP 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 the local port. The range is 2 to 25. The default is 17 streams.
---------------------------	--------------------	--

Defaults	17 streams
-----------------	------------

Command Modes	CS7 SGMP
----------------------	----------

Command History	Release	Modification
	12.2(4)MB5	This command was introduced.

Examples The following command specifies that a maximum of 10 streams is allowed on the local port:

```
cs7 sgmp 5000
local-ip 4.4.4.4
max-inbound-streams 10
```

Related Commands	Command	Description
	cs7 sgmp	Specifies the local port number for SGMP and enters CS7 SGMP submode.
	show cs7 sgmp	Displays SGMP 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 the local port. The range is 2 to 25. The default is 17 streams.
--------------------	--

Defaults

17 streams

Command Modes

CS7 SUA

Command History

Release	Modification
12.2(4)MB5	This command was introduced.

Examples

The following command specifies that a maximum of 10 streams is allowed on the local port:

```
cs7 sua 15000 offload 2 0
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 (cs7 mlr option)

To specify the desired action when MLR packet modification fails, use the **modify-failure** command in cs7 mlr option 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

modify-failure	Indicates the action to be taken when a MLR packet modification fails.
discard	Discard 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.
<i>sccp-error</i>	SCCP UDTS return cause values

Defaults

The default value is that the packet is discarded.

Usage Guidelines

Modify-failure 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.

Examples

```
cs7 mlr options
  modify-failure sccp-error 7
```

modify-profile (cs7 mlr ruleset rule)

To specify SCCP and MAP addresses to modify in messages which are MLR routed, use the **modify-profile** command in `cfg-cs7-mlr-set-rule` configuration submode. Use the **no** form of the command to disable the settings.

[modify-profile profile-name]

no [modify-profile profile-name]

Syntax Description	modify-profile	The modify-profile keyword is used to assign 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 be associated with a defined MLR modify-profile. The name is specified as a character string with a maximum of 12 characters.

Command Modes	cs7 mlr ruleset rule (cfg-cs7-mlr-set-rule) configuration submode
----------------------	---

Command History	12.2(18)IXC	This command was introduced.
------------------------	-------------	------------------------------

Examples	<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 sri-sm default orig-smsc 397777777 modify-profile SRISM result route </pre>
-----------------	--

Related Commands	Command	Description
	cs7 mlr ruleset	Specifies the rules for a routing trigger within a multi-layer ruleset table and enables CS7 MLR ruleset-rule configuration mode.
	rule (cs7 mlr ruleset)	Specifies the rules for a routing trigger within a multi-layer ruleset table.
	cs7 mlr modify-profile	Specifies an MLR modify profile.

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	Disabled
-----------------	----------

Command Modes	CS7 profile submode
----------------------	---------------------

Command History	Release	Modification
	12.2(4)MB	This command was introduced.

Examples	The following example defines a profile named timers, configures the profile to support MTP2, configures the t1 and t2 settings in the timers profile, then applies the timers profile to all the links in linkset ITPa:
-----------------	--

```
cs7 profile timers
 mtp2
  timer t1 15000
  timer t2 9000
.
.
.
cs7 linkset itpa
 profile timers
```

Related Commands	Command	Description
	cs7 profile	Defines a profile that you can apply to all 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 the 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	<p>ttc ta timer: TTC Timer for sending SIE. Valid range is 10 to 250 milliseconds. Default is 20 milliseconds.</p> <p>ttc te timer: TTC Timer for error monitoring. Valid range is 10 to 250 milliseconds. Default is 20 milliseconds.</p> <p>ttc tf timer: TTC Timer for sending FISU. Valid range is 10 to 250 milliseconds. Default is 20 milliseconds.</p> <p>ttc to timer: TTC Timer for sending SIO. Valid range is 10 to 250 milliseconds. Default is 20 milliseconds.</p> <p>ttc ts timer: TTC Timer for sending SIOS. Valid range is 10 to 250 milliseconds. Default is 20 milliseconds.</p>

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(4)MB	This command replaced the cs7 mtp2 interface configuration command.
	12.2(20)SW	TTC timers were added.

Usage Guidelines MTP2 parameters can also be specified in a CS7 profile.

Examples The following example sets the T1 timer for 25000 milliseconds:

```
cs7 linkset ITP2 6.100.5
link 0 serial0/0:0
→ mtp2-timer t1 25000
```

The following example sets 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	Define a profile of MTP2 parameters that you can apply to all 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 the command.

mtp2-timer ttc enable

no mtp2-timer ttc enable

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Defaults	No default behavior or values.
-----------------	--------------------------------

Command Modes	CS7 link submode
----------------------	------------------

Command History	Release	Modification
	12.2(20)SW	This command was introduced.

Usage Guidelines	After enabling the use of MTP2 TTC timers, you can set the timer values.
-------------------------	--

Examples	The following example enables 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	Tune MTP2 encapsulation timers.
	show cs7 mtp2	Displays ITP MTP2 status.

multi-message-dialogue (cs7 mlr ruleset rule)

Use the **multi-message-dialogue** command in cs7 mlr ruleset-rule configuration mode 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. To remove the specification, use the **no** form of this command.

multi-message-dialogue

no multi-message-dialogue

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Defaults	No default behavior or value
-----------------	------------------------------

Command Modes	CS7 MLR ruleset rule configuration
----------------------	------------------------------------

Command History	Release	Modification
	12.2(25)SW	This command was introduced.

Usage Guidelines	If the multi-message-dialogue command is configured, no other routing parameters may be configured within the CS7 mlr ruleset-rule configuration mode.
-------------------------	---

Unlike other routing parameters, this parameter is valid in a rule defined with the **all** operation.

The **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 specifies the multi-message-dialogue command:
-----------------	---

```
cs7 mlr ruleset ruleset1
rule 10 sms-mt
multi-message-dialogue
result group SMS1
```

Related Commands	Command	Description
	rule (cs7 mlr ruleset)	Specifies the rules for a routing trigger within a multi-layer ruleset table.

multiplicity

To specify a method for selecting destination in the application group, use the **multiplicity** CS7 gtt application group submode command. To restore the default multiplicity (share) use the **no** form of this command.

multiplicity {[cost | share | cgpa]}

no multiplicity

Syntax Description

cost	Use the destination with the least cost if available.
share	Share equally between all destinations.
cgpa	Use 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.

Defaults

The default multiplicity is share.

Command Modes

CS7 GTT application group configuration

Command History

Release	Modification
12.2(4)MB	This command was introduced.

Examples

The following example configures an application group with 3 items using the multiplicity command with the cgpa keyword. The first item gets used approximately twice as many times as the other two. The remaining 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.

nai

To specify a new nature of address 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 through 127.
------------	--

Defaults

No default behavior or values.

Command Modes

CS7 GTT address conversion submode

Command History

Release	Modification
12.2(4)MB2	This command was introduced.

Examples

The following example specifies that the *nai* value will be converted 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	No default behavior or values.
-----------------	--------------------------------

Command Modes	CS7 AS
----------------------	--------

Command History	Release	Modification
	12.2(19)SW	This command was introduced.

Usage Guidelines	If <code>network-appearance</code> is not configured, the actual instance number is used instead. If <code>network-appearance</code> is already configured on another AS, it is valid only if the other AS has the same instance.
-------------------------	---

Examples	The following example defines <code>network-appearance</code> parameter as 100: <code>network-appearance 100</code>
-----------------	--

Related Commands	Command	Description
	cs7 multi-instance	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 commando disable the configuration, use the **no** form of this command.

new-name *newselector*

no new-name

Syntax Description

<i>newselector</i>	New name for the GTT Selector.
--------------------	--------------------------------

Defaults

No default behavior or values

Command Modes

CS7 GTT Selector submode

Command History

Release	Modification
12.2(4)MB	This command was introduced.

Examples

The following example renames 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.

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 through 15.
--------------------	-----------	--

Defaults	No default behavior or values
----------	-------------------------------

Command Modes	CS7 GTT address conversion submode
---------------	------------------------------------

Command History	Release	Modification
	12.2(4)MB2	This command was introduced.

Examples	The following example specifies that the np value will be converted 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.

orig-imsi (cs7 mlr ruleset rule)

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.
	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.
	unknown	Unknown origin IMSI.

Defaults No default behavior or values

Command Modes CS7 mlr ruleset rule configuration

Command History	Release	Modification
	12.2(25)SW	This command was introduced.

Examples The following example specifies a ruleset named ruleset1, specifies a rule index of 20, and specifies an origin IMSI address 1111:

```
cs7 sms ruleset SMS-RULES
rule 20 sms-mo
orig-imsi 1111
result group grp1
```

Related Commands	Command	Description
	rule (cs7 mlr ruleset)	Specifies the rules for a routing trigger within a multi-layer ruleset table and enables CS7 MLR ruleset-rule configuration mode.

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 *tablename* [**noa** *noa-value* **np** *np-value*]

no orig-imsi-table *tablename*

Syntax Description

<i>tablename</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

No default behavior or values

Command Modes

CS7 mlr ruleset rule configuration

Command History

Release	Modification
12.2(25)SW	This command was introduced.

Usage Guidelines

The **dest-sme-table**, **orig-imsi-table**, and **orig-sme-table** rule parameters accept either an SMS address-table name OR an MLR address-table name. This ability is primarily for customers that 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 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** must match before the table is accessed.

Examples

The following example specifies an MLR ruleset named ruleset1, specifies a rule index of 20, and specifies an SMS table of origin IMSI addresses named SHORTLIST:

```
cs7 mlr ruleset ruleset1
rule 20 sms-mo
  orig-imsi-table SHORTLIST
  result block
```

Related Commands

Command	Description
rule (cs7 mlr ruleset)	Specifies the rules for a routing trigger within a multi-layer ruleset table and enables CS7 MLR ruleset-rule configuration mode.

orig-sme (cs7 mlr ruleset rule)

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	
<i>*</i>	Match all addresses
<i>address</i>	<p>When the rule operation is sms-mo, the <i>address</i> is an address string of 1 to 20 hexadecimal characters.</p> <p>When the rule operation is sms-mt, the <i>address</i> is an address string of 1 to 16 hexadecimal characters.</p> <p>The string is not input in BCD-String format, but in normal form. The string always carries an implicit '*' at the end of the string, allowing only the prefix of a range of addresses to be specified.</p>
exact	(Optional) The previously specified <i>orig-addr</i> should only be matched if the number of digits and the digit values exactly match. If exact is not specified, the <i>orig-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	(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>	<p>(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:</p> <ul style="list-style-type: none"> [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

No default behavior or values.

Command Modes

CS7 MLR ruleset rule configuration

Command History

Release	Modification
12.2(4)MB	This command was introduced.
12.2(21)SW	The exact keyword was added.
12.2(25)SW3	The keyword/argument ton ton replaced the keyword/argument noa noa .

Usage Guidelines**MLR/SMS rule-matching implementations prior to ITP release 12.2(25)SW3**

In ITP releases prior to 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 keyword **ton** replaces the keyword **noa**. 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 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 30 **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 specifies 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 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 multi-layer ruleset table and enables CS7 MLR ruleset-rule configuration mode.

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 *tablename* [**ton** *ton-value*] [**np** *np-value*]

no orig-sme-table *tablename* [**ton** *ton-value*] [**np** *np-value*]

Syntax Description

<i>tablename</i>	Identifies the name of a previously defined MLR address table that is to be used when searching with the orig-sme-table routing parameter. 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

No default behavior or values

Command Modes

CS7 mlr ruleset rule configuration

Command History

Release	Modification
12.2(25)SW	This command was introduced.
12.2(25)SW3	The keyword/argument ton <i>ton</i> replaced the keyword/argument noa <i>noa</i> .

Usage Guidelines

MLR/SMS rule-matching implementations prior to ITP release 12.2(25)SW3

In ITP releases prior to 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 keyword **ton** replaces the keyword **noa**. 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 parameters accept either an SMS address-table name OR an MLR address-table name. This ability is primarily for customers that want the SMS-MO Proxy functionality. The address-table names are unique between FDA 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 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 specifies an SMS ruleset named ruleset1, specifies a rule index of 20, and specifies 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 multi-layer ruleset table and enables CS7 MLR ruleset-rule configuration mode.

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	
*	Match 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. The <i>addr-type</i> is composed of the following keywords: <ul style="list-style-type: none"> The noa keyword specifies the nature-of-address value associated with the SMSC address. Messages received with an 'Unknown' (0) value will match any non-zero 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 non-zero 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 *orig-sme-addr-type* address defaults to an E.164/telephony address with international scope.

Command Modes CS7 mlr ruleset rule

Command History	Release	Modification
	12.2(19)SW	This command was introduced.
	12.2(21)SW	The exact keyword was added.

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, and it 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 specifies the originating service center address:

```
cs7 mlr ruleset ruleset1
rule 20 sms-mo
  orig-smsc 1111
  result block
```

Related Commands

Command	Description
rule (cs7 mlr ruleset)	Specifies the rules for a routing trigger within a multi-layer 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 the 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		
orig-smsc		Identifies that the originating service centre address needs to be modified.
prefix		The prefix keyword specifies that 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 '*' should be specified. To replace the entire address, specify that the maximum 38 digits are to be removed.
<i>prefix-add-digits</i>		An string of 1 to 38 hexadecimal digits which are to be added to the beginning of the address. If no digits are to be added, then '*' should be specified in this field. If the number of digits in the modified address would exceed 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		The ton keyword is used to indicate 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		The np keyword is used to indicate a numbering plan (np) replacement.
<i>new-np</i>		An integer in the range of 0 to 15 which defines the new numbering plan (NP) value for the modified address.

Command Modes	cs7 mlr modify-profile (cfg-cs7-mlr-modify)
---------------	---

Command History	12.2(18)IXC	This command was introduced.
-----------------	-------------	------------------------------

Usage Guidelines	For the 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 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.

Examples

```
cs7 mlr modify-profile gsm-map SRISM sri-sm
orig-smsc prefix 2 351
cgpa gt prefix 2 351
```

Related Commands

Command	Description
cs7 mlr modify-profile	Specifies an MLR modify profile.
modify-failure (cs7 mlr option)	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** | **both** } { **silent** | **file** [**verbose**] | **console** [**verbose**] | **file** [**verbose**] **console** [**verbose**]}] **result** { **action** *action-set-name* | **table** *tablename* }

no **outbound**

Syntax Description

logging	(Optional) Enables logging.
type	Specifies logging type.
allow	Messages allowed for further processing.
block	Messages blocked.
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</i>	Name of the next step action-set. Valid names may not exceed 12 alpha numeric characters.
table	Specifies that the next step is a table.
<i>table-name</i>	Name of the next step table.

Defaults

Default logging is silent

Command Modes

GWS AS configuration

Command History

Release	Modification
12.2(25)SW4	This command was introduced.

Examples

The following example configures outbound screening on an AS named as2.

```
cs7 instance 0 gws as name as2
  outbound result action ALLOW
```


The following example configures 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 a 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** | **both** } { **silent** | **file** [verbose] | **console** [verbose] | **file** [verbose] **console** [verbose]] **result** { **action** action-set-name | **table** tablename }

no outbound [logging type { **allow** | **block** | **both** } { **silent** | **file** [verbose] | **console** [verbose] | **file** [verbose] **console** [verbose]] **result** { **action** action-set-name | **table** tablename }

Syntax Description

logging	(Optional) Enables logging.
type	Specifies logging type.
allow	Messages allowed for further processing.
block	Messages blocked.
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</i>	Name of the next step action-set. Valid names may not exceed 12 alpha numeric characters.
table	Specifies that the next step is a table.
<i>table-name</i>	Name of the next step table.

Defaults

Default logging is silent

Command Modes

GWS linkset configuration

Command History

Release	Modification
12.2(25)SW4	This command was introduced.

Examples

The following example configures 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 as	Displays ITP gateway screening information for the AS.

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 through 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 ASP submode

Command History

Release	Modification
12.2(4)MB5	This command was introduced.

Examples

The following example sets 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 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 through 10 retries. The default is four retries.
---------------------------	--------------------	---

Defaults	Four retries.
-----------------	---------------

Command Modes	CS7 link submode
----------------------	------------------

Command History	Release	Modification
	12.2(1)MB	This command was introduced.

Usage Guidelines	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.
-------------------------	--

Examples	The following example sets the number of path retransmit retries to 10:
-----------------	---

```
cs7 linkset michael 10.1.1
link 0 sctp 172.18.44.147 7000 7000
path-retransmit 10
```

Related Commands	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 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 through 10 retries. The default is four retries.
---------------------------	--------------------	---

Defaults	Four retries.
-----------------	---------------

Command Modes	CS7 m2pa profile configuration
----------------------	--------------------------------

Command History	Release	Modification
	12.2(25)SW3	This command was introduced.

Usage Guidelines	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.
-------------------------	--

Examples	The following example defines a profile named m2parfc, specifies that the profile supports M2PA RFC, specifies the path-retransmit parameter in the profile, then applies the m2parfc profile to all the links in 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 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 through 10 retries. The default is four retries.
---------------------------	--------------------	---

Defaults	Four retries.
-----------------	---------------

Command Modes	CS7 M3UA submode
----------------------	------------------

Command History	Release	Modification
	12.2(4)MB5	This command was introduced.

Examples	The following example sets the number of path retransmit retries to 10:
-----------------	---

```
cs7 m3ua 2905 offload 2 0
local-ip 4.4.4.4
path-retransmit 10
```

Related Commands	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 through 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(4)MB5	This command was introduced.

Examples

The following example sets 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 SGMP)

To configure the maximum number 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 SGMP 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 through 10 retries. The default is four retries.
---------------------------	--------------------	---

Defaults	Four retries.
-----------------	---------------

Command Modes	CS7 SGMP submode
----------------------	------------------

Command History	Release	Modification
	12.2(4)MB5	This command was introduced.

Examples	The following example sets the number of path retransmit retries to 10:
-----------------	---

```
cs7 sgmp 5000
local-ip 4.4.4.4
path-retransmit 10
```

Related Commands	Command	Description
	cs7 sgmp	Specifies the local port number for SGMP and enables CS7 SGMP submode.

path-retransmit (CS7 SUA)

To configure the maximum number 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 through 10 retries. The default is four retries.
--------------------	---

Defaults

Four retries.

Command Modes

CS7 SUA submode

Command History

Release	Modification
12.2(4)MB5	This command was introduced.

Examples

The following example sets the number of path retransmit retries to 10:

```
cs7 sua 15000 offload 2 0
 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 configuration mode. To remove the point code and optional subsystem number, use the **no** form of the command.

```
[instance instance-number] pc pc [ssn ssn] [cost | wf] {gt | pcssn}
```

```
no [instance instance-number] pc pc [ssn ssn] [cost | wf] {gt | pcssn}
```

Syntax Description

instance	Specifies an instance.
<i>instance-number</i>	Instance number.
<i>pc</i>	Point code, in the form zone.region.sp.
ssn	(Optional) Specifies a subsystem number.
<i>ssn</i>	Subsystem number. Valid range is 2 through 255.
<i>cost</i>	Cost. Valid range is 1 through 8.
<i>wf</i>	Weighing factor. Any items added to the group require a cost if the multiplicity is specified as cgpa .
gt	Set the Routing Indicator to “route on global title.”
pcssn	Set the Routing Indicator to route on point code and subsystem number.

Defaults

No default behavior or values

Command Modes

CS7 gtt application group configuration

Command History

Release	Modification
12.2(4)MB	This command was introduced.
12.2(20)SW	The instance keyword was added.

Examples

The following example specifies 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 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.

pc *dest-pc* [**ssn** *ssn*] [**order** *order*] [**weight** *weight*]

no **pc** *dest-pc* [**ssn** *ssn*] [**order** *order*] [**weight** *weight*]

Syntax Description

<i>dest-pc</i>	A destination point code in variant-specific point-code format.
ssn	(Optional) Specifies that a subsystem number will 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) Specify 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 non-zero weighted resources are unavailable. If multiple zero-weighted resources exist, then messages are equally distributed between them if all non-zero weighted resources fail. If not specified, a default weight of 1 is used.

Defaults

If not specified, a default weight of 1 is used.

Command Modes

CS7 mlr result configuration

Command History

Release	Modification
12.2(4)MB	This command was introduced.
12.2(25)SW4	The order keyword was added. The <i>weight</i> interval for dest-sme-binding was added.

Usage Guidelines

If multiple zero-weighted resources exist, then messages are equally distributed between them if all non-zero weighted resources fail. If not specified, a default weight of 1 is used.

Examples

The following example specifies three resource in the result group SMS-WEIGHTED. The three resources are identified by point code 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
```

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 multi-layer information.

pc-range

To specify the a point code range entry in a pc table, use the **pc-range** command in gateway screening table configuration mode.

pc-range *pc-start* [*pc-end*] **result** {**action-set** *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	Specifies that the result will be to screen by action set.
<i>action-set-name</i>	Action set name. Valid names may not exceed 12 alpha numeric characters.
table	Specifies that the result will be to screen by table.
<i>table-name</i>	Table name. Valid names may not exceed 12 alpha numeric characters.

Defaults

No default behavior or values.

Command Modes

Gateway screening table configuration

Command History

Release	Modification
12.2(25)SW4	This command was introduced.

Usage Guidelines

The **pc-range** command is valid for the following table types: aff-dest, dpc, opc.
Wildcard can be used. Refer to [Table 13 on page 205](#).

Examples

The following example specifies 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 the a point code range entry in a pc-ssn table, use the **pc-range ssn** command in gateway screening table configuration mode.

```
pc-range ssn 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.
result	Specifies the next step.
action	Specifies that the result will be to screen by action set.
<i>action-set-name</i>	Action set name. Valid names may not exceed 12 alpha numeric characters.
table	Specifies that the result will be to screen by table.
<i>table-name</i>	Table name. Valid names may not exceed 12 alpha numeric characters.

Defaults No default behavior or values.

Command Modes Gateway screening table configuration

Command History	Release	Modification
	12.2(25)SW4	This command was introduced.

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 specifies 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 will be sent. The range is 500 through 30000 milliseconds. The default is 5000 milliseconds. Applies to M2PA RFC links only.
t01 msec		Alignment ready timer. The range is 500 through 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 through 150000 milliseconds. The default is 60000 milliseconds. Applies to M2PA RFC links only.
t3		Aligned timer. The range is 500 through 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 will be sent. The range is 100 through 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 will be sent. The range is 500 through 60000 milliseconds. The default is 8000 milliseconds. Applies to M2PA RFC links only.
t06		Remote congestion timer. The range is 500 through 12000 milliseconds. The default is 4000 milliseconds.
t7		Excessive delay of acknowledgment timer. The range is 0 through 30000 milliseconds. The default is 0 milliseconds. Applies to M2PA RFC links only.

Defaults See Syntax Description.

Command Modes CS7 link submode

Command History	Release	Modification
	12.2(1)MB	This command was introduced.
	12.2(25)SW3	An additional t01 (Alignment Ready) timer default value of 45000 milliseconds was added for a link that is defined as an M2PA RFC link. New timers were added with the keywords t2 , t3 , t4e , t4n , t06 , t7 and lssu .

Examples

The following example sets 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 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 will be sent. The range is 500 through 30000 milliseconds. The default is 5000 milliseconds. Applies to M2PA RFC links only.
t01 msec		Alignment ready timer. The range is 500 through 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 through 150000 milliseconds. The default is 60000 milliseconds. Applies to M2PA RFC links only.
t3		Aligned timer. The range is 500 through 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 will be sent. The range is 100 through 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 will be sent. The range is 500 through 60000 milliseconds. The default is 8000 milliseconds. Applies to M2PA RFC links only.
t06		Remote congestion timer. The range is 500 through 12000 milliseconds. The default is 4000 milliseconds.
t7		Excessive delay of acknowledgment timer. The range is 0 through 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(1)MB	This command was introduced.
	12.2(25)SW3	An additional t01 (Alignment Ready) timer default value of 45000 milliseconds was added for a link that is defined as an M2PA RFC link. New timers were added with the keywords t2 , t3 , t4e , t4n , t06 , t7 and lssu .

Examples

The following example defines a profile named m2parfc, specifies that the profile supports M2PA RFC, configures **peer-timer** settings and **hold-transport** settings in the profile, then applies the m2parfc profile to all the links in linkset named to_nyc:

```
cs7 profile m2parfc
  m2pa
    peer-timer t1 15000
    peer-timer t2 9000
  .
  .
  .
cs7 linkset to_nyc
  profile timers
```

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 the command.

pid *protocol-id*

no pid *protocol-id*

Syntax Description

<i>protocol-id</i>	An integer in the range of 0 to 255.
--------------------	--------------------------------------

Defaults

No default behavior or value.

Command Modes

CS7 mlr ruleset-rule configuration

Command History

Release	Modification
12.2(4)MB	This command was introduced.

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 specifies a protocol identifier (PID) value:

```
cs7 mlr ruleset ruleset1
rule 10 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 multi-layer ruleset table and enables CS7 MLR ruleset-rule configuration mode.

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</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. Can specify 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. 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 through 15. Default is 0.
stop	Stop the ping.
round-robin	Perform the ping in round-robin order.
<i>point-code</i>	The point code.
<i>host</i>	The hostname.

Defaults The primary point code is the default originating point code.

Command Modes EXEC

Command History	Release	Modification
	12.2(1)MB	This command was introduced.
	12.2(13)MB	The -opc flag was added.

Examples

The following example starts 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 command starts 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 command stops a ping to point code 10.44.156:

```
ping cs7 stop 10.44.156
```

Related Commands

Command	Description
cs7 host	
show cs7 linkset	Displays linkset information.
show cs7 ping	Displays output from a ping test.

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** version of the command.

plan-capacity-rcvd *bps*

no plan-capacity-rcvd *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(4)MB4	This command was introduced.

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. It is not necessary or recommended 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, there is not a direct way of determining the expected amount of traffic. The design of the IP cloud must consider the traffic from all SS7 links and allocate resources accordingly. In order to monitor link utilization on these types of links, a planned capacity must be specified.

Examples	The following example sets 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.
	threshold-receive	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 the 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(4)MB4	This command was introduced.
Usage Guidelines	<p>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. It is not necessary or recommended 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.</p> <p>In the case of SCTP/IP based links, there is not a direct way of determining the expected amount of traffic. The design of the IP cloud must consider the traffic from all SS7 links and allocate resources accordingly. In order to monitor link utilization on these types of links, a planned capacity must be specified.</p>	
Examples	<p>The following example sets the send planning capacity on link 0 to 56000 bps:</p> <pre>cs7 linkset michael 10.1.1 link 0 sctp 172.18.44.147 7000 7000 plan-capacity-send 56000</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.
	threshold-receive	Specifies the receive threshold for a link.
	threshold-send	Specifies the send threshold for a link.

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 *tablename*

no post-gtt-address-conversion *tablename*

Syntax Description	<i>tablename</i> Name of an already-defined address conversion table.
---------------------------	---

Defaults	No default behavior or values
-----------------	-------------------------------

Command Modes	CS7 GTT selector submode
----------------------	--------------------------

Command History	Release	Modification
	12.2(4)MB2	This command was introduced.

Examples	The following example specifies a conversion table named table1.
	<pre>cs7 gtt selector name tt np nai post-gtt-address-conversion table1</pre>

Related Commands	Command	Description
	cs7 gtt selector	Creates a GTT selector.
	pre-gtt-address-conversion	Specifies the global title address conversion table to apply prior to performing local global title translation.

pre-gtt-address-conversion

To specify the global title address conversion table to apply prior to 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 *tablename*

no pre-gtt-address-conversion *tablename*

Syntax Description	<i>tablename</i> Name of an already-defined prefix-conversion table.						
Defaults	No default behavior or values						
Command Modes	CS7 GTT selector submode						
Command History	<table> <tr> <th>Release</th><th>Modification</th></tr> <tr> <td>12.2(4)MB2</td><td>This command was introduced.</td></tr> </table>	Release	Modification	12.2(4)MB2	This command was introduced.		
Release	Modification						
12.2(4)MB2	This command was introduced.						
Examples	<p>The following example specifies a conversion table named table2.</p> <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 a MLR is selected in this instance, use **preserve-opc** command in cs7 mlr option configuration mode. To remove the specification, use the **no** form of this command. Refer to the **preserve-opc (cs7 mlr ruleset)** command for details.

preserve-opc

no preserve-opc

Syntax Description

This command has no arguments or keywords.

Defaults

The **preserve-opc** command is disabled. The OPC will be modified by MLR to the ITP local PC.

Command Modes

CS7 MLR ruleset configuration

Command History

Release	Modification
12.2(21)SW	This command was introduced.

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 simply routes the packet without modifying the original OPC in any way. The SCCP Calling Party Address is also not modified.

Examples

The second line in the following example specifies 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 the CS7 MLR options configuration mode.

preserve-opc (cs7 mlr options)

To preserve the original originating point code (OPC) when a MLR is selected in this instance, use **preserve-opc** command in cs7 mlr option 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 **preserve-opc** command is disabled. The OPC will be modified by MLR to the ITP local PC.

Command Modes

CS7 mlr options configuration

Command History

Release	Modification
12.2(18)IXC	This command was introduced.

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 simply routes the packet without modifying the original OPC in any way. The SCCP Calling Party Address is also not modified. This preserve-opc command applied to all messages which are MLR routed.

Examples

```
cs7 mlr options
preserve-opc
```

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

Enabled

Defaults

No default behavior or values

Command Modes

CS7 linkset

Command History

Release	Modification
12.2(4)MB12	This command was introduced.

Usage Guidelines

A preventive transfer-prohibited message is normally sent to an adjacent node to indicate that the adjacent node will be used for signalling traffic to a concerned destination. The purpose of the message is to avoid a routing loop by preventing the adjacent node from sending signalling traffic to a node that will route the signalling 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 disables 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 through 2999.
---------------------------	--

Defaults

No default behavior or values

Command Modes

CS7 QoS

Command History

Release	Modification
12.2(4)MB	This command was introduced.

Usage Guidelines

The **qos-access-group** command allows you to assign an ITP access list to a QoS class definition.

Examples

The following example assigns 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 the command.

qos-class *class*

no qos-class *class*

Syntax Description	<i>class</i>	QoS Class ID. Valid range is 1 through 7.
---------------------------	--------------	---

Defaults	No default behavior or values
-----------------	-------------------------------

Command Modes	CS7 AS submode
----------------------	----------------

Command History	Release	Modification
	12.2(4)MB5	This command was introduced.

Usage Guidelines	The QoS class must be defined before the class is assigned.
	Once 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 configures a QoS class 4 for AS1:
-----------------	---

```
cs7 as as1 m3ua
  qos-class 4
```

Related Commands	Command	Description
	cs7 as	Defines an Application Server.

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 the command.

qos-class *class* [*instance-number*]

no qos-class *class* [*instance-number*]

Syntax Description

<i>class</i>	QoS Class ID in the range 0 through 7.
<i>instance-number</i>	Required if multiple instances is configured. The valid range is 0 through 7. The default instance is instance 0.

Defaults

No default behavior or values

Command Modes

CS7 ASP submode

Command History

Release	Modification
12.2(4)MB5	This command was introduced.

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 configures a 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 and enables CS7 ASP submode.
cs7 qos class	Defines a QoS class.
show cs7 qos	Displays QoS class.

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 the command.

qos-class *class*

no qos-class *class*

Syntax Description

<i>class</i>	QoS Class ID. Valid range is 0 through 7.
--------------	---

Defaults

No default behavior or values

Command Modes

CS7 GTT selector submode

Command History

Release	Modification
12.2(4)MB	This command was introduced.

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 configures a QoS class of 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.

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 the command.

qos-class *class*

no qos-class *class*

Syntax Description

<i>class</i>	QoS Class ID. Valid range is 1 through 7.
--------------	---

Defaults

No default behavior or values

Command Modes

CS7 link submode

Command History

Release	Modification
12.2(4)MB	This command was introduced.

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 configures a 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.

qos-class (cs7 m2pa profile)

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 the command.

qos-class *class*

no qos-class *class*

Syntax Description	<i>class</i>	QoS Class ID. Valid range is 1 through 7.
--------------------	--------------	---

Defaults	No default behavior or values
----------	-------------------------------

Command Modes	CS7 m2pa profile configuration
---------------	--------------------------------

Command History	Release	Modification
	12.2(25)SW3	This command was introduced.

Usage Guidelines	<p>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.</p> <p>The QoS class must be defined before the class is assigned to a peer link.</p>
------------------	--

Examples	<p>The following example defines a profile named m2parfc, specifies that the profile supports M2PA RFC, specifies the qos-class parameter in the profile, then applies the m2parfc profile to all the links in linkset named to_nyc:</p>
----------	---

```
cs7 profile m2parfc
 m2pa
  qos-class 4
.
.
.
cs7 linkset to_nyc
 profile m2parfc
```

Related Commands	Command	Description
	m2pa	Specifies M2PA parameters in a CS7 profile.

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 the command.

qos-class *class* [*instance-number*]

no qos-class *class* [*instance-number*]

Syntax Description

<i>class</i>	QoS Class ID. Valid range is 1 through 7.
<i>instance-number</i>	Required if multiple instances is configured. The valid range is 0 through 7. The default instance is instance 0.

Defaults

No default behavior or values

Command Modes

CS7 Mated-SG submode

Command History

Release	Modification
12.2(4)MB5	This command was introduced.

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 configures a 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.

qos-ip-dscp

To define the Differential Services Code Point (DSCP) setting for a QoS class, use the **qos-ip-dscp** CS7 QoS submode configuration 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

ip-tos

DSCP setting for the IP TOS byte, in decimal notation. Valid range is 0 through 63. The default is zero.

Defaults

The IP TOS default is 0.

Command Modes

CS7 QoS submode

Command History

Release	Modification
---------	--------------

12.2(4)MB	This command was introduced.
-----------	------------------------------

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 sets 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 **ip-precedence-qos** CS7 QoS submode configuration 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 through 7. The default is zero.
---------------------------	---------------	--

Defaults	The IP TOS default is 0.
-----------------	--------------------------

Command Modes	CS7 QoS submode
----------------------	-----------------

Command History	Release	Modification
	12.2(4)MB	This command was introduced.

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 CS7 link submode command overrides the qos-ip-precedence tos settings assigned through a QoS class.
-------------------------	---

Examples	The following example sets the IP type of service to 3 for QoS class 1:
-----------------	---

```
cs7 qos class 1
  qos-ip-precedence 3
```

Related Commands	Command	Description
	cs7 linkset	Specifies a linkset.
	ip-precedence (CS7 Link)	Configure IP precedence TOS setting
	link (CS7 linkset)	Configures a link.

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 through 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(1)MB	This command was introduced.


Usage Guidelines	<p>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:</p>
-------------------------	---

$$\text{capacity (bits)} = \text{bandwidth (bits/sec)} \times \text{round-trip-time(sec)}$$

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.

Examples	The following example sets the receive-window size to 6000 bytes:
-----------------	---

```
cs7 local-peer 7000
receive-window 6000
```

 receive-window (CS7 local peer)**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 through 20971520 bytes. The default receive-window size is 64000 bytes.
--------------------	-------------	---

Defaults	64000 bytes.
----------	--------------

Command Modes	CS7 M3UA submode
---------------	------------------

Command History	Release	Modification
	12.2(4)MB5	This command was introduced.

Examples	The following example sets the receive-window size to 6000 bytes: <pre>cs7 m3ua 2905 offload 2 0 local-ip 4.4.4.4 receive-window 6000</pre>
----------	--

Related Commands	Command	Description
	cs7 m3ua	Specifies the local port number for M3UA and enters CS7 M3UA submode.

receive-window (CS7 SGMP)

To configure the local receive window size for the local port, use the **receive-window** CS7 SGMP 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 through 20971520 bytes. The default receive-window size is 64000 bytes.
---------------------------	-------------	---

Defaults	64000 bytes.
-----------------	--------------

Command Modes	CS7 SGMP submode
----------------------	------------------

Command History	Release	Modification
	12.2(4)MB5	This command was introduced.

Examples	The following example sets the receive-window size to 6000 bytes:
	<pre>cs7 sgmp 5000 local-ip 4.4.4.4 receive-window 6000</pre>

Related Commands	Command	Description
	cs7 sgmp	Specifies the local port number for SGMP and enter CS7 SGMP 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 through 20971520 bytes. The default receive-window size is 64000 bytes.
--------------------	-------------	---

Defaults	64000 bytes.
----------	--------------

Command Modes	CS7 SUA submode
---------------	-----------------

Command History	Release	Modification
	12.2(4)MB5	This command was introduced.

Examples	<p>The following example sets the receive-window size to 6000 bytes:</p> <pre>cs7 sua 15000 offload 2 0 local-ip 4.4.4.4 receive-window 6000</pre>
----------	--

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 goes 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 through 2000 msec. The default is 2000 msec.
---------------------------	-------------	---

Defaults	2000 msec.
-----------------	------------

Command Modes	CS7 AS submode
----------------------	----------------

Command History	Release	Modification
	12.2(4)MB5	This command was introduced.

Examples	The following example sets the recovery timeout to 1000 msec:
-----------------	---

```
cs7 as BLUE m3ua
  recovery-timeout 1000
```

Related Commands	Command	Description
	cs7 as	Defines an Application Server.
	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	No default behavior or values.
----------	--------------------------------

Command Modes	CS7 ASP
---------------	---------

Command History	Release	Modification
	12.2(4)MB5	This command was introduced.

Usage Guidelines	The remote-ip CS7 ASP command allows you to 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 multi-homing, 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 4 remote IP addresses by specifying additional remote-ip commands.
------------------	--

Examples	The following example configures remote IP address 2.2.2.2 for M3UA ASP1:
----------	---

```
s7 asp ASP1 5000 5000 m3ua
  remote-ip 2.2.2.2
```

Related Commands	Command	Description
	cs7 asp	Specifies an Application Server Process and enables CS7 ASP submode.

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

No default behavior or values.

Command Modes

CS7 Mated-SG

Command History

Release	Modification
12.2(4)MB5	This command was introduced.

Usage Guidelines

The **remote-ip** CS7 Mated-SG command allows you to 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 multi-homing, 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 4 remote IP addresses by specifying additional **remote-ip** commands.

Examples

The following example configures 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 this alternate specification of the default would be /24. For ITU the alternate specification of the default would be /14.

Defaults

No default values or behavior.

Command Modes

Route-table submode configuration

Command History

Release	Modification
12.2(4)MB	This command was introduced.

Usage Guidelines

The **remove route** command is the functional equivalent of “no update.” The specified route will be deleted from the active routing table. If the configuration contained an **update route** command for the specified point code then the **update route** command line is removed from the configuration. If there was no **update route** in the configuration then a **remove route** is added to the configuration.

The **remove route** configuration will show up in the ITP configuration until a new route-table is created using the **cs7 save route-table** privileged EXEC command.

Examples

The following is an example of the remove route command:

```
remove route 1.50.2 255.255.255 linkset nyc
```

Related Commands

Command	Description
update route (route-table)	Updates a route.

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.

```
result { gt addr-string [gt-addr-type] | pc dest_pc [ssn ssn] | asname as-name | group result-group
| block [sccp-error error] | continue | route }
```

no result

Syntax Description

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>addr-string</i>	Address string of 1 to 15 hexadecimal characters. The string is not input in BCD-String format, but in normal form.
<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.
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.
<i>dest_pc</i>	DPC in variant-specific point-code format.
ssn	Specifies that the message will be routed using the subsystem number.
<i>ssn</i>	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.
<i>as-name</i>	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.

<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 <i>error</i>	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.
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.

Defaults

If not specified, the default *gt-addr-type* 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(4)MB	This command was introduced.
12.2(21)SW	The ssn keyword and argument were added.
12.2(18)IXC	The keywords block sccp-error , continue and route were added.

Usage Guidelines

The MLR result group must be defined prior to configuring the **result** command.

One result must be specified.

If **sccp-error** *error* is configured and return-on-error is set in the UDT, an UDTs will be sent back for dropped SCCP packets to the originating user with the configured error as the return cause. Currently, the user can configure block results in MLR rules, triggers and address table entries.

Examples

The following example specifies that a packet that matches the configured trigger and rule will be routed for processing to the result group SMS-WEIGHTED:

```
cs7 mlr ruleset ruleset1
 rule 10 sms-mo
   dest-sme 1234
   orig sme 60920025
   result group SMS-WEIGHTED
```

Related Commands

Command	Description
cs7 mlr result	Specifies destination resources that process traffic to be routed based on multi-layer information.
rule (cs7 mlr ruleset)	Specifies the rules for a routing trigger within a multi-layer ruleset table and enables CS7 MLR ruleset-rule configuration mode.

retransmit-cwnd-rate (CS7 ASP)

To configure the rate at which the SCTP congestion window size is reduced due to retransmission timer expirations, 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 will be 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 a SCTP fast retransmission.

Defaults

The default is 50 percent.

Command Modes

CS7 ASP submode

Command History

Release	Modification
12.2(19)SW	This command was introduced.

Usage Guidelines

The **retransmit-cwnd-rate** command allows the administrator to configure a rate at which the SCTP congestion window will be decreased due to retransmission timer expirations. The administrator can select one of two methods for setting the congestion window as a result of the retransmission timer expiration. The administrator can elect to have the congestion window set as defined in RFC 2960 (the default) or elect to have the congestion window set in the manner as for a fast-retransmission.



Note

It is extremely important to note that the behavior of the SCTP congestion control algorithms are not compliant with RFC 2960 when this parameter is changed to values other than the default. This parameter should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples

The following example sets 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 expirations, 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 will be 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 a SCTP fast retransmission.

Defaults

The default is 50 percent.

Command Modes

CS7 link submode

Command History

Release	Modification
12.2(19)SW	This command was introduced.

Usage Guidelines

The **retransmit-cwnd-rate** command allows the administrator to configure a rate at which the SCTP congestion window will be decreased due to retransmission timer expirations. The administrator can select one of two methods for setting the congestion window as a result of the retransmission timer expiration. The administrator can elect to have the congestion window set as defined in RFC 2960 (the default) or elect to have the congestion window set in the manner as for a fast-retransmission.



Note

It is extremely important to note that the behavior of the SCTP congestion control algorithms are not compliant with RFC 2960 when this parameter is changed to values other than the default. This parameter should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples

The following example sets 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 expirations, 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 will be 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 a SCTP fast retransmission.

Defaults

The default is 50 percent.

Command Modes

CS7 m2pa profile configuration

Command History

Release	Modification
12.2(25)SW3	This command was introduced.

Usage Guidelines

The **retransmit-cwnd-rate** command allows the administrator to configure a rate at which the SCTP congestion window will be decreased due to retransmission timer expirations. The administrator can select one of two methods for setting the congestion window as a result of the retransmission timer expiration. The administrator can elect to have the congestion window set as defined in RFC 2960 (the default) or elect to have the congestion window set in the manner as for a fast-retransmission.



Note

It is extremely important to note that the behavior of the SCTP congestion control algorithms are not compliant with RFC 2960 when this parameter is changed to values other than the default. This parameter should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples

The following example defines a profile named m2parfc, specifies that the profile supports M2PA RFC, specifies the **retransmit-cwnd-rate** parameter in the profile, then applies the m2parfc profile to all the links in 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 expirations, 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 will be 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 a SCTP fast retransmission.

Defaults

The default is 50 percent.

Command Modes

CS7 M3UA submode

Command History

Release	Modification
12.2(19)SW	This command was introduced.

Usage Guidelines

The **retransmit-cwnd-rate** command allows the administrator to configure a rate at which the SCTP congestion window will be decreased due to retransmission timer expirations. The administrator can select one of two methods for setting the congestion window as a result of the retransmission timer expiration. The administrator can elect to have the congestion window set as defined in RFC 2960 (the default) or elect to have the congestion window set in the manner as for a fast-retransmission.



Note

It is extremely important to note that the behavior of the SCTP congestion control algorithms are not compliant with RFC 2960 when this parameter is changed to values other than the default. This parameter should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples

The following example sets the rate for reducing the congestion window to 70 percent due to a retransmission timer expiration.

```
cs7 m3ua 2905 offload 2 0
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 expirations, 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 will be 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 a SCTP fast retransmission.

Defaults

The default is 50 percent.

Command Modes

CS7 Mated-SG submode

Command History

Release	Modification
12.2(19)SW	This command was introduced.

Usage Guidelines

The **retransmit-cwnd-rate** command allows the administrator to configure a rate at which the SCTP congestion window will be decreased due to retransmission timer expirations. The administrator can select one of two methods for setting the congestion window as a result of the retransmission timer expiration. The administrator can elect to have the congestion window set as defined in RFC 2960 (the default) or elect to have the congestion window set in the manner as for a fast-retransmission.



Note

It is extremely important to note that the behavior of the SCTP congestion control algorithms are not compliant with RFC 2960 when this parameter is changed to values other than the default. This parameter should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples

The following example sets 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 SGMP)

To configure the rate at which the SCTP congestion window size is reduced due to retransmission timer expirations, use the **retransmit-cwnd-rate** CS7 SGMP 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 will be 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 a SCTP fast retransmission.

Defaults

The default is 50 percent.

Command Modes

CS7 SGMP submode

Command History

Release	Modification
12.2(19)SW	This command was introduced.

Usage Guidelines

The **retransmit-cwnd-rate** command allows the administrator to configure a rate at which the SCTP congestion window will be decreased due to retransmission timer expirations. The administrator can select one of two methods for setting the congestion window as a result of the retransmission timer expiration. The administrator can elect to have the congestion window set as defined in RFC 2960 (the default) or elect to have the congestion window set in the manner as for a fast-retransmission.



Note

It is extremely important to note that the behavior of the SCTP congestion control algorithms are not compliant with RFC 2960 when this parameter is changed to values other than the default. This parameter should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples

The following example sets the rate for reducing the congestion window to 70 percent due to a retransmission timer expiration.

```
cs7 sgm 5000
local-ip 4.4.4.4

retransmit-cwnd-rate 70
```

Related Commands

Command	Description
retransmit-timeout (CS7 SGMP)	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 expirations, 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 will be 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 a SCTP fast retransmission.

Defaults

The default is 50 percent.

Command Modes

CS7 SUA submode

Command History

Release	Modification
12.2(19)SW	This command was introduced.

Usage Guidelines

The **retransmit-cwnd-rate** command allows the administrator to configure a rate at which the SCTP congestion window will be decreased due to retransmission timer expirations. The administrator can select one of two methods for setting the congestion window as a result of the retransmission timer expiration. The administrator can elect to have the congestion window set as defined in RFC 2960 (the default) or elect to have the congestion window set in the manner as for a fast-retransmission.



Note

It is extremely important to note that the behavior of the SCTP congestion control algorithms are not compliant with RFC 2960 when this parameter is changed to values other than the default. This parameter should not be changed without a thorough understanding of SCTP congestion control algorithms.

Examples

The following example sets the rate for reducing the congestion window to 70 percent due to a retransmission timer expiration.

```
cs7 sua 15000 offload 2 0
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 300 through 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 300 through 60000 milliseconds. The default is 1000 milliseconds

Defaults

The default is the value specified under the local port instance.

Command Modes

CS7 ASP submode

Command History

Release	Modification
12.2(4)MB5	This command was introduced.

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. 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.

Examples

The following example sets the minimum values 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 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 *min-msec max-msec*

no retransmit-timeout

Syntax Description

<i>min-msec</i>	Retransmission timeout minimum value in milliseconds. Range is 100 through 60000 milliseconds. The default is 1000 milliseconds.
<i>max-msec</i>	Retransmission timeout maximum value in milliseconds. Range is 100 through 60000 milliseconds. The default is 1000 milliseconds.

Defaults

Default *min-sec* value is 1000 milliseconds.

Default *max-sec* value is 1000 milliseconds.

Command Modes

CS7 link submode

Command History

Release	Modification
12.2(1)MB	This command was introduced.

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. 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.

Examples

The following example sets the minimum and maximum values of the retransmit timeout to 300 milliseconds (minimum) and 30000 milliseconds (maximum):

```
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** CS7 link submode command. To disable the timeout value, use the **no** form of this command.

retransmit-timeout *min-msec max-msec*

no retransmit-timeout

Syntax Description

<i>min-msec</i>	Retransmission timeout minimum value in milliseconds. Range is 100 through 60000 milliseconds. The default is 1000 milliseconds.
<i>max-msec</i>	Retransmission timeout maximum value in milliseconds. Range is 100 through 60000 milliseconds. The default is 1000 milliseconds.

Defaults

Default *min-sec* value is 1000 milliseconds.

Default *max-sec* value is 1000 milliseconds.

Command Modes

CS7 m2pa profile configuration

Command History

Release	Modification
12.2(25)SW3	This command was introduced.

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. 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.

Examples

The following example defines a profile named m2parfc, specifies that the profile supports M2PA RFC, specifies the **retransmit-timeout** parameter in the profile, then applies the m2parfc profile to all the links in 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*

no retransmit-timeout

Syntax Description	<i>rto-min</i>	Retransmission timeout minimum value in milliseconds. Range is 300 through 60000 milliseconds. The default is 1000 milliseconds.
	<i>rto-max</i>	Retransmission timeout maximum value in milliseconds. Range is 300 through 60000 milliseconds. The default is 1000 milliseconds

Defaults	1000 milliseconds.
-----------------	--------------------

Command Modes	CS7 M3UA submode
----------------------	------------------

Command History	Release	Modification
	12.2(4)MB5	This command was introduced.

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. 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.

Examples

The following example sets the minimum value of the retransmit timeout to 300 milliseconds and the maximum value to 3000 milliseconds:

```
cs7 m3ua 2905 offload 2 0
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*

no retransmit-timeout

Syntax Description

<i>rto-min</i>	Retransmission timeout minimum value in milliseconds. Range is 300 through 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 300 through 60000 milliseconds. The default is 1000 milliseconds

Defaults

The default is the value specified under the local port instance.

Command Modes

CS7 Mated-SG submode

Command History

Release	Modification
12.2(4)MB5	This command was introduced.

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. 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.

Examples

The following example sets 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 SGMP)

To configure the minimum retransmission timeout value used when a new SCTP association is started, use the **retransmit-timeout** CS7 SGMP submode command. To disable the timeout value, use the **no** form of this command.

retransmit-timeout *rto-min*

no retransmit-timeout

Syntax Description	<i>rto-min</i>	Retransmission timeout minimum value in milliseconds. Range is 300 through 60000 milliseconds. The default is 1000 milliseconds.
	<i>rto-max</i>	Retransmission timeout maximum value in milliseconds. Range is 300 through 60000 milliseconds. The default is 1000 milliseconds

Defaults	1000 milliseconds.
-----------------	--------------------

Command Modes	CS7 SGMP submode
----------------------	------------------

Command History	Release	Modification
	12.2(4)MB5	This command was introduced.

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. 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.

Examples

The following example sets the minimum retransmit timeout value to 300 milliseconds and the maximum value to 3000 milliseconds:

```
cs7 sgmp 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*

no retransmit-timeout

Syntax Description	<i>rto-min</i>	Retransmission timeout minimum value in milliseconds. Range is 300 through 60000 milliseconds. The default is 1000 milliseconds.
	<i>rto-max</i>	Retransmission timeout maximum value in milliseconds. Range is 300 through 60000 milliseconds. The default is 1000 milliseconds

Defaults	1000 milliseconds.
-----------------	--------------------

Command Modes	CS7 SUA submode
----------------------	-----------------

Command History	Release	Modification
	12.2(4)MB5	This command was introduced.

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. 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.

Examples

The following example sets the minimum value of the retransmit timeout to 300 milliseconds and the maximum value to 3000 milliseconds:

```
cs7 sua 15000 offload 2 0
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

no rotate-sls

Syntax Description

This command has no arguments or keywords.

Defaults

SLS rotation is enabled by default for ANSI linksets.

Command Modes

CS7 linkset submode

Command History

Release	Modification
12.2(1)MB	This command was introduced.

Usage Guidelines

This command is only valid when the variant is ANSI.

ANSI specifications state that SLS rotation should not be performed on C linksets. Use the no form of the command to disable SLS rotation on C linksets.

Examples

The following example disables SLS rotation:

```
no rotate-sls
```

Related Commands

Command	Description
cs7 linkset	Configures a linkset.

routing-key (CS7 AS)

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 is extremely important to ensure that traffic is routed correctly. Routing key combinations vary for M3UA and SUA.

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 {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 {isup | sccp | tup}] [[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. The destination point code indicates 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 of this command reference entry.
opc		Originating point code. The originating point code parameter 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. The point code mask allows the user to specify a range of originating point codes by indicating the number of significant bits.
si		Service indicator. The user may specify a service indicator of either isup or sccp. (This parameter applies to M3UA ASs only. SUA ASs imply an sccp service indicator.)
isup		Service indicator is isup.
sccp		Service indicator is sccp.
tup		Service indicator is tup.
cic		Circuit identification code. (This parameter applies to M3UA ASs only. Configuring CIC implies an isup service indicator.)
<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 ASs only. Configuring SSN implies a sccp service indicator.)
<i>ssn</i>	Subsystem number value.

Defaults

No default values or behavior.

Command Modes

CS7 AS submode

Command History

Release	Modification
12.2(4)MB5	This command was introduced.

Usage Guidelines

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. Below is a list of 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 ASs, the routing key has the following parameters:

```
routing-key rcontext { gtt [gtt-selector-name [gtt-gta]] | dpc [opc pc pc-mask] [si {isup | sccp}}
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 ASs, the routing key has the following parameters. SUA only supports **si sccp**.

```
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

Special care must be taken when planning the assignment of point codes to ASs. The ITP SG feature allows point code assignment to ASs 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 ASs or groups of ASs serviced by the SG may share a given point code. Any group of ASs 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 affect 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 will vary. If a trap has been enabled for unallocated messages, the DPC, OPC, and SIO of an unallocated MSU will be reported to the designated management entity. If the unallocated MSU trap has not been enabled, the MSU will be counted and dropped.

To prevent this from happening 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 would catch 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 would be sent to the isupbucket ASP. It should be noted that if the isupbucket ASP is not active, the MSU is dropped with the appropriate warning.

Examples

The following are examples of 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 and enters CS7 AS submode.

rule (cs7 mlr ruleset)

To specify the rules for a routing trigger within a multi-layer 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}
```

```
[no] rule order {{gsm-map | ansi-41} operation-name [default] | all-operations}
```

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 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 tables below.
default		(Optional) 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, since there can be only one rule configured for each new operation.
all-operations		Identifies 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.

Defaults	None
-----------------	------

Command Modes	CS7 mlr ruleset configuration
----------------------	-------------------------------

Command History	Release	Modification
	12.2(4)MB	This command was introduced.
	12.2(21)SW	The alertsc , smdpp , smsreq , and smsnot operations were added.
	12.2(18)IXB	MAP operation support was extended to include all GSM-MAP (3GPP TS 29.002 version 5.9.0 Release 5) operations in MLR rules. The protocol keywords gsm-map and ansi-41 were added. The valid operation-name specifications are presented in the CLI depending on the specified protocol and are listed in this command reference entry in Table 30 , Table 31 , and Table 32 .

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 the MLR Ruleset Rule configuration mode.
-------------------------	--

Table 30 and Table 31 list GSM-MAP and GSM-MAP Version 1 operation names mapped to ITP operations names. Table 32 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 31 *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

Table 31 *GSM-MAP Operation Name Mapping to ITP CLI Operation Name (continued)*

Operation Name in GSM-MAP Specification	ITP CLI Operation Name	Opcode Value
processGroupCallSignalling	processGrpCallSig	41
processUnstructuredSS-Request	processUnstructSSReq	59
provideRoamingNumber	provideRoamNumber	4
provideSIWFSSNumber	provideSIWFSSNumber	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
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		

Table 31 *GSM-MAP Operation Name Mapping to ITP CLI Operation Name (continued)*

Operation Name in GSM-MAP Specification	ITP CLI Operation Name	Opcode Value
updateGprsLocation	updGprsLoc	23
updateLocation	updLoc	2
NoteMM-Event	noteMMEvent	89

Table 32 *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

Table 32 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
TraceSubscriberActivity	traceSubAct	52
updateLocationArea	updateLocArea	1

Table 32 lists the parameters that are valid based on the specified **rule** operation.

Table 33 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
allow-multi-message-dialogue 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 will be used in the default cases and MAP operation will be matched with the rules in the ascending order. If a rule matches, the result of the rule will be 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 (cs7 mlr ruleset)

```

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
  allow-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
    allow-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
cs7 mlr ruleset	Specifies sets of rules that will be used to process traffic-matching triggers defined in a multi-layer routing table.
dest-port (cs7 mlr ruleset rule)	Specifies the application destination port number.

Command	Description
dest-sme (cs7 mlr ruleset rule)	Specifies the address of the destination Short Message Entity (SME) within an SMS operation.
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 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 which are MLR routed.
multi-message-dialogue	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	Configures origin IMSI.
orig-imsi-table	Configures an MLR table of origin IMSI addresses
orig-sme (cs7 mlr ruleset rule)	Specifies the address of the origin Short Message Entity.
orig-sme-table	Configures MLR table of origin SME addresses.
pid (cs7 mlr ruleset rule)	Configure the protocol identifier.
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.

rule (cs7 mlr ruleset)



ITP Command Set: S - Z

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 publications.

- [sccp-msg, page 851](#)
- [set, page 853](#)
- [show cs7, page 855](#)
- [show cs7 access-lists, page 857](#)
- [show cs7 accounting, page 858](#)
- [show cs7 as, page 861](#)
- [show cs7 asp, page 864](#)
- [show cs7 gtt address-conversion, page 869](#)
- [show cs7 gtt application-group, page 870](#)
- [show cs7 gtt concern-pclist, page 871](#)
- [show cs7 gtt config, page 872](#)
- [show cs7 gtt consistency, page 874](#)
- [show cs7 gtt gta, page 876](#)
- [show cs7 gtt map, page 878](#)
- [show cs7 gtt measurements, page 880](#)
- [show cs7 gtt selector, page 883](#)
- [show cs7 gws action-set, page 884](#)
- [show cs7 gws as, page 886](#)
- [show cs7 gws linkset, page 888](#)
- [show cs7 gws table, page 890](#)
- [show cs7 linkset, page 893](#)
- [show cs7 log, page 899](#)
- [show cs7 m2pa, page 901](#)
- [show cs7 m3ua, page 909](#)
- [show cs7 mated-sg, page 911](#)
- [show cs7 mlr address-table, page 913](#)

- [show cs7 mlr dest-sme-binding, page 914](#)
- [show cs7 mlr modify-profile, page 915](#)
- [show cs7 mlr result, page 916](#)
- [show cs7 mlr ruleset, page 917](#)
- [show cs7 mlr statistics, page 920](#)
- [show cs7 mlr table, page 927](#)
- [show cs7 mtp2, page 930](#)
- [show cs7 mtp3 error, page 938](#)
- [show cs7 mtp3 event-history, page 942](#)
- [show cs7 mtp3 timers, page 943](#)
- [show cs7 nso, page 944](#)
- [show cs7 offload mtp3, page 946](#)
- [show cs7 pc-conversion, page 948](#)
- [show cs7 ping, page 949](#)
- [show cs7 point-codes, page 950](#)
- [show cs7 qos, page 952](#)
- [show cs7 route, page 954](#)
- [show cs7 sccp gti-conversion, page 959](#)
- [show cs7 sccp instance-conversion, page 961](#)
- [show cs7 sccp ssn-conversion, page 962](#)
- [show cs7 sctp address-table, page 963](#)
- [show cs7 sctp port-map, page 964](#)
- [show cs7 sgmp, page 965](#)
- [show cs7 sua, page 966](#)
- [show cs7 tcap, page 968](#)
- [show cs7 version, page 969](#)
- [show cs7 virtual linkset, page 970](#)
- [show hosts, page 973](#)
- [show ip sctp, page 975](#)
- [show redundancy states, page 982](#)
- [show sscf-nni, page 984](#)
- [show sscop, page 986](#)
- [show tech-support, page 989](#)
- [shutdown \(cs7 as\), page 991](#)
- [shutdown \(cs7 asp\), page 992](#)
- [shutdown \(cs7 link\), page 993](#)
- [shutdown \(cs7 linkset\), page 994](#)
- [shutdown \(cs7 m3ua\), page 996](#)

- [shutdown \(cs7 mated-sg\), page 997](#)
- [shutdown \(cs7 sgmp\), page 998](#)
- [shutdown \(cs7 sua\), page 999](#)
- [si, page 1000](#)
- [sls-shift, page 1003](#)
- [snmp-server enable traps bits-clock, page 1004](#)
- [snmp-server enable traps cs7, page 1005](#)
- [snmp-server enable traps sctp, page 1008](#)
- [sscf-nni, page 1009](#)
- [sscop, page 1011](#)
- [teleservice, page 1013](#)
- [threshold-receive, page 1014](#)
- [threshold-send, page 1015](#)
- [timer \(cs7 hs-mtp2 profile\), page 1016](#)
- [timer \(cs7 linkset\), page 1018](#)
- [timer \(cs7 profile\), page 1021](#)
- [traffic-mode, page 1023](#)
- [trigger cdpa \(cs7 mlr table\), page 1025](#)
- [trigger cgpa \(cs7 mlr table\), page 1030](#)
- [trigger default, page 1033](#)
- [trigger mtp3, page 1035](#)
- [ttmap, page 1037](#)
- [tt-range, page 1038](#)
- [tx-queue-depth \(cs7 asp\), page 1040](#)
- [tx-queue-depth \(cs7 hs-mtp2 profile\), page 1041](#)
- [tx-queue-depth \(cs7 link\), page 1042](#)
- [tx-queue-depth \(cs7 m2pa profile\), page 1044](#)
- [tx-queue-depth \(cs7 m3ua\), page 1046](#)
- [tx-queue-depth \(cs7 mated-sg\), page 1047](#)
- [tx-queue-depth \(cs7 profile\), page 1048](#)
- [tx-queue-depth \(cs7 sgmp\), page 1049](#)
- [tx-queue-depth \(cs7 sua\), page 1050](#)
- [unordered-priority \(cs7 m3ua\), page 1051](#)
- [unordered-priority \(cs7 sgmp\), page 1052](#)
- [unordered-priority \(cs7 sua\), page 1053](#)
- [unrouteable-accounting, page 1054](#)
- [update \(cs7 gtt address conversion\), page 1055](#)
- [update \(cs7 sccp gti conversion\), page 1056](#)

- [update route \(route-table\), page 1058](#)
- [variant, page 1060](#)
- [variant jt1, page 1061](#)

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-set** *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 34 .
	result	Specifies the next step.
	action	Specifies that the result will be to screen by action set.
	<i>action-set-name</i>	Action set name. Valid names may not exceed 12 alpha numeric characters.
	table	Specifies that the result will be to screen by table.
	<i>table-name</i>	Table name. Valid names may not exceed 12 alpha numeric characters.

Command Default No default behavior or values.

Command Modes CS7 GWs table configuration

Command History	Release	Modification
	12.2(25)SW4	This command was introduced.

Usage Guidelines [Table 34](#) lists valid SCCP message type.

Table 34 *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 specifies 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.

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** *tablename*] [**gti-conversion** *tablename*] [**message-handling** *option*]
[**national-indicator** *natl-ind*] [**ssn-conversion** *tablename*]}

no set {[**address-conversion** *tablename*] [**gti-conversion** *tablename*] [**message-handling** *option*]
[**national-indicator** *natl-ind*] [**ssn-conversion** *tablename*]}

Syntax Description	address-conversion <i>tablename</i>	Specifies an address-conversion table.
	gti-conversion <i>tablename</i>	Specifies a gti-conversion table.
	message-handling <i>option</i>	Specifies the SCCP message handling option. The values for message-handling are as follows:
	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 are valid options:
	0	international
	1	national
	no change	leave field unchanged
	ssn-conversion <i>tablename</i>	Specifies an ssn-conversion table.

Defaults No default behavior or values.

Command Modes CS7 SCCP Instance Conversion configuration

Command History	Release	Modification
	12.2(20)SW	This command was introduced.

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 will not be changed.

Examples

The following are examples of 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 ssr-conversion ssrtable
```

```
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 update 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

Command Modes EXEC

Command History	Release	Modification
	12.2(1)MB	This command was introduced.

Examples The following is sample 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
Available Linksets    0
Total Links          2

MTP3 offload         Enabled

Non Disruptive Upgrade In Progress
                      CS7 config locked out
```

Table 35 describes the fields in the display.

Table 35 *show cs7 Field Descriptions*

Field	Description
Point Code	The unique address of the node.
SS7 Variant	The SS7 variation (ANSI or ITU).
Network Indicator	The network indicator (international, national, reserved, or spare).
Network Name	The network name.
Capability Point Code	The 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 through 7. The default instance is instance 0.
	<i>access-list-number</i>	Access list number. Valid number is in range from 2700 through 2999.
	<i>access-list-name</i>	Access list name.

Command Modes	EXEC
----------------------	------

Command History	Release	Modification
	12.2(1)MB	This command was introduced.

Examples

The following is sample 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 36](#) describes the fields in the display.

Table 36 *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 are matched.
dpc	This access list is applied destination point code 4.100.0 with wildcard mask 0.0.255.

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*] [**access-violations** | **gtt**]
[**checkpoint**] [**unroutable**]

Syntax Description

<i>instance-number</i>	Specifies the instance. The valid range is 0 through 7. The default instance is instance 0.
<i>point-code</i>	(Optional) Point code filter.
<i>linkset</i>	(Optional) Linkset name.
access-violations	(Optional) Displays the CS7 access-violations database.
checkpoint	(Optional) Displays the CS7 checkpointed data.
gtt	(Optional) Displays the CS7 GTT accounting database(s).
unroutable	(Optional) Displays the CS7 unroutable MSU database.

Command Modes

EXEC

Command History

Release	Modification
12.2(1)MB	This command was introduced.
12.2(25)SW	The unroutable keyword was added.

Examples

The following is sample 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
```

Here is the output for the 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 is sample 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 zero 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 back-end 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 is sample 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 is sample 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 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 is sample output from the **show cs7 accounting** command with the **gtt** keyword:

```
ITP# show cs7 accounting gtt
```

```
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

[Table 37](#) describes the fields in the display.

Table 37 *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	Enables GTT accounting on a linkset.
clear cs7 accounting	Clears the ITP accounting databases.
show tech support	Displays a large amount of ITP configuration information that can be used for troubleshooting.

show cs7 as

To display AS and routing key information, use the **show cs7 as** privileged EXEC command.

```
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]
```

Syntax Description

<i>instance-number</i>	(Optional) Specifies the instance. The valid range is 0 through 7. The default instance is instance 0.
m3ua	(Optional) Filter on M3UA.
include-gtt	(Optional) Include ASs with GTT routing keys. (Default)
exclude-gtt	(Optional) Exclude ASs with GTT routing keys.
only-gtt	(Optional) Display only ASs with GTT routing keys.
sua	(Optional) Filter on SUA.
all	(Optional) Display all ASs. (Default)
name	(Optional) Filter on AS name.
<i>asname</i>	AS name.
operational	(Optional) Display operational ASs. (non-shut state)
active	(Optional) Display active ASs
statistics	(Optional) Display AS statistics
detail	(Optional) Display detail format.
brief	(Optional) Display brief format. (Default)

Defaults

The default display includes ASs with GTT routing keys.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)MB5	This command was introduced.

Usage Guidelines

The ASs and routing keys are displayed in the order of priority (with the first entry having the highest priority).

ASs with gtt routing keys are displayed first.

The gtt ASs are ordered alphabetically based on the AS name.

ASs with non-gtt routing keys are grouped by dpc (highest to lowest).

ASs 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 displays all M3UA ASs in detail form:

```
show cs7 as m3ua detail
```

The following command displays AS the AS named BLUE.

```
show cs7 as name blue
```

The following command displays all non-gtt ASs (default).

```
show cs7 as
```

Output examples

If multi-instances has been enabled, the instance number is displayed following the colon in the displayed point code.

The following is output from the **show cs7 as** command with the **all** keyword 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	Dpc	Routing Key Si	Opc	Ssn	Cic Min	Cic Max
kure2as	active	1	0.0.2:0	isup			0	1000
kure2as2	inactiv	2	0.0.2:4	isup			1001	2000

The following is output from the **show cs7 as** command in **detail** format:

```
ITP# show cs7 as detail
```

```
AS name: as1           State: down           Type: M3UA
RoutContxt: 1         Traffic mode: undefined
Mate AS state: unknwn Recovery tmout: 2000 ms  Recovery queue depth: 0
QOS Class: 0          Burst recovery tmout: 4000 ms
Routing Key:
Dest PC: 2.3.4:0      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
asp1          as1          down      M3UA      2906     172.18.48.68
asp2          as1          down      M3UA      2906     172.18.57.146
```

```

AS name: as2                State: down                Type: M3UA
RoutContext: 2              Traffic mode: undefined
Mate AS state: unknwn       Recovery tmout: 2000 ms  Recovery queue depth: 0
QOS Class: 0                Burst recovery tmout: 4000 ms
Routing Key:
Dest PC: 3.4.5:4            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
aspl          as2          down       M3UA      2906     172.18.48.68

```

The following is output from the **show cs7 as** command, with the **name** and **detail** keywords:

```

ITP# show cs7 as name BLUE detail
AS name: blue                State: active                Type: M3UA
Routing context: 100         Traffic mode: override
Recovery timeout: 2000 msec   Recovery queue depth: 0
Routing Key:
Dest PC: 10.3.8:0            Origin PC: n/a                Origin PC mask: n/a
SI: isup                     CIC min: n/a                  CIC max: n/a
SSN: n/a
GTT: n/a                     Selector: n/a                 GT addr: n/a
ASP Name      AS Name      State      Type      Rmt Port Remote IP Addr  Sctp Assoc
ASP1          blue         active     M3UA      10001    1.1.1.1         0
ASP2          blue         active     M3UA      10001    2.2.2.2         1

```

Options for AS State include: Shutdown/Down/Inactive/Active/Pending

Options for AS Traffic Mode include: Loadshare/Override

The following is 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.
show tech-support	Collects and displays a large amount of ITP configuration information that can be used for troubleshooting.

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 through 7. The default instance is instance 0.
all	Display all ASPs. (Default)
asname	Filter on AS name.
<i>as-name</i>	AS name.
bindings	Display ASP bindings
detail	Display detail format.
event-history	Display ASP history.
m3ua	Filter on M3UA.
name	Filter on ASP name.
<i>asp-name</i>	ASP name.
statistics	Display ASP statistics.
sua	Filter on SUA.

Defaults

If no keyword is included, the keyword **all** will take effect.

Unless the keyword **detail** is included, the output defaults to **brief** format.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)MB5	This command was introduced.

Usage Guidelines

In the brief format, an entry is displayed for each ASP/AS pair. So, the ASP name might appear multiple times if the ASP is in multiple ASs.

The AS name filter checks all ASs (regardless of gtt).

Examples

Output of the detail format

The following is output from the **show cs7 asp** command in the **detail** format and filtering on the ASP name **asp1**. This ASP asp1 (type SUA) is **down** and the association state is **closed**. It is offloaded to the linecard in slot 6.

AspVipId is an internal number used to identify the ASP.

Options for ASP state include: Down/Inactive/Active/Standby

If the ASP is down or shutdown, 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
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 VIP: 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 linecard. 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
SCTP association state: established                Association id: x0301000B
AS name: as2                                       ASP state: active
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 VIP: 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
```

show cs7 asp

```

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 is sample 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

```

The following is sample output from the **show cs7 asp** command with the **statistics** and **detail** keywords:

```

ITP# 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 Type:     0
ERR Unexpected Msg:       0
ERR Invalid Stream ID:   0
ERR ASP ID Required:      0
ERR Invalid Parm Value:   0
ERR Unexpected Parm:      0
ERR Inv Network App:      0
ERR RK Change Refused:    0
ERR No Cfg As For Asp:    0
ERR Unsupported Class:    0
ERR Traffic Mode:         0
ERR Protocol Error:       0
ERR Refused, Mgmt Block:  0
ERR Invalid ASP ID:       0
ERR Parm Field Error:     0
ERR Dest Status Unknown:  0
ERR Missing Parm:         0
ERR Inv Routing Context:  0
ERR Subsystem Status : 0

XUA Error Messages Received Stats
ERR Invalid Version:      0
ERR Unsupported Type:     0
ERR Unexpected Msg:       0
ERR Invalid Stream ID:   0
ERR ASP ID Required:      0
ERR Invalid Parm Value:   0
ERR Unexpected Parm:      0
ERR Inv Network App:      0
ERR RK Change Refused:    0
ERR No Cfg As For Asp:    0
ERR Unsupported Class:    0
ERR Traffic Mode:         0
ERR Protocol Error:       0
ERR Refused, Mgmt Block:  0
ERR Invalid ASP ID:       0
ERR Parm Field Error:     0
ERR Dest Status Unknown:  0
ERR Missing Parm:         0
ERR Inv Routing Context:  0
ERR Subsystem Status : 0

XUA Notify Messages Sent Stats
NOTIFY-AS Inactive:       0
NOTIFY-AS Pending:        0
NOTIFY-Alt ASP Active:    0
NOTIFY-AS Active:         0
NOTIFY-Insuf ASP:         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

Output of the event-history format

The **event-history** keyword displays events related to an xua asp. The following is sample 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, the log is sent from the FlexWAN to the line card at a max of 100 every 10 secs.

To clear the log use **clear cs7 asp event-history all** or **clear cs7 all** command.

If XUA offload is running only on a Cisco 7600, the timestamp refers to the time the log is received on the SUP, not to the time it occurs on the FlexWAN. Thus the log is sorted by most recent time on the SUP.

The ErrorReason field may be any of the following:

"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 and enables CS7 ASP submode.
cs7 sua	Specifies the local port number for SUA and enter CS7 SUA submode
cs7 m3ua	Specifies the local port number for M3UA and enter M3UA submode.
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*] **cs7gtt address-conversion** [*name*]

Syntax Description

<i>instance-number</i>	Specifies the instance. The valid range is 0 through 7. The default instance is instance 0.
<i>name</i>	(Optional) Displays output for a specified address conversion table.

Command Modes

privileged EXEC

Command History

Release	Modification
12.2(4)MB2	This command was introduced.

Examples

The following is sample 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 GTA 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**] [*app-grp*]

Syntax Description

<i>instance-number</i>	Specifies the instance. The valid range is 0 through 7. The default instance is instance 0.
brief	(Optional) Displays a brief form of the output.
<i>app-grp</i>	(Optional) Displays information about a specific app-grp.

Command Modes

privileged EXEC

Command History

Release	Modification
12.2(4)MB	This command was introduced.

Examples

The following is sample output from the **show cs7 gtt application-group** command:

```
ITP# show cs7 gtt application-group
Application Group Name: group1
Multiplicity           : share
Ref Count              : 1

Application Identifier  RI      Cost
-----
PC=1.1.1              SSN=10   gt      1
PC=1.1.2              SSN=10   gt      2
PC=1.1.3              SSN=10   gt      3

Application Group Name: group2
Multiplicity           : share
Ref Count              : 1

Application Identifier  RI      Cost
-----
PC=2.2.2              SSN=10   pcssn   1
PC=2.2.3              SSN=10   pcssn   2
PC=2.2.4              SSN=10   pcssn   3
```

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.

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*]

Syntax Description

<i>instance-number</i>	Specifies the instance. The valid range is 0 through 7. The default instance is instance 0.
<i>name</i>	(Optional) GTT concerned PC list name.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)MB	This command was introduced.

Examples

The following is sample 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 range is 0 through 7. The default instance is instance 0.
------------------------	---

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)MB	This command was introduced.

Usage Guidelines

This command displays the equivalent of a **show running config** command for GTT commands.

Examples

The following is sample output from the **show cs7 gtt config** command:

```
ITP# show cs7 gtt config
cs7 gtt concern-pclist list1 1.1.1
cs7 gtt concern-pclist list2 1.3.4
cs7 gtt concern-pclist list2 1.3.5
cs7 gtt concern-pclist list2 1.3.6
!
cs7 gtt map 1.1.1 10 sol
cs7 gtt map 1.1.1 200 sol
cs7 gtt map 1.2.3 10 sol
cs7 gtt map 1.12.1 10 sol
cs7 gtt map 2.2.2 20 dom 4.5.6 20
cs7 gtt map 4.1.2 10 rrc cspclist list1 adj dom 4.1.3 10
cs7 gtt map 4.1.3 10 dom 4.1.2 10
cs7 gtt map 4.5.6 20 dom 2.2.2 20
cs7 gtt map 5.6.7 10 sol
cs7 gtt map 7.255.7 100 sol
!
cs7 gtt application-group group1
multiplicity share
pc 1.1.1 1 gt
pc 1.2.3 ssn 10 4 pcssn
!
cs7 gtt application-group group2
multiplicity share
!
cs7 gtt selector steve 0 4 7 4
gta 800 pcssn 1.1.1 gt ssn 116
gta 801 pcssn 1.1.1 gt ssn 200
gta 802 pcssn 1.1.1 gt ntt 10
gta 803 pcssn 1.1.1 pcssn ssn 200
gta 804 pcssn 1.1.1 pcssn ssn 10
gta 805 qos-class 1 pcssn 7.255.7 pcssn ssn 100
```

```
gta 919 app-grp group1
!  
cs7 gtt selector mysel 10 2  
gta 919 app-grp group1
```

Related Commands

Command	Description
cs7 gtt application-group	Configures a GTT application group.
cs7 gtt concern-pclist	Specifies a GTT concerned point code list.
cs7 gtt map	Specifies a GTT Mated Application entry.
cs7 gtt selector	Creates a CTT selector.
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.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(25)SW1	This command was introduced.

Examples The following is sample 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	Configure a Global Title Mated Application (MAP) entry.
show cs7 gtt application-group	Displays CS7 GTT Application Group entries.
show cs7 gtt gta	Display 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*]

Syntax Description

<i>instance-number</i>	Specifies the instance. The valid range is 0 through 7. The default instance is instance 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.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)MB	This command was introduced.

Examples

The following is sample output of the **show cs7 gtt gta** command for all GTAs on the selector named c7gsp:

ITP# **show cs7 gtt gta c7gsp**

```

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

GTA            PC           RI   SSN   TT   App-Grp   QOS   ASNAME
-----
3330810        158           gt
3335114        245           pcssn 250
328                                     intergroup1
339            245           pcssn 250

```

[Table 38](#) describes the fields in the display.

Table 38 *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

Table 38 *show cs7 gtt gta Field Descriptions*

DFLTQOS	Default QoS characteristics for the selector
GTAs	Number of GTAs for the selector
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

Related Commands

Command	Description
gta app-grp	Creates or modifies a GTA entry that translates a GTA to a GTT application group.
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** [**ppc** *ppc* [**SSN** *ssn*]] [**status**]

Syntax Description

<i>instance-number</i>	Specifies the instance. The valid range is 0 through 7. The default instance is instance 0.
ppc	Specifies a primary point code.
<i>pc</i>	Primary SS7 point code, in the form zone.region.sp.
SSN	Specifies a subsystem number.
<i>ssn</i>	Subsystem number in the range 2 through 255.
status	Display the status of the subsystems.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)MB	This command was introduced.

Examples

The following is sample output of 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 is sample output of 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 39](#) describes the fields in the display.

Table 39 *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	(Optional) Displays measurements kept on a GTT application group basis.
<i>app-grp-name</i>	GTT application group name.
counters	(Optional) Displays Q.752 counters for GTT.
<i>instance-number</i>	Specifies the instance. The valid range is 0 through 7. The default instance is instance 0.
line-card	(Optional) Display measurements kept on a line card basis. The line-card option is available only if MTP3 offload is enabled (only on the Cisco 7500.)
<i>line-card-num</i>	(Optional) Line card number. If <i>line-card-num</i> is not specified, all line-card measurements for all line cards are displayed.
map	(Optional) Displays measurements kept on a GTT MAP basis.
selector	(Optional) Display statistics kept on a GTT selector basis.
<i>selector</i>	(Optional) Display statistics for a specified selector.
systot	(Optional) Displays measurements kept on a system-wide basis.

Defaults If no keyword is specified, the system totals (systot) is displayed.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)MB	This command was introduced.

Examples The following is sample output of 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

The following is sample output of the **show cs7 gtt measurements selector** command with no selector specified:

```
ITP# show cs7 gtt measurements selector
GTT/SCCP Selector Measurements Report

Selector Name  GTT_PERF    GTA_NF
c7gsp          0            0
itp_gtt        0            0
test           0            0
```

The following is sample output of the **show cs7 gtt measurements selector** command for the selector named c7gsp:

```
ITP# show cs7 gtt measurements selector c7gsp
GTT/SCCP Selector Measurements Report

Selector Name  GTT_PERF    GTA_NF
c7gsp          0            0
```

The following is sample output of 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
```

Table 40 describes the fields in the display.

Table 40 *show cs7 gtt measurements Field Descriptions*

Field	Description
GTT_PERF	The total # of successful translations performed
GTTSEL_NF	The total # 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	The total # of times a message requiring GTT was received with an invalid or not support format.
GTA_NF	The total # 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	The total # of times a message requiring GTT was alternate routed to a backup because of congestion.
GTT_HOP_ERR	The total # of times a message requiring GTT was received with a hop count that violated the rules concerning XUDT messages.
GTT_MAP_NF	The total # of times a message requiring GTT was received and final GTT was performed to a PC and SSN that was not provisioned in the GTT MAP table.
UNEQUIP_SS	The total number of times SCCP failed to route due to a subsystem being unequipped in the MAP table.

Table 40 *show cs7 gtt measurements Field Descriptions*

SCCP_UNAV	The total number of times SCCP failed to route due the SCCP subsystem being unavailable on a remote node.
DPC_UNAV	The total number of times SCCP failed to route due the destination point-code being unavailable.
SS_UNAV	The total number of times SCCP failed to route due the subsystem on a remote node being unavailable.
DPC_CONG	The total number of times SCCP failed to route due the destination point-code being congested.
SS_CONG	The total number of times SCCP failed to route due the subsystem on a remote node being congested.
MTP3_FAIL	The total number of times SCCP failed to route due to an MTP3 failure. (This occurs when 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 through 7. The default instance is instance 0.
gti		(Optional) Specifies a global title indicator.
<i>gti</i>		Global title indicator. Valid range is 0 through 4.
nai		(Optional) Specifies a nature of address indicator.
<i>nai</i>		Nature of address indicator.
name		(Optional) CS7 GTT selector name.
<i>name</i>		Selector name.
np		(Optional) Specifies a numbering plan.
<i>np</i>		Numbering plan.
tt		(Optional) Specifies a translation type.
<i>tt</i>		Translation type.

Command Modes	EXEC
---------------	------

Command History	Release	Modification
	12.2(1)MB	This command was introduced.
	12.2(4)MB	ttmap keyword added.

Examples The following is sample output from the **show cs7 gtt selector** command with no keyword options:

```
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	(Optional) Specifies the action-set name.
<i>action-set-name</i>	(Optional) Action-set name. Valid names contain no more than 12 alpha-numeric characters.

Command Modes

EXEC

Command History

Release	Modification
12.2(25)SW4	This command was introduced.

Examples

The following is sample output from the **show cs7 gws action-set** command with no arguments:

```
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 41](#) describes the fields in the display.

Table 41 *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 time 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 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 through 7. The default instance is instance 0.
name		(Optional) Specifies the AS.
<i>as-name</i>		(Optional) Name of the AS.
default		(Optional) Displays information about the default entry for the AS.

Command Modes	EXEC
---------------	------

Command History	Release	Modification
	12.2(25)SW4	This command was introduced.

Examples

The following is sample output from the **show cs7 gws as** command with no arguments:

```
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 42](#) describes the fields in the display.

Table 42 *show cs7 gws as Field Descriptions*

Field	Description
AS name	AS name.
Instance	Instance number.

Table 42 *show cs7 gws as Field Descriptions*

Field	Description
Screening	Indicates whether screening is enabled or disabled. If the corresponding CS7 AS is defined, this field indicates enabled .
Inbound Screening	Indicates whether inbound screening is defined and, if defined, indicates the result.
Result	Indicates the result action-set or table name.
Inbound Logging	Indicates the logging parameters that have been configured.
MSUs Screened	Indicates number of MSUs screened.
Allowed:	Indicates the number of MSUs allowed.
Blocked:	Indicates the 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	Indicates the logging parameters that have been configured.
MSUs Screened	Indicates number of MSUs screened.
Allowed:	Indicates the number of MSUs allowed.
Blocked:	Indicates the number of MSUs blocked.

Related Commands

Command	Description
cs7 gws as	Specifies an AS table for gateway screening.

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 through 7. The default instance is instance 0.
name	(Optional) Specifies the linkset.
<i>ls-name</i>	(Optional) Name of the linkset.
default	(Optional) Show the default linkset information.

Command Modes

EXEC

Command History

Release	Modification
12.2(25)SW4	This command was introduced.

Examples

The following is sample output from the **show cs7 gws linkset** command with no arguments:

```
ITP# show cs7 gws linkset
Linkset name: 'default'   Instance: 0   Screening: Enabled
  Inbound Screening ---- Result: Table OPC6
  Inbound Logging : type both file verbose
    MSUs Screened:      84, Allowed:      84, Blocked:      0
    MSUs Suspended:     0, Resumed:      0
Outbound screening - not defined
Linkset name: dallas     Instance: 0   Screening: Enabled
  Inbound Screening ---- Result: Action-set ALLOW
  Inbound Logging : type both file verbose
    MSUs Screened:     170, Allowed:     170, Blocked:      0
    MSUs Suspended:     0, Resumed:      0
Outbound Screening ---- Result: Action-set ALLOW
  Outbound Logging : type both test file verbose
    MSUs Screened:     167, Allowed:     167, Blocked:      0
```

[Table 43](#) describes the fields in the display.

Table 43 *show cs7 gws linkset* Field Descriptions

Field	Description
Linkset name	Indicates the linkset name.
Instance	Instance number.
Screening	Indicates whether screening is enabled or disabled. If the corresponding CS7 linkset is defined, this field indicates enabled .

Table 43 *show cs7 gws linkset Field Descriptions (continued)*

Field	Description
Inbound Screening	Indicates whether inbound screening is defined and if defined, indicates the result.
Result	Indicates the result action-set or table name.
Inbound Logging	Indicates the logging parameters that have been configured.
MSUs Screened	Indicates number of MSUs screened.
Allowed:	Indicates the number of MSUs allowed.
Blocked:	Indicates the 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.
Inbound Logging	Indicates the inbound logging parameters that have been configured.
Outbound Logging	Indicates the outbound logging parameters that have been configured.
MSUs Screened	Indicates the number of MSUs screened.
MSUs Suspended	Indicates that for CDPA screening MSU screening is suspended for GTT.

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>	(Optional) Specifies the instance. The valid range is 0 through 7. The default instance is instance 0.
name <i>table-name</i>	(Optional). Specifies the table name.
type <i>table-type</i>	(Optional) Specifies the table type. Valid table-types are:
	aff-dest Affected Dest Table
	aff-pc-ssn SCCP Aff. PC-SSN Table
	cdpa-digit-scr CdPA Digit Scr Table
	cdpa-pc-ssn CdPA PC-SSN Table
	cdpa-sccp-sel CdPA Selector Table
	cgpa-digit-scr CgPA Digit Scr Table
	cgpa-pc-ssn CgPA PC-SSN Table
	cgpa-sccp-sel 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
type <i>table-type</i>	(Optional) Display information about tables of a specified type.
detail	(Optional) Displays detailed statistics of the table.
result-summary	(Optional) Displays a summary of the table results.
entry-summary	(Optional) Displays a summary of the table entries.

Command Modes

EXEC

Command History

Release	Modification
12.2(25)SW4	This command was introduced.

Examples

The following is sample 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              Action-set ALLOW
3.3.3          3.3.4          Table al-cg-pcssn
3.3.5              Table al-cg-pcssn

```

The following is sample 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 44](#) describes the fields in the display.

Table 44 *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	The action-set or table.
Table Statistics:	
MSUs Screened	Indicates number of MSUs screened.
MSUs Allowed	Indicates the number of MSUs allowed.
MSUs Blocked	Indicates the number of MSUs blocked.
Num Entries	Number of entries defined in this table.
Ref Count	Number of times this table is referenced by others.

Table 44 *show cs7 gws table Field Descriptions (continued)*

Field	Description
Parameters:	
Default Result	Default result action-set or table.
Start PC End PC	Start and End PCs
Result	Result action-set or table.
MSUs Screened	Indicates number of MSUs screened.
MSUs Allowed	Indicates the number of MSUs allowed.
MSUs Blocked	Indicates the 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* | **routes** | **sls** | **statistics** | **state** | **timers** | **ttmap**] [**brief** | **detailed**]

Syntax Description

<i>instance-number</i>	Specifies the instance. The valid range is 0 through 7. The default instance is instance 0.
brief	(Optional) Does not display individual links.
cell	(Optional) Displays HSL cell counts for the linkset.
detailed	(Optional) Displays detailed linkset information
<i>ls-name</i>	(Optional) Linkset name. Displays information for a particular linkset.
routes	(Optional) Displays all routes using a linkset.
sls	(Optional) Displays SLC to SLS relationship.
state	(Optional) Displays MTP3 states for link.
statistics	(Optional) Displays link usage statistics.
timers	(Optional) Displays timer values.
ttmap	(Optional) Display TT mappings for linkset.
utilization	(Optional) Displays link utilization statistics.

Command Modes

EXEC

Command History

Release	Modification
12.2(1)MB	This command was introduced.
12.2(4)MB	Keyword ttmap added.
12.2(4)MB5	Keywords cell and utilization added.

Examples

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 linecard
 - MTP3 offload has been permanently disabled on a linecard by the system due to excessive errors. When MTP3 offload has been permanently disabled on a linecard (by the system) all links on that linecard will be in the sys-shutdown state.

The following is sample 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 is sample 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 is sample output from the **show cs7 linkset** command with the **detail** keyword:

```
MSTP# show cs7 linkset STP1 detail
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 is sample 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 is partial sample 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 (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 is sample 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
```

show cs7 linkset

```

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 is sample 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 is sample 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 is sample 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 is sample 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
```

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-receive	Specifies the receive threshold for a link.
threshold-send	Specifies the send threshold for a link.

Command	Description
timer (cs7 linkset)	Configures MTP3 timers that control the linkset (and, optionally, timers for links on the linkset.)
ttmap	Assigns a translation type mapping rule to the linkset.

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: <ul style="list-style-type: none">• 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.
--------------------	-------------	--

Command Modes	Global configuration
---------------	----------------------

Command History	Release	Modification
	12.2(25)SW	This command was introduced for <i>type gtt</i> .
	12.2(25)SW4	The <i>types gws-test</i> and <i>gws-nontest</i> were added

Examples

The following is sample 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
```

The following is sample output from the **show cs7 log gws-test** command:

```
itp# show cs7 log gws-test
```

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]]}
```

Syntax Description

congestion	(Optional) Displays M2PA congestion status.
local-peer	(Optional) Displays an M2PA local peer information.
<i>port-num</i>	Port number of the local peer. Valid range is 4096 through 32767.
peer	(Optional) Displays an M2PA remote peer information.
sctp parameters	(Optional) Displays SCTP peer parameters.
sctp statistics	(Optional) Displays SCTP peer statistics.
state	(Optional) Display the M2PA state machine status.
statistics	(Optional) Display the M2PA peer statistics.
timers	(Optional) Displays M2PA timers for RFC.
<i>ls-name</i>	Linkset name.
<i>slc</i>	(Optional) Signaling Link Code. Valid range is 0 through 15.

Command Modes

EXEC

Command History

Release	Modification
12.2(1)MB	This command was introduced.
12.2(25)SW3	The congestion , sctp statistics , and timers keywords were added.

Examples

The following is sample 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 is sample output from the **show cs7 m2pa** command using the **local-peer** keyword with the port number of the local peer (*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 is sample output from the **show cs7 m2pa** command using the **peer** keyword with the linkset name (*ls-name* argument) **to_nagshead**:

```
ITP#show cs7 m2pa peer to_nagshead
CS7 M2PA internal Peer Control Block Info for (50.0.0.5 : 4000)

Peer Protocol      : sctp
Peer Port          : 4000
Peer Version       : RFC
Peer Address       : 50.0.0.5           172.18.44.162
Primary Address    : 50.0.0.5
Effective Address  : 50.0.0.5

Transport Handle   : 0x00010001           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      ms          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
nl                 : 1000                   Debug mask          : 0x00000000
```

The following is sample 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 is sample 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 is sample 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 is sample 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 is sample 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 45](#) describes the fields in the **show cs7 m2pa stats** display.

Table 45 *show cs7 m2pa stats 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 (MSU's 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 when into congestion

Table 45 *show cs7 m2pa stats Field Descriptions*

Field	Description
T1_TMO_Count	Number of times link alignment timer expired
T6_TMO_Count	Number of times remote congestion timer expired

[Table 46](#) describes the fields in the **show cs7 m2pa state** display.

Table 46 *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 Units has been received
Transport Handle	Identifier assigned by transport for this peer

[Table 47](#) describes the fields in the **show cs7 m2pa peer** display.

Table 47 *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.
Local Recv Window	Local receive window size.

Table 47 **show cs7 m2pa peer Field Descriptions (continued)**

Field	Description
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 will be decreased due to the association being idle.
Retrans cwnd rate	Rate at which the size of the SCTP congestion window will be decreased due to retransmission timer expirations.
Retrans cwnd mode	The congestion window is set for a fast-retransmission.
FastRetransmit cwnd rate	Rate at which the size of the SCTP congestion window will be 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
Debug Mask	Mask indicating which levels of M2PA debug are active.

Table 48 describes the fields in the **show cs7 m2pa local-peer** display.

Table 48 *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 will be delivered to MTP3.
Instance IP Precedence	IP ToS setting that is 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*

Syntax Description	<i>instance-number</i>	Specifies the instance. The valid range is 0 through 7. The default instance is instance 0.
	<i>local_port</i>	(Optional) M3UA local port number. Range is 1024 to 65535.

Defaults	No default behavior or values
-----------------	-------------------------------

Command Modes	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	12.2(4)MB5	This command was introduced.

Examples

The following is sample 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 linecard.

```
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 VIP:            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.

show cs7 mated-sg

To display mated SG information, use the **show cs7 mated-sg** privileged EXEC command.

show cs7 [*instance-number*] **mated-sg** [**detail** | **statistics**] |

Syntax Description	<i>instance-number</i>	Specifies the instance. The valid range is 0 through 7. The default instance is instance 0.
	detail	(Optional) Display detail format.
	statistics	(Optional) Display mated SG statistics.

Command Modes	privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	12.2(4)MB5	This command was introduced.

Examples

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.

ITP# **show cs7 mated-sg**

Mate Name	State	Passive	Remote Port	Effect Remote IP Addr	Primary Sctp Assoc
bermuda	active	no	14002	172.18.48.15	0

The following is sample 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 detail**

Mated SG name: bermuda	Type: SGMP
State: active	Passive: no
SCTP association state: established	Association id: 0
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)
Local receive window: 5555	Cumulative sack timeout: 200 ms
Assoc retrans: 17	Path retrans: 4
Max init retrans: 8	Max init RTO: 1000 ms
Minimum RTO: 1001 ms	Maximum RTO: 1002 ms
Bundle status: on	Bundle timeout: 100 ms
Keep alive status: true	Keep alive timeout: 23234 ms
Unordered priority: equal	Cleanup timeout: 0 ms
Link status T1 timeout: 0 ms	Remote congest T6 timeout: 0 ms
Initial cwnd: 3000	Idle cwnd rate: 50
Retrans cwnd rate: 50	Retrans cwnd mode: RFC
Transmit queue depth: 1000	Congestion transmit level: 0

■ **show cs7 mated-sg**

```

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

```

The following is sample 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 Invalid ASP ID: 0          ERR Inv Routing Context: 0
      ERR Invalid Parm Value: 0          ERR Ukwn Routing Context: 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 Context: 0
      ERR Invalid Parm Value: 0          ERR Ukwn Routing Context: 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 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** *table-name*

Syntax Description	<i>instance-number</i>	Specifies the instance. The valid range is 0 through 7. The default instance is instance 0.
	<i>table-name</i>	The name associated with the multi layer result table.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(21)SW	This command was introduced.

Examples The following is sample output of the **show cs7 mlr result** 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
	cs7 mlr address-table	Specifies a table of addresses that is to be used when searching with the previously specified routing parameter.

show cs7 mlr dest-sme-binding

To display the result that will be selected from an SMS result group for 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 wish to display. Valid dest-sme addresses are between 1 and 20 hexadecimal characters in length. Only the final 4 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 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.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)SW4	This command was introduced.

Examples

The following is sample output of the **show cs7 sms dest-sme-binding** command:

```
ITP#show cs7 sms dest-sme-binding 12345035
Dest-sme: 12345035
Instance: 0   Result Group: MLR1
Order: 100   Result: PC 5.5.5
```

```
Dest-sme: 12345035
Instance: 0   Result Group: MLR5
Order: 600   Result: AS berm4
```

Related Commands

Command	Description
cs7 mlr result	Configures an MLR result group.

show cs7 mlr modify-profile

The **show cs7 mlr modify-profile** command 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.

show cs7 [*instance-number*] **mlr modify-profile** [*profile-name*]

Examples

```
linus# show cs7 mlr modify-profile
Instance 0
```

Name	Protocol	Operation	Matches	Modify Failures
MLR1	gsm-map	sri-sm	2	0

show cs7 mlr result

To display multi-layer SMS routing result information, use the **show cs7 mlr result** privileged EXEC command.

show cs7 [*instance-number*] **mlr result**

Syntax Description	<i>instance-number</i>	Specifies the instance. The valid range is 0 through 7. The default instance is instance 0.
--------------------	------------------------	---

Defaults	No default behavior or values.
----------	--------------------------------

Command Modes	Privileged EXEC
---------------	-----------------

Command History	Release	Modification
	12.2(4)MB	This command was introduced.

Examples

The following is sample output of 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	tti 0 gti 4 npi 1 nai 4	avail	1	1	0

Related Commands	Command	Description
	cs7 mlr result	Specifies a multi-layer result table.

show cs7 mlr ruleset

To display multi-layer routing (MLR) ruleset information, use the **show cs7 mlr ruleset** privileged EXEC command.

show cs7 [*instance-number*] **mlr ruleset** *name* [**rule-summary**]

Syntax Description

<i>instance-number</i>	Specifies the instance. The valid range is 0 through 7. The default instance is instance 0.
<i>name</i>	Ruleset name. A valid ruleset name is a character string with a maximum of 12 characters.
rule-summary	(Optional) Displays summary of all rules and operations.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)MB	This command was introduced.
12.2(18)IXB	The rule-summary keyword was expanded to display all supported operations.

Examples

The following is sample output of 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
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
Rule Oper  dest-sme      orig-sme      dest-smsc     Matches
----
10  sms-mo -            -            -            0
```

show cs7 mlr ruleset

The following is sample output of 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
```

The following is sample output of 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
-----
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

Name: MLR_RULES Instance:0 Protocol: n/a
Rule Operation Protocol Matches
-----
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

Name: GEN_OPC_GSM Instance:0 Protocol: gsm-map
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

Name: DEF Instance:0 Protocol: n/a
Rule Operation Protocol Matches
-----
10 sms-mo gsm-map 0

Name: TRACE Instance:0 Protocol: n/a Event-trace:disabled
Rule Operation Protocol Matches
-----
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
-----
10      smdpp                ansi-41                0

```

```

Name: GEN_OPC_SM     Instance:0   Protocol: n/a
Rule      Operation      Protocol      Matches
-----
102     all-operations        n/a                    0

```

```

Name: MLRRULESET4    Instance:4   Protocol: n/a
Rule      Operation      Protocol      Matches
-----
20      updLocation          gsm-map                0
30      smdpp                ansi-41                0
40      all-operations        n/a                    0

```

```

Name: MLR_GSM_4      Instance:4   Protocol: gsm-map
Rule      Operation      Protocol      Matches
-----
10      updLocation          gsm-map                0
19      allocHandOverNum     gsm-map                0
20      all-operations        gsm-map                0

```

The following is partial output of the show cs7 mlr ruleset command with the keywords **rule-summary** **gsm operation** **updLocation**. The output displays rules with the updLocation operation.

```
router# show cs7 mlr rule rule-summary gsm operation updLocation
```

```

Name: GEN_OPCODE     Instance:0   Protocol: n/a
Rule      Operation      Protocol      Matches
-----
10      updLocation          gsm-map                0
27      all-operations        n/a                    0

```

```

Name: MLR_RULES      Instance:0   Protocol: n/a
Rule      Operation      Protocol      Matches
-----
50      all-operations        n/a                    0

```

```

Name: GEN_OPC_GSM    Instance:0   Protocol: gsm-map
Rule      Operation      Protocol      Matches
-----
10      updLocation          gsm-map                0
100     all-operations        gsm-map                0

```

Related Commands

Command	Description
cs7 mlr ruleset	Specifies a multi-layer 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 through 7. The default instance is instance 0.
	operations	Displays the number of times each MAP operation was received.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)MB	This command was introduced.
	12.2(18)IXB	The operations keyword was added.

Examples The following is sample output of 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 is sample output of 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

```

show cs7 mlr statistics

GSM-MAP	regSS	operations :	0
GSM-MAP	eraseSS	operations :	0
GSM-MAP	actSS	operations :	0
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	provideSIWFSSNumber	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 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 dialogue and hence no MAP version, but with a component portion with the opcode value that is shared between different MAP versions.

If a CONTINUE is received with no dialogue portion, no MAP version, and the component portion has a shared opcode value, the rule match algorithm will look 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 will be considered the best match.

Table 49 describes the significant fields shown in the display.

Table 49 *show cs7 mlr statistics Field Descriptions*

Field	Description
Instance	The ITP instance for these MLR statistics.
Total packets processed by MLR:	The 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 MLR trigger(s).
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.

Table 49 **show cs7 mlr statistics Field Descriptions (continued)**

Continue trigger matches:	Number of packets that match a trigger that specifies the trigger action to continue (route the message as received).
Result trigger matches	Total number of trigger matches with a result trigger action.
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 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 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. In other words, a packet may be a segmented TCAP CONTINUE 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 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).

Table 49 **show cs7 mlr statistics Field Descriptions (continued)**

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.
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, etc.
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 to continue (route the message as received).
Result action route:	This count indicates the total number of MLR packets that select a result route specified on a rule result . These are modified packets that 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-group configuration command.
Failed to modify MSU:	This count 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 to block (drop) the packet.
Destination unavailable	Number of packets that MLR failed to route to 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-group configuration command.
Failed to modify MSU:	This count 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 49 *show cs7 mlr statistics Field Descriptions (continued)*

MLR Packets which 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	<ul style="list-style-type: none"> This statistic is an existing statistic that 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	<ul style="list-style-type: none"> This statistic is an existing statistic that 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 multi-layer ruleset table.

show cs7 mlr table

To display multi-layer SMS routing information use the **cs7 mlr table** privileged EXEC command. The default display is rule-summary.

show cs7 *instance-number* **mlr table** *name* [**detail** | **result-summary** | **rule-summary**]

Syntax Description

<i>instance-number</i>	(Optional) Displays output for a specified instance. Valid range is 0 to 7.
detail	Display the parameters and results associated with each routing trigger.
<i>name</i>	The name of the CS7 MLR table.
result-summary	Display 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	Display the rule parameters associated with a particular rule along with the number of times the rule has been matched for the given trigger.

Defaults

The default display is rule-summary.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)MB	This command was introduced.
12.2(21)SW	The <i>instance</i> argument was added.

Examples

The following is sample output of the **show cs7 mlr table** command:

```
ITP# show cs7 mlr table MLR
Name: MLR          Instance: 0
-----
Insert-dpc-in-cdpa enabled
Preserve-opc enabled
Modify-failure: sccp-error 0x7
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 50 describes the fields in the display.

Table 50 *show cs7 mlr table Field Descriptions*

Field	Description
Name	The name of the CS7 MLR table
Protocol	The name of the protocol.
Primary Trigger	The SS7 network layer routing parameters that constitute the routing key, or trigger, used to identify traffic requiring parsing into the application layers.
Ruleset	The name of the ruleset that is used to process matching triggers.
Matches	The total number of matches.
Rule	The order in which the rules in the ruleset are searched.
Operation	The GSM MAP operation code. The operation name represents a multi-layer routing feature that may comprise one or more actual MAP operations. In the current release, there is one valid choice for this parameter: sms-mo is used to identify SMS MO request messages for the table-appropriate protocol. This operation is valid for the GSM MAP, and will match all BEGIN requests containing an SMS-MO INVOKE component.
Dest-SME	The address of the destination Short Message Entity (SME) within an SMS operation.
Orig-SME	The address of the origin SME within an SMS operation.
Dest SMSC	The address of the destination service center address within an SMS operation.
PID	The 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 multi-layer SMS routing table.

show cs7 mtp2

To display current modify-profiles and their statistics, use the show **cs7 mlr modify-profile** display.

show cs7 mtp2 [**congestion** | **state** | **statistics** | **timers** | **variant**] *interface*

Syntax Description

congestion	MTP2 congestion status.
state	MTP2 state machine status.
statistics	MTP2 link statistics.
timers	MTP2 timer values.
variant	MTP2 protocol variant.
<i>interface</i>	Serial interface number.

Defaults

No default behavior or values

Command Modes

Privilege EXEC

Command History

Release	Modification
12.2(1)MB	This command was introduced.
12.2(20)SW	TTC timer values are displayed in output.

Usage Guidelines

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.

Examples

This section includes samples of output from the **show cs7 mtp2** command using the keywords **congestion**, **state**, **statistics**, **timers**, and **variant**.

The following is sample output of 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 51 describes the fields in the display.

Table 51 *show cs7 mtp2 congestion Field Descriptions*

Field	Description
Layer3 congestion status	<p>Receive congestion status at Layer3 (i.e. MTP3). There are 2 possible values:</p> <ul style="list-style-type: none"> Abate = MTP3 not congested. MTP2 may forward packets to MTP3 Onset = MTP3 congested. MTP2 may NOT forward paks to MTP3 <p>During Layer 3 congestion onset, MTP2 will send SIBs to the remote to indicate the route is “Busy” and cannot accept input packets</p>
CongestionRxInd	<p>Receive congestion status at Layer2 (i.e. MTP2)</p> <p>There are 2 possible values:</p> <ul style="list-style-type: none"> Abate = MTP2 not congested; Remote may send packets to MTP2. Onset = MTP2 congested:Remote may NOT send paks to MTP2. <p>During MTP2 congestion onset, MTP2 will send SIBs to the remote to indicate the route is “Busy” and cannot accept input packets.</p>

Table 51 *show cs7 mtp2 congestion Field Descriptions (continued)*

Field	Description
CongestionTxInd	<p>Transmit congestion status at Layer2 (i.e. MTP2)</p> <p>There are 5 possible values:</p> <ul style="list-style-type: none"> 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 not send packets to MTP2. <p>The levels correspond to ANSI congestion levels. (ITU has a similar option.)</p> <p>MTP3 paks have an associated priority (0-3).</p> <p>For example, if CongestionTxInd is Onset (Level2), MTP3 may continue sending packets with a priority of 2 or above, but must drop any packets with a priority of 1 or below.</p>
CongestionTxOnset Level1	MTP2 transmit congestion level thresholds.
CongestionTxOnset Level2	MTP2 determines its txCongestion level as a percentage of packets waiting on its transmitQ (i.e. "XmitQ depth (max-allowed)").
CongestionTxOnset Level3	The thresholds are documented in this output (and may NOT be configured or changed by the user).
CongestionTxOnset Level4	<p>The XmitQ depth (max-allowed) value is configurable by the user and the new threshold values will be reflected in the output.</p> <p>For example, if you configure a new xmitQ maxDepth via "cs7 mtp2 transmitQ 256":</p> <p>CongestionTxOnset Level1 = 128 (50% of xmitQ maxDepth)</p> <p>CongestionTxOnset Level2 = 179 (70% of xmitQ maxDepth)</p> <p>CongestionTxOnset Level3 = 230 (90% of xmitQ maxDepth)</p> <p>CongestionTxOnset Level4 = 256 (100% of xmitQ maxDepth)</p>
XmitQ depth (max-used)	<p>Maximum number of packets that have waited on the xmitQ</p> <p>This count indicates how much of the xmitQ is being used and may help guide configuration of "XmitQ depth (max-allowed)" value.</p>
XmitQ depth (max-allowed) = 500	Maximum-allowed depth of xmitQ: (used by MTP2 to determine txCongestion thresholds)

The following is sample output of 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 52 describes the fields in the display.

Table 52 *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 Layer3 perspective. There are 2 values: Started or Stopped
Layer3 congestion status = Abate	Indicates the congestion status from Layer3 perspective. There are 2 values: <ul style="list-style-type: none"> Abate = MTP3 not congested --- MTP2 may forward packets to MTP3 Onset = MTP3 congested ----- MTP2 may NOT forward paks to MTP3

The following is sample output of 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 53 describes the fields in the display.

Table 53 *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 Layer3 for transmit
OMMSU_XMIT_Count	Number of MSUs actually transmitted (includes retransmits)
OMMSUBytesTransmitted	Number of MSU bytes transmitted (includes retransmits)
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
OMAERMCount	Number of times AERM has been activated

Table 53 *show cs7 mtp2 statistics Field Descriptions (continued)*

Field	Description
OMAERMFailCount	Number of times AERM has failed
OMSUERMCount	Number of times SUERM has been activated
OMSUERMFailCount	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	Max number of paks that were ever waiting on xmitQ
OMNACK_XMIT_Count	Number of negative acknowledgement transmitted on link
OMNACK_RCV_Count	Number of negative acknowledgement 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 is sample output of 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 54 describes the fields in the display.

Table 54 *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.
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 ANSI or ITU defined.

The following is sample output of 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 55](#) describes the fields in the display.

Table 55 *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. There are 4 possible values: <ul style="list-style-type: none"> 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 error

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 No default behavior or values.

Command Modes EXEC

Command History

Release	Modification
12.2(13)MB	This command was introduced.

Examples

The following is sample 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 56](#) 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 56 *show cs7 mtp3 errors*

Error	Description
ACL received linkset match	An access list applied to all MSU arriving on a linkset matched and the result was to drop MSU.
ACL send linkset match	An access list applied to all MSU to be transmitted on a linkset matched and the result was to drop MSU.
AS not found for routing Context	Unable to locate routing context for Application service. No error message will be issued and Packet will be dropped.
Denied	A 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 match the signalling points primary or secondary point-coded. The packet will be dropped and no messages will be issued.

Table 56 *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 will be issued and Packet will be dropped.
Failure to locate active ASP	Unable to locate active Application Server Process. No error message will be issued and Packet will be dropped.
HMRT event overflow	The signalling message handling - message routing queue has reached limit and MSU will be discard 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 will be logged to console indicating source of packet and packet will be dropped.
Incorrect H1 value in SLTC message	A packet was received that contained an incorrect value for H1 field. An error message will be logged to console indicating source of packet and packet will be dropped
Incorrect link type	A packet was received that contained an undefined link type in "lp->type" field. This is likely a software error. Packet will be 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	This error type is not currently used.
Incorrect SCTP link status	This error type is not currently used.
Incorrect SCTP stream number	This error type is not currently used.
Invalid packet size (MSU size exceeded)	A MSU was received that exceed specified limit. No error message will be issued and Packet will be dropped.
Link event discarded (verification failed)	A MTP3 event was queued for processing. However, event can not be processed because the target resource does not exist. This can occur when links or linkset are un-configured. MTP3 event will be discarded without issuing error message.
Local Point Code not defined	A packet was received before local point-coded 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	A MSU processed by Multi-layer Routing has matched rule indicating it should be aborted. No error message will be issued and Packet will be dropped.
No instance	A MSU was received on a link and the Instance information is inconsistent. This can occur when instances are removed or linkset are moved between instances. It may also occur as a by-product of some software error. MSU will be discarded without issuing message to log.
No link	A MSU was received that specified a destination point code. The output linkset did not have any operational links. MSU will be dropped and no error messages will be displayed.

Table 56 *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	A 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 will be dropped and no error messages will be displayed.
No memory for cs7_info chunk	A MSU was received but could not be processed because necessary additional storage was unavailable. No error message will be issued. Packet will be 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 will be issued. Packet will be dropped.
Received partial SCTP buffer	A partial packet was received and could not be processed by SCTP layer. No error message will be issued. Packet will be dropped.
Remote congestion	A link used to transport MSU to next Signalling point is congestions. MSU are discarded as required by congestion control. Messages will be logged to console when link enters and exits congestions.
Send failure	An error occurred when attempting to send packet on link. Packet will be dropped without issuing error message.
SLT failed	A Signalling Link Test Message failed. This error occurs when the sender of the SLT messages did not receive a response in the required time frame. <ul style="list-style-type: none"> • The variant is miss-configured. • The link has some type of mismatch on configuration • Link has some type of hardware problem.
SLT incorrect network indicator	A Signalling Link Test Message was received with a different network indicator. An Error message will be logged to console indicating link receiving SLTM.
SLT incorrect OPC	A Signalling 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 will be logged to console indicating the linkset on which link was received and the linkset that should have received SLTM.
SLT incorrect SLC	A Signalling Link Test Message was received from a different Signalling Link Code than was expected for the link. For example a link is configured with SLC of 5 and is incorrect connected to link with SLC of 15.2.1. Error messages will be logged to console indicating the link that was miss-configured.

Table 56 *show cs7 mtp3 errors (continued)*

Error	Description
SLT invalid	A Signalling Link Test Message which contained incorrectly formatted data and could not be processed.
SLT received bad pattern	A Signalling Link Test Message received with an incorrectly formatted pattern. This can occur in the following situations: <ul style="list-style-type: none"> • 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 Signalling 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 will be logged to console indicating the linkset on which this SLTM was received.
SLT undefined OPC	A Signalling Link Test Message was received from an Origination Point-Code that is not defined to any linkset.
SLT undefined SLC	A Signalling Link Test Message was received from a Signalling Link Code not in use for linkset. An error message will be logged indicating which link received SLTM messages and the incorrect SLC.
Undefined Error Type	An error unknown error type was encountered that likely 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 will be issued. Packet will be dropped.
Unsupported management messages	This error type is 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 3 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 through 7. The default instance is instance 0.
<i>number</i>	Number of events to display. Valid numbers are in the range 0 to 1024.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
12.2(1)MB	This command was introduced.

Usage Guidelines

To capture all events in one display, configure the **terminal length** EXEC command to 0.

Examples

The following is sample output from the **show cs7 mtp3 event-history** command with the number of events to display (*number* argument) **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 through 7. The default instance is instance 0.
--------------------	------------------------	---

Command Modes	EXEC
---------------	------

Command History	Release	Modification
	12.2(1)MB	This command was introduced.

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 is sample 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
	cs7 mtp3 timer	Configures MTP3 management timers globally.

show cs7 nso

To display NSO information, use the **show cs7 nso** command in EXEC mode.

show cs7 nso { counters [detailed] | state }

Syntax Description	counters	Display counters maintained by NSO.
	detailed	(Optional) Display detailed output.
	state	Display NSO state information.

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 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 57](#) describes the significant fields shown in the display.

Table 57 *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 RSP.
Checkpointing state	Fields describe current state of checkpointing.

Table 57 *show cs7 nso Field Descriptions (continued)*

Field	Description
Last seq # sent	Sequence number of last NSO Checkpointing message sent to other RSP.
Last seq # rcvd:	Sequence number of last NSO Checkpointing message received from other RSP.
Congested	TRUE if congestion is present on communication to other RSP.
Current send queue depth	Number of messages waiting to be sent to other RSP.

Related Commands

Command	Description
cs7 nso	Enable ITP Non-Stop Operation (NSO).
show tech-support	Collects and displays a large amount of ITP configuration information that can be used for troubleshooting.

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>	(Optional) linecard slot number. Valid numbers are in the range 0 to 12.
events	(Optional) Displays all the events logged in the maintenance of the configuration and status on the linecard. If the slot number and combined keyword are not specified, then the events are displayed independently for each linecard.
detailed	(Optional) Displays the counters maintained for the configuration download to the linecard. When the detailed keyword is specified with the events keyword, additional information related to the event is also displayed.
combined	(Optional) When specified without a slot number, displays the events intervixed for all linecards in the timestamp order in which they occurred.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.2(4)MB	This command was introduced.

Examples

The following is sample output from the **show cs7 offload mtp3** command. The output indicates that MTP3 Offload is enabled on linecards 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 59 describes the fields in the display, including the possible values that can be displayed in the Status and Offload columns.

Table 58 *show cs7 offload mtp3 Field Descriptions*

Field	Description
Slot	Linecard slot.
Status	The Status column indicates which phase is currently applicable for the MTP3 offload on each linecard. 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 linecard. This will be indicated when error recovery is in progress.
Init	MTP3 offload is being initialized on the linecard.
Normal	MTP3 offload is enabled and operating normally.
PermDisabled	<p>MTP3 offload has been permanently disabled on the linecard. This will be indicated when excessive errors have been encountered on the linecard and repeated error recovery attempts have failed.</p> <p>When a linecard enters this state, the status of all links on the linecard will be displayed as “sys-shutdown” when the show cs7 linkset command is executed.</p> <p>A linecard in this state can be restarted manually by issuing the cs7 offload mtp3 restart command.</p>
Offload	The Offload column indicates whether or not MTP3 is operational on the linecard. 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 will be displayed whenever the ITP is performing error recovery or when MTP3 offload has been permanently disabled on the linecard.
Enabled	MTP3 offload has been enabled on the linecard.

Related Commands

Command	Description
cs7 offload mtp3	Enables MTP3 offload on all linecards.

show cs7 pc-conversion

To display mapping of real to alias point codes, use the **show cs7 pc-conversion** EXEC command.

show cs7 [*instance-number*] **pc-conversion**

Syntax Description

<i>instance-number</i>	Instance number.
------------------------	------------------

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.2(4)MB	This command was introduced.

Usage Guidelines

This command can be issued either globally or on an instance.

Examples

The following is sample 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 bwtween instances on the ITP.
cs7 multi-instance	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** EXEC command.

show cs7 ping *point-code*

Syntax Description	<i>point-code</i>	Point code of the device to ping.
--------------------	-------------------	-----------------------------------

Defaults	No default behavior or values.
----------	--------------------------------

Command Modes	EXEC
---------------	------

Command History	Release	Modification
	12.2(1)MB	This command was introduced.

Examples	<p>The following is sample output from the show cs7 ping command:</p> <pre>ITP# show cs7 ping 10.44.156 running state Generating, 5 seconds left current send sequence 4, receive seq 4</pre>
----------	---

Related Commands	Command	Description
	ping cs7	Starts a ping to a point code.

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**]

Syntax Description

<i>instance-number</i>	Specifies the instance. The valid range is 0 through 7. The default instance is instance 0.
event-history	Displays point code history.
ssn	Displays SUA point code/SSN status.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)MB5	This command was introduced.

Usage Guidelines

The **show cs7 point-codes** command will display 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 is sample 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 use 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 through 7. The default instance is instance 0.
class	(Optional) Specifies QoS class.
<i>class</i>	QoS class identifier. Valid range is 0 through 7.
statistics	Displays QoS link usage statistics.
<i>ls-name</i>	Linset name.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
12.2(1)MB	This command was introduced.

Examples

The following is sample 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      14      none
    1     3      14      any      to_nyc
    2     3      2701  access-group  to_la
    3     4      none
```

[Table 59](#) describes the fields in the display.

Table 59 *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 is defined.

The following is sample 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 60 describes the fields in the display.

Table 60 *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 route

To display the ITP routing table, use the **show cs7 route** EXEC command.

show cs7 [*instance-number*] **route** [*pc* [**summary-routes**]] [**brief** | **detailed**]

Syntax Description

<i>instance-number</i>	Required only if the cs7 multi-intance feature is enabled. Specifies the instance. The valid range is 0 through 7. The default instance is instance 0.
<i>pc</i>	Point code.
summary-routes	(Optional) Displays summary routes information for the specified pc.
brief	(Optional) Displays a brief form of the output.
detailed	(Optional) Displays a detailed form of the output.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
12.2(1)MB	This command was introduced.
12.2(4)MB	Show output enabled for multiple instance feature.

Usage Guidelines

The output of the **show cs7 route** command will vary based on the options specified, the variant, the masks used to configure routes and configuration options.

There are two basic types of routes. 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 would have a mask of 255.255.255 or mask length of 24 bits. When the variant is ITU the fully qualified route would have a mask of 7.255.7 or 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 and 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 ANSI variant and mask where the mask must be 255.255.0.

In ITP release 12.2(18)IXC, the displayed XUA pointcode status includes the MTP destination status of that pointcode.

The following configuration options effect the route and destination status information:

summary-routing-exception

The summary-routing-exception configuration option indicates whether to use the summary route when the fully qualified route is not available. By default the summary-routing-exception option is off and summary route can be used to route MTP3 messages. In this case, when a summary route is available

and fully qualified route is unavailable the destination status for the fully qualified route will be restricted rather than unavailable. When summary-routing-exception option is enable the destination status for the fully qualified route will be unavailable.

max-dynamic-routes

The max-dynamic-routes configuration option defines the maximum number of dynamic route allowed for the signalling point. If the limit is reached the status of some routes will 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 signalling points. When this options 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 will not update all route and destination statuses. Routing behavior will change correctly, although it might not match what would be 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 are 2 samples of output from the **show cs7 route** command executed with no modifier keywords.:

```
ITP# show cs7 route
Routing table = system Destinations = 3 Routes = 3
Instance = 3
```

Destination	Prio	Linkset Name	Route
1.1.0/11	access	1 barbados	avail
1.1.1/14	access	1 bermuda	avail
		5 bimini	avail
3.1.1/14	access	5 bermuda	avail

```
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 following sample includes an example of a host names to point code mapping.

```
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

show cs7 route

```

green          INACC  5  one          UNAVAIL
red            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
green	INACC 5	two	UNAVAIL
3.3.3/24	INACC 1	two	UNAVAIL

The show cs7 route command with the brief keyword produces only a list of destinations. The following is sample 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 route command with the detailed option produces a list of destinations and associated routes with the available management information. The following is sample output from the **show cs7 route** command executed with the **detailed** keyword:

```

ITP# show cs7 route detailed
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		avail
1.1.1/14	acces		1	bermuda	avail	allowed	avail
			5	bimini	avail	allowed	avail
3.1.1/14	acces		5	bermuda	avail	allowed	avail

Routing table = XUA

Destination	Type	XUA Name
2.1.1/14	INACC AS	cuba down
2.2.2/14	RESTR AS Route	asrout2
4.1.1/14	INACC AS	newone down
	AS	as2 down
4.4.4/14	RESTR AS Route	asrout1

The following is sample output from the **show cs7 route** command executed with a destination point code (*destination* 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 and summary-routes keyword will produce a list of route matching the specified destination. The following is sample output from the show cs7 route command executed with the point-code destination 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 61 describes the fields in the display.

Table 61 *show cs7 route Field Descriptions*

Field	Description						
Destination	<p>This field is displayed in the format "dpc/masklength status".</p> <p>dpc is the destination point code.</p> <p>masklength is the number of significant leading bits in the point code.</p> <p>status can be one of the following:</p> <table> <tr> <td>acces</td><td>Accessible</td></tr> <tr> <td>INACC</td><td>Inaccessible</td></tr> <tr> <td>RESTR</td><td>Restricted</td></tr> </table> <p>The restricted status is only available under the ITU variant when the cs7 national-options TFR configuration option has been specified.</p> <p>The destination information is followed by one or more routes to that destination in the default and detailed views.</p>	acces	Accessible	INACC	Inaccessible	RESTR	Restricted
acces	Accessible						
INACC	Inaccessible						
RESTR	Restricted						
C	<p>Congestion information will appear when the brief or detailed keyword has been specified. This 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 numbers 1, 2, or 3. In ITU networks with the national option for multiple congestion levels turned off, this field would display the number 1 if the destination is congested.</p>						
Q	<p>This is the QoS class assigned to the destination, a decimal number in the range 1 to 7.</p>						

Table 61 *show cs7 route Field Descriptions (continued)*

Field	Description
P	This is the route priority, a decimal number in the range 1 to 9.
Linkset Name	This identifies the linkset for a route to the destination.
Linkset	The linkset status can be one of the following: <div> <div>avail</div> <div>Available</div> </div> <div> <div>UNAVAIL</div> <div>Unavailable</div> </div>
Non-adj	The non-adjacent status shows the accessibility of the destination from the adjacent point code at the remote end of the linkset. It can be one of the following: <div> <div>allowed</div> <div>Allowed</div> </div> <div> <div>RESTRIC</div> <div>Restricted</div> </div> <div> <div>PROHIB</div> <div>Prohibited</div> </div>
Route	This is the route status. This can be one of the following: <div> <div>avail</div> <div>Available</div> </div> <div> <div>RESTRIC</div> <div>Restricted</div> </div> <div> <div>UNAVAIL</div> <div>Unavailable</div> </div> <p>The route status is derived from the linkset status and the non-adjacent status. The latter are displayed in the detailed view. If the linkset is unavailable, the route is unavailable. If the linkset is available, the non-adjacent status is mapped to Route Status as follows:</p> <div> <div> <div>Non-Adjacent</div> <div>allowed</div> <div>restricted</div> <div>prohibited</div> </div> <div> <div>Route</div> <div>available</div> <div>restricted</div> <div>unavailable</div> </div> </div>

Related Commands

Command	Description
cs7 host	Maps a host name 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 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	Display a count of how many MSUs matched each rule in the GTI table.
--------------------	--------------	--

Command Modes	privileged EXEC
---------------	-----------------

Command History	Release	Modification
	12.2(20)SW	This command was introduced.

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 is sample 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 is sample 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
```

 **show cs7 sccp gti-conversion****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	Display a count of how many SCCP MSUs were converted from one instance to another.
--------------------	--------------	--

Command Modes	privileged EXEC
---------------	-----------------

Command History	Release	Modification
	12.2(20)SW	This command was introduced.

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 is sample 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-gtt-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 No default behavior or value

Command Modes Privileged EXEC

Release	Modification
12.2(20)SW	This command was introduced.

Examples The following is sample 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

Command	Description
cs7 sccp ssn-conversion	Creates a subsystem mapping table

show cs7 sctp address-table

To display status information about the interfaces being used by Sctp, use the **show cs7 sctp address-table** privileged EXEC command.

show cs7 sctp address-table

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Defaults	No default behavior or value
-----------------	------------------------------

Command Modes	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.

Examples	The following is sample output from the show cs7 sctp address-table command:
-----------------	---

```
FlexWAN-ENH-2/1#show cs7 sctp address-table
      Sctp IP address table
address      vlan      mtu      state
-----
20.0.0.1      1032      1500      UP
70.0.0.2      1023      4470      DOWN
80.0.0.2      1022      4470      UP
90.0.0.1      1033      1500      UP
```

Table 62 describes the field in the display

Table 62 *show cs7 sctp address-table Field Descriptions*

Field	Description
address	IP address.
vlan	Internal VLAN ID.
mtu	MTU size.
state	Status of the interface.

show cs7 sctp port-map

To display all of the open SCTP ports, use the **show cs7 sctp port-map** privileged EXEC command.

show cs7 sctp port-map

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or value

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.

Examples The following is sample output from the **show cs7 sctp port-map** command:

```
FlexWAN-ENH-2/1#show cs7 sctp address-table
                        Sctp port to ltl map
  port    ltl    prot    txpkts    txdrops    rxpkts    rxdrops
-----
  5000    255    m2pa         10         0         0         0
  5001    255    m2pa         0         0         0         0
  2905    1151   m3ua         0         0        88         0
```

[Table 63](#) describes the field in the display

Table 63 *show cs7 sctp port-map Field Descriptions*

Field	Description
port	SCTP port number.
ltl	Linecard identifier.
prot	Protocol that owns the open SCTP port.
txpkts	Number of packets transmitted from this linecard to the destination linecard.
txdrops	Number of packets dropped on this linecard that could not be delivered to the destination linecard.
rxpkts	Number of packets received from other linecards.
rxdrops	Number of received packets from other linecards that were dropped.

show cs7 sgmp

To display Signaling Gateway Mate Protocol (SGMP) information, use the **show cs7 sgmp** privileged EXEC command.

show cs7 [*instance-number*] **sgmp**

Syntax Description

<i>instance-number</i>	Specifies the instance. The valid range is 0 through 7. The default instance is instance 0.
------------------------	---

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)MB5	This command was introduced.

Examples

The following is sample 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 VIP: 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
```

Related Commands

Command	Description
cs7 sgmp	Establish an association to the mated signaling gateway and enters CS7 SGMP submode.

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. The valid range is 0 through 7. The default instance is instance 0.
<i>local-port</i>	SUA local port number. Valid range is 4096 to 32767.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)MB5	This command was introduced.

Examples

The following is sample output from the **show cs7 sua** command. This SUA instance is offloaded to the linecard 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.

This SUA instance is offloaded to the linecard in slot 6.

```
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 VIP:                  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	No default behavior or values.
----------	--------------------------------

Command Modes	Privileged EXEC
---------------	-----------------

Command History	Release	Modification
	12.2(25)SW3	This command was introduced.

Examples	The following is sample output of the show cs7 tcap command with the no keywords:
----------	--

```
ITP# show cs7 tcap1
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 ITP version that is running on the Supervisor and on all the linecards on the system, use the show cs7 version command in EXEC mode.

show cs7 version

Syntax Description This command has no arguments or keywords

Command Modes EXEC

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.

Examples The following is sample 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 64](#) describes the fields in the display.

Table 64 *show cs7 version Field Descriptions*

Field	Description
Major	Major version.
Minor	Minor version.
Sup	Supervisor.
LC	Linecard.

Related Commands	Command	Description
	show tech-support	Collects and displays a large amount of ITP configuration information.

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>	(Optional) Display information about a specific linkset.
brief	(Optional) Display output in brief format. Don't display individual links.
routes	(Optional) Display all routes using linkset.
statistics	(Optional) Display link usage statistics.
utilization	(Optional) Display link utilization for linkset.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(23)SW1	This command was introduced.

Usage Guidelines

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 instanceX and instanceY, 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.

Examples

The following is partial sample 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
  SLC  Interface      Service  PeerState      Inhib
  00   Virtual      avail    -----      -----
```

The following is sample 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 is sample 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 is sample 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           0
```

The following is sample 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  Sent  Lvl
0    0    0    40  40  256  256  0    0    0
all  0    0    --- --- 256  256  0    0    ---
```

Table 65 describes the fields shown in the display.

Table 65 *show cs7 virtual linkset Field Descriptions*

Field	Description
lsn=VirtualLS1-0	The link set name, in this example a virtual linkset from instance 1 to instance 0.
apc=0.30.1:0	The adjacent point code. This is the alias point code, 0.30.1 instance 0.
state=avail	The state of the virtual linkset, in this example available. Allowed state are avail and UNAVAIL. The virtual linkset is unavail when all real linksets to instance are down.
avail/links=1/1	The 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 0-15.
Interface	Interface type. This is a virtual interface.
Service	The status of the service. In this example the service is available. Allowed state 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 host** privileged EXEC command.

show hosts

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)MB	This command was introduced.

Examples The following is sample output from the **show hosts** command with no keywords:

```
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
```

show hosts

```

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	Map a host name 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 assocId | statistics assocId]] | [errors] | [instances]
| [statistics]}
```

Syntax Description

association	Specifies an Sctp connection.
list	Current Sctp association.
parameters	Sctp association parameters.
<i>assocId</i>	Association ID number. Valid range is 0 through 1024.
statistics	Sctp association statistics.
errors	Sctp error statistics.
instances	Sctp local peer instances.
statistics	Sctp internal statistics.

Command Modes

EXEC

Command History

Release	Modification
12.2(1)MB	This command was introduced.

Examples

This section shows sample output from various forms of the **show ip sctp** command. Each sample is followed by a table describing the fields in the output display.

The following is sample output from **show ip sctp** command using the **association list** keywords:

```
ITP# show ip sctp association list
** Sctp Association List **

AssocID:0, Instance ID:0
Current state:ESTABLISHED, uptime:00:21:24
Local port:9000, Addr:172.18.44.162
Remote port:9000, Addr:172.18.44.170
```

[Table 66](#) describes the fields in the show ip sctp association list display.

Table 66 *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

Table 66 *show ip sctp association list Field Descriptions (continued)*

Field	Description
Addr	Local or Remote Peer Addresses
Remote Port	Remote port number

The following is sample output from **show ip sctp** command using the **association parameters** keywords with *assocId* 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 67](#) describes the fields in the **show ip sctp association parameters** display.

Table 67 *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
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

Table 67 *show ip sctp association parameters Field Descriptions (continued)*

Field	Description
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 is sample output from the **show ip sctp** command using the **association statistics** keywords with *assocId* 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 68 describes the fields in the **show ip sctp association statistics** display.

Table 68 *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

Table 68 *show ip sctp association statistics Field Descriptions (continued)*

Field	Description
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 is sample output from **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 69](#) 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 69 *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 can't 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.

Table 69 **show ip sctp errors Field Descriptions**

Field	Description
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 params received in Init or Init-Ack chunks.
Invalid stream error rcvd	Invalid stream error cause received in error chunk.
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 rcv'd 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	IO memory is low. packets are dropped.

The following is sample output from **show ip sctp** command using the **instances** keyword:

```
ITP# show ip sctp instances

** SCTP Instances **

Instance ID:0 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 70 describes the fields in the **show ip sctp instances** display.

Table 70 *show ip sctp instances Field Descriptions*

Field	Description
Instance ID	SCTP instance ID
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 is sample output from **show ip sctp** command using the **statistics** keyword:

```

ITP# show ip sctp statistics

** 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 71 describes the fields in the **show ip sctp statistics** display.

Table 71 *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 rrdered 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 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** command in privileged EXEC mode.

show redundancy states

Syntax Description This command has no arguments or keywords.

Command Modes privileged EXEC

Command History	Release	Modification
	12.2(18)IXA	This command was introduced.

Examples The following output shows the redundancy state on the ACTIVE Supervisor before 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 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 linecard.
cs7 upgrade analysis	Displays a report indicating the probable impact of performing a software upgrade.

show sscf-nni

To display SSCF information, use the **show sscf-nni atm** EXEC command.

show sscf-nni *interface*

Syntax Description	<i>interface</i>	If no interface number is specified, all interfaces supporting SSCF-NNI will be displayed.
--------------------	------------------	--

Defaults	No default behavior or values.
----------	--------------------------------

Command Modes	EXEC
---------------	------

Command History	Release	Modification
	12.2(2)MB	This command was introduced.

Examples The following is sample 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 72](#) describes the fields in the **show sscf** display.

Table 72 *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 as defined in Q.2140.
Configured parameters	The configured parameters.

Table 72 ***show sscf Field Descriptions***

Field	Description
Dynamic parameters	Variables used by SSCE, defined in Q.2140.
SSCOP-UU values	Most recent values sent or received, 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 will be displayed.
------------------	--

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following is sample 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 73 describes the fields in the **show sscop** display.

**Note**

“Inactive” status (in the Timer fields) does not mean that the timer is disabled. Inactive means that the timer is currently not running.

Table 73 *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 milli-seconds and the Active/Inactive status.
Timer_CC	Configured sscop cc-timer in milli-seconds.
Timer_POLL	Configured sscop poll-timer in milli-seconds.
Timer_KEEPAKIVE	Configured sscop keepalive-timer in milli-seconds.
Timer_NO-RESPONSE	Configured sscop noResponse-timer in milli-seconds.
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 pransmit 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 received/sent.
Begin Ack	Number of Begin Ack frames received/sent.

Table 73 *show sscop Field Descriptions (continued)*

Field	Description
Begin Reject	Number of Begin Reject frames received/sent.
End	Number of End frames received/sent.
End Ack	Number of End Ack frames received/sent.
Resync	Number of Resync frames received/sent.
Resync Ack	Number of Resync Ack frames received/sent.
Sequenced Data	Number of Sequenced Data frames received/sent.
Sequenced Poll Data	Number of Sequenced Poll Data frames received/sent.
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's frames received/sent.
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 send window was closed by the peer.

show tech-support

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(25)SW1	This command was enhanced to display information about ITP.

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 of 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 of the following commands is displayed:

- show cs7 m3ua
- show cs7 sua
- show cs7 asp
- show cs7 as
- show cs7 point-codes

When ITP Non-stop Operation (NSO) is configured, output of the following commands is displayed:

- show cs7 nso state
- show cs7 nso counters detailed

When ITP Group is configured, output of the following commands is displayed:

- show cs7 group state
- show cs7 group counters detailed
- show cs7 group transport

Defaults

No default behavior or values.

Command Modes

CS7 M3UA

Command History

Release	Modification
12.2(4)MB5	This command was introduced.

Examples

The following example disables 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 as)

To disable an AS without deleting the configuration, use the **shutdown** CS7 AS submode command. To reen able, use the **no** version of this command.

shutdown

no shutdown

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Defaults	No default behavior or values
-----------------	-------------------------------

Command Modes	CS7 AS submode
----------------------	----------------

Command History	Release	Modification
	12.2(4)MB5	This command was introduced.

Examples	The following example disables the AS named as1 without deleting the configuration: <pre>cs7 as as1 shutdown</pre>
-----------------	---

Related Commands	Command	Description
	cs7 as	Specifies the Application Server and enters CS7 AS submode.

shutdown (cs7 asp)

To disable an ASP without deleting the configuration, use the **shutdown** CS7 ASP submode command. To reenale, use the **no** version of this command.

shutdown

no shutdown

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes CS7 ASP

Command History	Release	Modification
	12.2(4)MB5	This command was introduced.

Examples The following example disables the ASP named ASP1:

```
cs7 asp ASP1 2904 2905 m3ua
shutdown
```

Related Commands	Command	Description
	cs7 asp	Specifies an Application Server Process and enables CS7 ASP submode.

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 the command.

shutdown

no shutdown

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes CS7 link submode

Command History	Release	Modification
	12.2(1)MB	This command was introduced.

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/link.

Examples The following example disables the link:

```
cs7 linkset michael 10.1.1
link 0 sctp 172.18.44.147 7000 7000
shutdown
```

Related Commands	Command	Description
	cs7 inhibit	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 No default behavior or values.

Command Modes CS7 linkset submode

Command History	Release	Modification
	12.2(1)MB	This command was introduced.

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 will be shown as “SHUTDOWN” in the output of the **show term** command.

However, the links in the linkset will not appear as “SHUTDOWN” because they were not administratively shutdown.

Also, when a link is administratively shut down, it remains in the shutdown state (and will not be 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 the user to maintain the state of the link when linksets are activated, in case the user does 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/link.

Examples The following example shuts down the linkset, and all links in the linkset:

```
cs7 linkset rosebud
shutdown
```

The following example reactivates 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 shutdown the M3UA protocol, use the **shutdown** CS7 M3UA submode command. To reenable, use the **no shutdown** command.

shutdown

no shutdown

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes CS7 M3UA

Command History	Release	Modification
	12.2(4)MB5	This command was introduced.

Examples The following example disables 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 mated-sg)

To disable a mated SG without deleting the configuration, use the **shutdown** CS7 Mated-SG submode command. To re-enable, use the **no** version of this command.

shutdown

no shutdown

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Defaults	No default behavior or values
-----------------	-------------------------------

Command Modes	CS7 Mated-SG
----------------------	--------------

Command History	Release	Modification
	12.2(4)MB5	This command was introduced.

Examples	The following example disables 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 re-enable, use the **no** version of this command.

shutdown

no shutdown

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes CS7 SGMP

Command History	Release	Modification
	12.2(4)MB5	This command was introduced.

Examples The following example disables 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 AS submode command. To re-enable, use the **no** version of this command.

shutdown

no shutdown

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Defaults	No default behavior or values
-----------------	-------------------------------

Command Modes	CS7 SUA
----------------------	---------

Command History	Release	Modification
	12.2(4)MB5	This command was introduced.

Examples	The following example disables 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.

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-set action-set-name | table tablename }
```

```
no si si mtp-msg-h0 mtp-msg-h0 mtp-msg-h1-range mtp-msg-h1-start [mtp-msg-h1-end] result
    { action-set action-set-name | table tablename }
```

or

```
si si mtp-msg-type mtp-msg-type result { action-set action-set-name | table tablename }
```

```
no si si mtp-msg-type mtp-msg-type result { action-set action-set-name | table tablename }
```

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-set action-set-name | table tablename }
```

```
no si si [priority-range pri-start [pri-end]] result { action-set action-set-name | table tablename }
```

Syntax Description

<i>si</i>	Service indicator. Valid SI values are mgmt , test1 , test2 , sccp , and isup .
mtp-msg-h0	Specify MTP3 message type - H0
<i>mtp-msg-h0</i>	Valid <i>mtp-msg-h0</i> values: CHM Changeover and Changeback messages DLM Sig Data Link Connection Order messages ECM Emergency Changeover messages FCM Transfer Controlled and Sig Routeset Congestion messages MIM Management Inhibit messages RSM Routeset test messages TFM Transfer Prohibited, Allowed & Restricted messages TRM Traffic Restart Allowed messages UFC User Part Flow Control messages
mtp-msg-h1-range	Specify starting H1 - MTP3 message type.
<i>mtp-msg-h1-start</i>	Starting H1 - MTP3 message type. Valid values are 1 through 8.
<i>mtp-msg-h1-end</i>	Ending H1 - MTP3 message type. Valid values are 1 through 8.
mtp-msg-type	Specify MTP message type.

<i>mtp-msg-type</i>	Valid <i>mtp-msg-type</i> 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	Specify a priority-range
<i>pri-start</i>	Priority start value.
<i>pri-end</i>	Priority end value.
result	Specifies the next step.
action	Specifies that the default result will be to screen by action set.
<i>action-set-name</i>	Action set name. Valid names may not exceed 12 alpha numeric characters.
table	Specifies that the default result will be to screen by table.
<i>table-name</i>	Table name. Valid names may not exceed 12 alpha numeric characters.

Command Default No default behavior or values.

Command Modes CS7 GWS table configuration

Command History	Release	Modification
	12.2(25)SW4	This command was introduced.

Usage Guidelines The **si** command is valid in the following table types: mtp-msg-type, sio.

Examples The following example specifies a 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 specifies 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 0, the equivalent of the **no sls-shift** command.

Command Modes

CS7 linkset configuration

Command History

Release	Modification
12.2(1)MB	This command was introduced.

Usage Guidelines

This command is only valid when the variant is ITU. It affects MSUs received on the linkset, and changes which bit in the SLS is used for linkset selection.

It is necessary to be able 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 won't balance evenly.

Examples

The following example specifies 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.

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 the command.

snmp-server enable traps bits-clock

no snmp-server enable traps bits-clock

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Defaults	No default behavior or values.
-----------------	--------------------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.2(25)SW1	This command was introduced.

Usage Guidelines	The snmp-server enable traps bits-clock command provides support for CISCO-BITS-CLOCK-MIB.my
-------------------------	---

Examples	<p>The following example generates notifications to indicate when clocking sources change roles or become unavailable:</p> <pre>snmp-server enable traps bits-clock</pre>
-----------------	---

Related Commands	Command	Description
	snmp-server community	Configures community access string to permit access to the Simple Network Management Protocol protocol.
	snmp-server host	Specifies the recipient of a Simple Network Management Protocol notification operation.

snmp-server enable traps cs7

To enable Simple Network Management Protocol (SNMP) ITP traps to be sent, use the **snmp-server enable traps cs7** global configuration command. To disable the sending of traps, use the **no** form of the command.

```
snmp-server enable traps cs7 [dsmr-smpp-dest] [dsmr-table-load] [dsmr-ucp-dest]
[gtt-map-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] [link-congestion] [link-state]
[link-utilization] [linkset-state] [mlr-table-load] [monitor-congestion] [monitor-state]
[route-state] [xua-state]
```

```
no snmp-server enable traps cs7 [dsmr-smpp-dest] [dsmr-table-load] [dsmr-ucp-dest]
[gtt-map-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] [link-congestion] [link-state]
[link-utilization] [linkset-state] [mlr-table-load] [monitor-congestion] [monitor-state]
[route-state] [xua-state]
```

Syntax Description	
dsmr-smpp-dest	(Optional) Enables the ciscoItpDsmrSmppSessionState notification from the CISCO-ITP-DSMR-SMPP-MIB.my.
dsmr-table-load	(Optional) Enables the ciscoItpDsmrTableLoad notification from the CISCO-ITP-DSMR-MIB.my.
dsmr-ucp-dest	(Optional) Enables the ciscoItpDsmrUCPSessionState notification from the CISCO-ITP-DSMR-UCP-MIB.my.
gtt-map-state	(Optional) 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-state	(Optional) Enables the gateway destination state change trap (ciscoGrtDestStateChange) in CISCO-ITP-GRT-MIB.my.
gw-gtt-errors	(Optional) 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 the cgsccpGttErrorPeriod or when the cgsccpInstErrorIndicator is set to false.
gw-gtt-load	(Optional) Enables the gateway GTT load table trap (ciscoGsccpGttLoadTable) in CISCO-ITP-GSCCP-MIB.my.
gw-isolation	(Optional) Enables the gateway isolation trap (ciscoGspIsolation) in CISCO-ITP-GSP-MIB.my.
gw-link-congestion	(Optional) Enables the gateway link-congestion trap (ciscoGspCongestionChange) in CISCO-ITP-GSP-MIB.my.
gw-link-state	(Optional) Enables the gateway link-state trap (ciscoGspLinkStateChange) in CISCO-ITP-GSP-MIB.my.
gw-link-utilization	(Optional) Enable gateway link-utilization traps (ciscoGspLinkRcvdUtilChange, ciscoGspLinkSentUtilChange) in CISCO-ITP-GSP-MIB.my.
gw-linkset-state	(Optional) Enables the gateway linkset-state trap (ciscoGspLinksetStateChange) in CISCO-ITP-GSP-MIB.my.

gw-map-state	(Optional) Enables gateway Mated Appl (MAP) state trap.
gw-route-load	(Optional) Enables the gateway route table load trap (ciscoGrtRouteTableLoad) in CISCO-ITP-GRT-MIB.my.
gw-route-mgmt-state	(Optional) Enables the gateway route management state change trap (ciscoGrtMgmtStateChange) in CISCO-ITP-GRT-MIB.my.
link-congestion	(Optional) Enables the link-congestion trap (cItpSpCongestionChange) in CISCO-ITP-SP-MIB.my. <i>Deprecated and replaced by gw-link-congestion.</i>
link-state	(Optional) Enables the link-state trap (cItpSpLinkStateChange) in CISCO-ITP-SP-MIB.my. <i>Deprecated and replaced by gw-link-state.</i>
link-utilization	(Optional) Enable link-utilization trap. <i>Deprecated and replaced by gw-link-utilization.</i>
linkset-state	(Optional) Enables the linkset-state trap (cItpSpLinksetStateChange) in CISCO-ITP-SP-MIB.my. <i>Deprecated and replaced by gw-linkset-state.</i>
mlr-table-load	(Optional) Enables the MLRtable 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. This allows MLR tables to be reloaded whenever a device restarts.
monitor-congestion	(Optional) Enables the ciscoItpMonitorCongestion notification in CISCO-ITP-MONITOR-MIB.my.
monitor-state	(Optional) Enables the monitor-state trap in CISCO-ITP-MONITOR-MIB.my. Notification is generated when a connection changes states. The value of cItpmConnMonitorState indicates new state.
route-state	(Optional) Enables the route-state trap (cItpRouteStateChange) in CISCO-ITP-RT-MIB.my. <i>Deprecated and replaced by gw-route-mgmt-state.</i>
xua-state	(Optional) 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

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(1)MB	This command was introduced.
12.2(4)MB	The keywords gtt-map-state , link-utilization , and route-state were added.
12.2(4)MB5	The keyword xua-state was added.
12.2(21)SW	The keyword monitor-congestion was added.
12.2(25)SW	The monitor-state keyword was added.
12.2(25)SW1	The gw-gtt-errors and mlr-table-load keywords were added.
12.2(25)SW3	The dsmr-smpp-dest , dsmr-table-load , dsmr-ucp-dest and gw-isolation keywords were added.

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 enables 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 10 events) to 100 events to reduce the possibility of dropping traps:

```
snmp-server enable traps cs7
snmp community public RO
snmp host 64.102.86.159 version 2c public
snmp-server queue-length 100
```

Related Commands

Command	Description
snmp-server community	Configures community access string to permit access to the Simple Network Management Protocol protocol.
snmp-server host	Specifies the recipient of a Simple Network Management Protocol notification operation.
snmp-server queue-length	Specifies the message queue length for each TRAP host.

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 the command.

snmp-server enable traps sctp [dest-address-state]

no snmp-server enable traps sctp [dest-address-state]

Syntax Description

dest-address-state	Enables destination address state change trap.
---------------------------	--

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(4)MB3	This command was introduced.

Examples

The following example enables the destination address state change trap:

```
snmp-server enable traps sctp dest-address-state
```

Related Commands

Command	Description
snmp-server community	Configures community access string to permit access to the Simple Network Management Protocol protocol.
snmp-server host	Specifies the recipient of a Simple Network Management Protocol notification operation.

sscf-nni

To specify SSCF NNI parameters for the CS7 HSL profile, use the **sscf-nni** CS7 HSL profile commands. To remove the configuration, use the **no** form of the 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 **force-proving** *minutes* is 10 minutes.
 The default **n1** *number* is 1000 (ITU) and 60000 (ANSI).
 The default **no-credit** *seconds* is 100 milliseconds.
 The default **nrp** *number* is 4 retries.
 The default **sscop-recovery** *minutes* is 500 Sd frames.
 The default **t1** *seconds* is 1500 milliseconds.
 The default **t2** *seconds* is 100 milliseconds.
 The default **t3** *milliseconds* is 1024 frames.

Command Modes

CS7 HSL profile, CS7 linkset

Command History

Release	Modification
12.2(4)MB4	This command was introduced.

Usage Guidelines

SSCF NNI parameters can be configured in either a CS7 HSL profile or individually under a link.

sscop

To specify SSCOP parameters for the CS7 HSL profile, use the **sscop** CS7 HSL profile commands. To remove the configuration, use the **no** form of the 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 our 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 frames. The default is 1024 frames.

Defaults

The default cc-timer is 200 milliseconds.

The default idle-timer is 100 milliseconds.

The default keepalive-timer is 100 milliseconds.

The default max-cc is 4 retries.

The default max-pd is 500 Sd frames.

The default noResponse-timer is 1500 milliseconds.

The default poll-timer is 100 milliseconds.

The default receive-window is 1024 frames.

The default send-sindow is 1024 frames.

Command Modes CS7 HSL profile, CS7 linkset

Command History	Release	Modification
	12.2(4)MB4	This command was introduced.

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** CS7 MLR ruleset configuration mode command. To remove the configuration, use the **no** form of the command.

teleservice *id*

no teleservice

Syntax Description	<i>id</i>	An integer in the range 0 to 65535.
Defaults	No default behavior or values.	
Command Modes	CS7 MLR ruleset	
Command History	Release	Modification
	12.2(21)SW	This command was introduced.
Usage Guidelines	The value of the teleservice maps to the values specified for the SMS TeleserviceIdentifier parameter in IS-41.	
Examples	The following example sets the teleservice id to 500: <pre>teleservice 500</pre>	
Related Commands	Command	Description
	cs7 mlr ruleset	Specifies a set of rules that will be used to process traffic matching triggers defined in an MLR table.

threshold-receive

To configure the receive threshold for a link, use the **threshold-receive** CS7 link submode command. To remove the configuration, use the **no** form of the command.

threshold-receive *percent*

no threshold-receive *percent*

Syntax Description	<i>percent</i>	Receive threshold for trap generation in percent. The range is 0 to 100 percent.
--------------------	----------------	--

Defaults	The range defaults to the value specified by the cs7 util-threshold global command.
----------	--

Command Modes	CS7 link submode
---------------	------------------

Command History	Release	Modification
	12.2(4)MB4	This command was introduced.

Usage Guidelines	This value is only required when the value specified by the cs7 util-threshold global command is not appropriate for a particular link.
------------------	--

Examples	The following example sets 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-receive 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 the command.

threshold-send *percent*

no threshold-send *percent*

Syntax Description	<i>percent</i>	Send threshold for trap generation in percent. The range is 0 to 100 percent.
---------------------------	----------------	---

Defaults	The range defaults to the value specified by the cs7 util-threshold global command.
-----------------	--

Command Modes	CS7 link submode
----------------------	------------------

Command History	Release	Modification
	12.2(4)MB4	This command was introduced.

Usage Guidelines	This value is only required when the value specified by the cs7 util-threshold global command is not appropriate for a particular link.
-------------------------	--

Examples	The following example sets 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-receive	Specifies the receive threshold for a link.

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 the 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 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 hs-mtp2 profile

Command History	Release	Modification
	12.2(25)SW5	This command was introduced.

Usage Guidelines High speed MTP2 parameters can also be specified in CS7 Linkset configuration mode.

Examples The following example defines a profile named TIMER, configures the profile to support high speed MTP2, configures the t1 and t2 settings in the TIMERS profile, then applies the profile to all the links in linkset 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	Define a profile of MTP2 parameters that you can apply to all 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-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 | 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 ANSI or ITU defined.

Syntax Description

retry msec	(ANSI, ITU) Link activation retry timer. (ANSI, ITU) Range of msec is 60000 through 90000 milliseconds. Default is 60000 milliseconds.
slt-t1 msec	(ANSI, ITU) Link test acknowledgment timer. (ANSI, ITU) ITU Range of msec is 4000 through 12000 milliseconds. Default is 8000 milliseconds.
slt-t2 msec	(ANSI, ITU) Interval timer for sending test messages. (ANSI, ITU) Range of msec is 30000 through 90000 milliseconds. (ANSI, ITU) Default is 60000 milliseconds.
t01 msec	(ANSI, ITU) Delay to avoid message mis-sequencing. (ANSI, ITU) Range of msec is 500 through 1200 milliseconds. (ANSI, ITU) Default is 800 milliseconds.
t02 msec	(ANSI, ITU) Wait for changeover acknowledgment. (ANSI, ITU) Range of msec is 700 through 2000 milliseconds. (ANSI, ITU) Default is 1400 milliseconds.
t03 msec	(ANSI, ITU) Delay to avoid mis-sequencing in changeback. (ANSI, ITU) Range of msec is 500 through 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 through 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 through 1200 milliseconds. (ANSI, ITU) Default is 800 milliseconds.
t12 msec	(ANSI, ITU) Wait for uninhibited acknowledgment. (ANSI, ITU) Range of msec is 800 through 1500 milliseconds. (ANSI, ITU) Default is 1150 milliseconds.
t13 msec	(ANSI, ITU) Wait for force uninhibited. (ANSI, ITU) Range of msec is 800 through 1500 milliseconds. (ANSI, ITU) Default is 1150 milliseconds.

t14 msec	(ANSI, ITU) Wait for inhibition acknowledgment. (ANSI, ITU) Range of <i>msec</i> is 2000 through 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 through 1500 milliseconds. (ANSI, ITU) Default is 1150 milliseconds.
t19 msec	(ANSI) Failed link craft referral timer. (ANSI) Range of <i>msec</i> is 480000 through 600000 milliseconds. (ANSI) Default is 540000. (ITU) Supervision timer during MTP restart. (ITU) Range of <i>msec</i> is 67000 through 69000 milliseconds. (ITU) Default is 68000 milliseconds.
t20 msec	(ANSI) Waiting to repeat local inhibit test. (ANSI) Range of <i>msec</i> is 90000 through 120000 milliseconds. (ANSI) Default is 105000 milliseconds.
t21 msec	(ANSI) Waiting to repeat remote inhibit test. (ANSI) Range of <i>msec</i> is 90000 through 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 through 65000 milliseconds. (ITU) Default is 64000 milliseconds.
t22 msec	(ITU) Local inhibit test timer. (ITU) Range of <i>msec</i> is 180000 through 360000 milliseconds. (ITU) Default is 300000 milliseconds.
t23 msec	(ITU) Remote inhibit test timer. (ITU) Range of <i>msec</i> is 180000 through 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 through 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 through 35000 milliseconds. (ANSI) Default is 30000 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 through 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 through 65000 milliseconds. (ANSI) Default is 63000 milliseconds.

■ timer (cs7 linkset)

t30 <i>msec</i>	(ANSI) Timer to limit sending TFPs and TFRs in response to unexpected TRA and TRW. (ANSI) Range of <i>msec</i> is 30000 through 35000 milliseconds. (ANSI) Default is 33000 milliseconds.
t32 <i>msec</i>	(ANSI) Link oscillation timer - Procedure A. Range of <i>msec</i> is 60000 through 120000 milliseconds. Default is 60000 milliseconds.

Defaults

See defaults listed in Syntax Description.

Command Modes

CS7 linkset submode

Command History

Release	Modification
12.2(1)MB	This command was introduced.

Usage Guidelines

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.

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 will override any global values.

All 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.

Examples

The following example sets 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** CS7 profile configuration command. To reset the timers, use the **no** form of the 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 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	<p>ttc ta timer: TTC Timer for sending SIE. Valid range is 10 to 250 milliseconds. Default is 20 milliseconds.</p> <p>ttc te timer: TTC Timer for error monitoring. Valid range is 10 to 250 milliseconds. Default is 20 milliseconds.</p> <p>ttc tf timer: TTC Timer for sending FISU. Valid range is 10 to 250 milliseconds. Default is 20 milliseconds.</p> <p>ttc to timer: TTC Timer for sending SIO. Valid range is 10 to 250 milliseconds. Default is 20 milliseconds.</p> <p>ttc ts timer: TTC Timer for sending SIOS. Valid range is 10 to 250 milliseconds. Default is 20 milliseconds.</p>

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

Command History

Release	Modification
12.2(4)MB	This command was introduced.

Usage Guidelines

MTP2 parameters can also be specified in CS7 Linkset configuration mode.

Examples

The following example defines a profile named timers, configures the profile to support MTP2, configures the t1 and t2 settings in the timers profile, then applies the timers profile to all the links in linkset 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	Define a profile of MTP2 parameters that you can apply to all links in a linkset.
show cs7 mtp2	Displays ITP MTP2 status.
tx-queue-depth (cs7 link)	Configures the MTP2 transmit queue depth.

traffic-mode

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** | **roundrobin**] | **override** }

no traffic-mode { **broadcast** | **loadshare** [**bindings** | **roundrobin**] | **override** }

Syntax Description		
broadcast		Broadcast mode. In broadcast mode, the ASP will receive 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. The user can loadshare based on ASP bindings or using a roundrobin algorithm.
bindings		Loadshare based on ASP bindings. (Default)
roundrobin		Loadshare based on roundrobin.
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 Loadshare based on ASP bindings.

Command Modes CS7 AS submode.

Command History	Release	Modification
	12.2(4)MB5	This command was introduced.

Usage Guidelines This command is used to validate the traffic mode specified on the ASP Active messages. ASPs connecting with a different traffic mode will be failed.

The traffic mode type supported by an AS is dynamically determined as follows. The traffic mode of the AS is set to **loadshare** if the first valid ASP Active message received from an ASP in the AS has the traffic mode type set to **loadshare**.

Examples The following example sets the traffic-mode to loadshare mode:

```
cs7 as BLUE m3ua
  routing-key 100 10.3.8
  asp ASP1
  asp ASP2
  traffic-mode loadshare
```

Related Commands	Command	Description
	cs7 as	Defines an Application Server and enters CS7 AS submode.
	cs7 asp	Specifies an Application Server Process 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.

trigger cdpa (cs7 mlr table)

To specify the routing key, or trigger, for a Multi-layer 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** CS7 MLR table mode command. To delete the trigger command and disable the 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 asname | gt gta [gt-addr-type] | group
group-name}]
```

```
no trigger cdpa
```

Syntax Description	
gt	Indicates that the CdPA trigger being defined is received with RI=GT.
selector	Specifies that the trigger will be matched based on a global title selector value.
<i>addr-string</i>	Address string of 1 to 15 hexadecimal characters. The string is not input in BCD-String format, but in normal form.
<i>gt-addr-type</i>	<p>(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.</p> <pre>tt <i>tt</i> [gti <i>gti</i>] [np <i>np</i> nai <i>nai</i>]</pre> <p>tt Identifies the translation type specified within the address.</p> <p><i>tt</i> An integer value from 0 to 255.</p> <p>gti Identifies the global title indicator value for the specified address. This value is only specified when the CS7 variant is ITU or China.</p> <p><i>gti</i> Integer value of 2 or 4.</p> <p>np Identifies the numbering plan of the specified address. Only specified when the <i>gti</i> parameter value is 4.</p> <p><i>np</i> Integer value from 0 to 15.</p> <p>nai Identifies the nature of specified address. Only specified when the <i>gti</i> parameter value is 4.</p> <p><i>nai</i> Integer value from 0 to 127.</p>
pc	Specifies that the trigger will be matched if it contains the specified point code. The PC within the SCCP CdPA will be inspected first. If the PC is not present, then the DPC in the routing label is used.
<i>point-code</i>	The point code in variant-specific point-code format.
ssn	Specifies that the trigger will be matched if it contains the specified subsystem.
<i>ssn</i>	Subsystem number in decimal. Valid range is 2 to 255.
block	(Optional) This trigger action specifies that messages matching this trigger should be dropped. The block parameter is ignored if combination triggers are defined within the CS7 MLR trigger configuration submode.

continue	(Optional) This trigger action specifies that messages matching this trigger should be routed as received. This is the same behavior that would occur if no primary trigger had been matched. The continue parameter is ignored if combination triggers are defined within the CS7 MLR trigger mode.
ruleset	(Optional) This trigger action specifies the MLR ruleset table that should be used if this trigger is matched and not overruled by a secondary trigger ruleset. Ruleset is ignored if combination triggers are defined within the 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	(Optional) This trigger action 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 simply redirected as indicated in the trigger result. Note: Result groups with dest-sme-binding mode are not valid trigger results.
pc	Route based on point code.
<i>pc</i>	Point code
ssn	(Optional) Route based on PC and subsystem number.
<i>ssn</i>	Subsystem number.
asname	Route based on AS name.
<i>asname</i>	AS name.
gt	Route based on Global Title.
<i>gta</i>	Global title address.
group	Route based on result group.
<i>group-name</i>	Result group name.

Defaults

If a **default** trigger is configured, it is defined as the last trigger in the MLR table. The **default** trigger will be used only if all other triggers are unmatched. If a **default** trigger is not configured, then packets not matching a trigger will be routed according to standard SCCP or MTP3 procedures.

Command Modes

CS7 MLR table

Command History

Release	Modification
12.2(4)MB	This command was introduced.
12.2(21)SW	The continue trigger action was added.
12.2(25)SW3	The selector trigger action was added.
12.2(25)SW4	The result trigger action was added.

Usage Guidelines

Use the **trigger cdpa** command to configure a primary routing key that will be used to route or block messages based on the CdPA. (If no primary triggers are specified, creation of the MLR table will fail.)

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 default trigger is defined (the only trigger configured).
2. SCCP CdPA GT address
3. SCCP CdPA GT selector
4. SCCP CdPA PC/SSN
5. SCCP CgPA GTaddress
6. SCCP CgPA GT selector
7. SCCP CgPA PC/SSN

Trigger Terminology

[Table 71](#) describes types of triggers and the commands you use to specify triggers at various configuration levels.

Table 74 **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	<p>The primary trigger represents the network layer information that is first compared to an incoming packet for possible MLR routing.</p> <p>A primary trigger is specified in CS7 MLR table mode (after the cs7 mlr table command has been specified).</p> <p>The following example shows the command to specify a primary trigger. (Note that the CLI prompt changes to indicate that CL7 MLR trigger mode has been enabled.)</p> <pre>Router(config-cs7 mlr)# trigger mtp3 dpc 1-1-1 Router(cfg-cs7-mlr-trigger)#</pre> <p>Primary trigger values must be unique.</p> <p>Possible primary trigger commands are trigger cdpa, trigger cgpa, trigger default, and trigger mtp3.</p> <p>MTP3 may be specified as a primary trigger only.</p>

Table 74 **Trigger Terminology (continued)**

secondary trigger	<p>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 AND 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.</p> <p>The following example shows the command to specify a secondary trigger. Note that configuring a secondary trigger does not enable a new mode. The prompt does not change.</p> <pre>Router(cfg-cs7-mlr-trigger)# cgpa pc 1-1-1 ssn 11 Router(cfg-cs7-mlr-trigger)#</pre> <p>Secondary triggers need not be unique.</p> <p>Possible secondary trigger commands are cdpa, cgpa, and default.</p> <p>The primary trigger must be for a called party for the cgpa submode command to be valid.</p> <p>The primary trigger must be for a calling party for the cdpa submode command to be valid.</p>
tertiary trigger	<p>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 AND 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.</p> <p>The following example shows the command to specify a tertiary trigger. Note that configuring a tertiary trigger does not enable a new mode. The prompt does not change</p> <pre>Router(cfg-cs7-mlr-trigger)#cgpa pc 2-2-2 ssn 8</pre> <p>Tertiary triggers need not be unique.</p> <p>Possible tertiary trigger commands are cdpa, cgpa, and default.</p>
subtrigger	<p>A subtrigger is a generic term used to describe a trigger defined within another trigger's submode. A default trigger cannot have subtriggers.</p>
combination trigger	<p>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.</p>

Examples

The following example specifies 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 configures triggers to block messages based on 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 multi-layer SMS routing table and enables CS7 MLR table mode.
trigger cgpa	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 Multi-layer 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** CS7 MLR table mode command. 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 asname | 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 not input in BCD-String format, but in normal form.
<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 only specified 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. Only specified when the <i>gti</i> parameter value is 4. <i>np</i> Integer value from 0 to 15. nai Identifies the nature of specified address. Only specified when the <i>gti</i> parameter value is 4. <i>nai</i> Integer value from 0 to 127.
pc	Specifies that the trigger will be matched if it contains the specified point code. The PC within the SCCP CgPA will be inspected first. If the PC is not present, then the OPC is used.
<i>point-code</i>	The point code in variant-specific point-code format.
ssn	Specifies that the trigger will be matched if it contains the specified subsystem.
<i>ssn</i>	Subsystem number in decimal. Valid range is 2 to 255.
block	(Optional) This trigger action specifies that messages matching this trigger should be dropped. The block parameter is ignored if combination triggers are defined within the CS7 MLR trigger configuration submode.

continue	(Optional) This trigger action specifies that messages matching this trigger should be routed as received. This is the same behavior that would occur if no primary trigger had been matched. The continue parameter is ignored if combination triggers are defined within the CS7 MLR trigger mode.
ruleset	(Optional) This trigger action specifies the MLR ruleset table that should be used if this trigger is matched and not overruled by a secondary trigger ruleset. Ruleset is ignored if combination triggers are defined within the 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	(Optional) This trigger action 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 simply redirected as indicated in the trigger result. Note: Result groups with dest-sme-binding mode are not valid trigger results.
pc	Route based on point code.
<i>pc</i>	Point code
ssn	(Optional) Route based on PC and subsystem number.
<i>ssn</i>	Subsystem number.
asname	Route based on AS name.
<i>asname</i>	AS name.
gt	Route based on Global Title.
<i>gta</i>	Global title address.
group	Route based on result group.
<i>group-name</i>	Result group name.

Defaults

If a **default** trigger is configured, it is defined as the last trigger in the MLR table. The **default** trigger will be used only if all other triggers are unmatched. If a **default** trigger is not configured, then packets not matching a trigger will be routed according to standard SCCP or MTP3 procedures.

Command Modes

CS7 MLR table

Command History

Release	Modification
12.2(4)MB	This command was introduced.
12.2(21)SW	The continue trigger action was added.
12.2(25)SW3	The selector trigger action was added.
12.2(25)SW4	The result trigger action was added.

Usage Guidelines

Use the **trigger cgpa** command to configure a primary routing key that will be used to route or block messages based on the CgPA. (If no primary triggers are specified, creation of the MLR table will fail.)

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 default trigger is defined (the only trigger configured).
2. SCCP CdPA GT address
3. SCCP CdPA GT selector
4. SCCP CdPA PC/SSN
5. SCCP CgPA GTaddress
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 specifies 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 configures triggers to block messages based on 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 multi-layer SMS routing table and enables CS7 MLR table mode.
default	Creates a trigger to be used if all other subtriggers are unmatched.
trigger cdpa	Specifies a primary routing trigger that is located in the SCCP CdPA field of the incoming MSU.

trigger default

To specify that the trigger matches all packets received, use the **trigger default** CS7 MLR table mode command. To delete the trigger command and disable the specific routing trigger, use the **no** form of this command

```
trigger default [block | continue | ruleset ruleset-name] | result { pc pc [ssn ssn] | asname asname
| gt gta [gt-addr-type] | group group-name]
```

```
no trigger default
```

Syntax Description	
block	(Optional) This optional trigger-action specifies that messages matching this trigger should be dropped. The block parameter is ignored if combination triggers are defined within the CS7 MLR trigger mode.
continue	(Optional) This optional trigger-action specifies that messages matching this trigger should be routed as received. This is the same behavior as if no primary trigger had been matched. The continue parameter is ignored if combination triggers are defined within the CS7 MLR trigger mode.
ruleset	(Optional) This optional trigger-action specifies the MLR ruleset table that should be used if this trigger is matched and not overruled by a secondary trigger ruleset. Ruleset is ignored if combination triggers are defined within the 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	(Optional) This trigger action 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 simply redirected as indicated in the trigger result. Note: Result groups with dest-sme-binding mode are not valid trigger results.
pc	Route based on point code.
<i>pc</i>	Point code
ssn	(Optional) Route based on PC and subsystem number.
<i>ssn</i>	Subsystem number.
asname	Route based on AS name.
<i>asname</i>	AS name.
gt	Route based on Global Title.
<i>gta</i>	Global title address.
group	Route based on result group.
<i>group-name</i>	Result group name.

Defaults

No default behavior or value.

Command Modes CS7 MLR table

Command History

Release	Modification
12.2(4)MB	This command was introduced.
12.2(21)SW	The continue keyword was added.
12.2(25)SW4	The result trigger action was added.

Usage Guidelines

The **trigger default** command enables the CS7 MLR trigger mode.

Examples

The following example specifies that the trigger matches 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 multi-layer SMS routing table and enables CS7 MLR table mode.

trigger mtp3

To specify the routing key, or trigger, for a Multi-layer 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] | asname asname | gt gta [gt-addr-type] | group
group-name}]
```

no trigger mtp3

Syntax Description	
dpc	Indicates that the trigger is found 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	Specifies that the trigger is found 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 in the range of 3 to 15.
block	(Optional) This trigger action specifies that messages matching this trigger should be dropped. The block parameter is ignored if combination triggers are defined within the CS7 MLR trigger configuration submode.
continue	(Optional) This trigger action specifies that messages matching this trigger should be routed as received. This is the same behavior that would occur if no primary trigger had been matched. The continue parameter is ignored if combination triggers are defined within the CS7 MLR trigger mode.
ruleset	(Optional) This trigger action specifies the MLR ruleset table that should be used if this trigger is matched and not overruled by a secondary trigger ruleset. Ruleset is ignored if combination triggers are defined within the 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	(Optional) This trigger action 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 simply redirected as indicated in the trigger result. Note: Result groups with dest-sme-binding mode are not valid trigger results.
pc	Route based on point code.
<i>pc</i>	Point code
ssn	(Optional) Route based on PC and subsystem number.
<i>ssn</i>	Subsystem number.
asname	Route based on AS name.
<i>asname</i>	AS name.

■ trigger mtp3

gt	Route based on Global Title.
<i>gta</i>	Global title address.
group	Route based on result group.
<i>group-name</i>	Result group name.

Defaults

No default behavior or value.

Command Modes

CS7 MLR table

Command History

Release	Modification
12.2(21)SW	This command was introduced.
12.2(25)SW4	The result trigger action was added.

Usage Guidelines

The **trigger mtp3** command enables the CS7 MLR trigger mode.

Examples

The following example specifies 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 configures triggers to block messages based on 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 multi-layer 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.

tmap

TT mapping rules can be added to existing linksets. To add a rule, use the **tmap** CS7 linkset submode command. To remove a TT map rule, use the **no** form of this command.

tmap *existing_tt mapped_tt*

no tmap *existing_tt mapped_tt*

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.

Defaults	No default behavior or values
-----------------	-------------------------------

Command Modes	CS7 linkset submode
----------------------	---------------------

Command History	Release	Modification
	12.2(4)MB	This command was introduced.
	12.2(25)SW3	Prior to 12.2(25)SW3, linkset based TT mapping was supported for ANSI linksets only. With 12.2(25)SW3, TT mapping is available for all variants. The valid range of <i>existing_tt</i> and <i>mapped_tt</i> was changed. The old range was 1 to 255. The new range is 0 to 255.

Usage Guidelines	This command is available for all variants.
-------------------------	---

Examples	The following example adds a rule that maps all incoming messages that have a TT=6 to now have a TT=254:
-----------------	--

```
cs7 linkset to_doc
  tmap 6 254 in
```

Related Commands	Command	Description
	show cs7 linkset tmap	Displays TT mapping rules for the linkset.

tt-range

To specify the 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-set** *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>	(Optional) Ending pc in the range.
gti	(Optional) Identifies the global title indicator for the specified address. This value is only specified 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. Only configured when the gti parameter value is 4.
<i>np</i>	Integer in the range 0 through 15.
nai	(Optional) Identifies the nature of the specified address. Configured only when the gti parameter value is 4.
<i>nai</i>	Integer in the range 0 through 127.
result	Specifies the next step.
action	Specifies that the default result will be to screen by action set.
<i>action-set-name</i>	Action set name. Valid names may not exceed 12 alpha numeric characters.
table	Specifies that the default result will be to screen by table.
<i>table-name</i>	Table name. Valid names may not exceed 12 alpha numeric characters.

Defaults

No default behavior or values.

Command Modes

Gateway screening table configuration

Command History

Release	Modification
12.2(25)SW4	This command was introduced.

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 specifies 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 through 20000 packets. The default is the value specified under the local port instance.
--------------------	--------------	---

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(4)MB5	This command was introduced.

Examples	The following example sets 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 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** CS7 hs-mtp2 profile configuration 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 250 to 50000 packets.	
Defaults	5000 packets	
Command Modes	CS7 hs-mtp2 profile configuration	
Command History	Release	Modification
	12.2(25)SW5	This command was introduced.
Usage Guidelines	<p>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 link congestion, the tx-queue-depth will control the number of packets that can be queued before packets are discarded, causing application retransmissions.</p>	
Examples	<p>The following example defines a profile named HSMTP2, specifies that the profile supports high speed MTP2, specifies the tx-queue-depth parameter in the profile, then applies the HSMTP2 profile to all the links in linkset named TO_NYC:</p> <pre> cs7 profile HSMTP2 hs-mtp2 tx-queue-depth 2000 . . . cs7 linkset TO_NYC profile HSMTP2 </pre>	
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 *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. 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 submode

Command History

Release	Modification
12.2(1)MB	This command was introduced.
12.2(25)SW5	This timer was added for high speed MTP2 links.

Usage Guidelines

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 link congestion, the tx-queue-depth will control the number of packets that can be queued before packets are discarded, causing application retransmissions.

Examples

The following example sets 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** CS7 link 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 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(25)SW3	This command was introduced.

Usage Guidelines	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 link congestion, the tx-queue-depth will control the number of packets that can be queued before packets are discarded, causing application retransmissions.
------------------	--

Examples	The following example defines a profile named m2parfc, specifies that the profile supports M2PA RFC, specifies the tx-queue-depth parameter in the profile, then applies the m2parfc profile to all the links in linkset named to_nyc:
----------	---

```
cs7 profile m2parfc
  m2pa
  tx-queue-depth 2000
.
.
.
cs7 linkset to_nyc
  profile m2parfc
```


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	<i>queue-depth</i>	Number of packets to be queued. The range is 100 through 20000 packets. The default is 1000 packets.
--------------------	--------------------	--

Defaults	1000 packets.
----------	---------------

Command Modes	CS7 M3UA submode
---------------	------------------

Command History	Release	Modification
	12.2(4)MB5	This command was introduced.

Examples	The following example sets 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 through 20000 packets. The default is the value specified under the local port instance.
---------------------------	--------------------	---

Defaults	The default is the value specified under the local port instance.
-----------------	---

Command Modes	CS7 Mated-SG submode
----------------------	----------------------

Command History	Release	Modification
	12.2(4)MB5	This command was introduced.

Examples	The following example sets the transmit queue depth to 2000 packets:
-----------------	--

```
cs7 mated-sg BLUE 5000
tx-queue-depth 2000
```

Related Commands	Command	Description
	cs7 mated-sg	Establish an association to the mated SG and enters CS7 Mated SG submode.

tx-queue-depth (cs7 profile)

To configure the MTP2 maximum transmit queue depth in a CS7 MTP2 profile, use the **tx-queue-depth** CS7 MTP2 profile configuration 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 25 through 5000 packets.
--------------------	--------------------	---

Defaults	The default is the value specified under the local port instance.
----------	---

Command Modes	CS7 MTP2 profile
---------------	------------------

Command History	Release	Modification
	12.2(4)MB5	This command was introduced.

Examples	The following example defines a profile named timers, configures the profile to support MTP2, configures the tx-queue-depth to 3000 packets, then applies the timers profile to all the links in linkset 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 through 20000 packets. The default is 1000 packets.
---------------------------	--------------------	--

Defaults	1000 packets.
-----------------	---------------

Command Modes	CS7 SGMP submode
----------------------	------------------

Command History	Release	Modification
	12.2(4)MB5	This command was introduced.

Examples	The following example sets the transmit queue depth to 2000 packets:
-----------------	--

```
cs7 sgmp 5000
tx-queue-depth 2000
```

Related Commands	Command	Description
	cs7 sgmp	Establish 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 through 20000 packets. The default is 1000 packets.
--------------------	--------------------	--

Defaults	1000 packets.
----------	---------------

Command Modes	CS7 SUA submode
---------------	-----------------

Command History	Release	Modification
	12.2(4)MB5	This command was introduced.

Examples	The following example sets 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.

unordered-priority (cs7 m3ua)

To configure the priority of the 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 delivered in the order received.
----------	--

Command Modes	CS7 M3UA
---------------	----------

Command History	Release	Modification
	12.2(4)MB5	This command was introduced.

Examples	<p>The following example specifies that unordered packets are delivered before any sequenced data:</p> <pre>cs7 m3ua 2905 unordered-priority high</pre>
----------	--

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 the 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 delivered in the order received.

Command Modes

CS7 SGMP

Command History

Release	Modification
12.2(4)MB5	This command was introduced.

Examples

The following example specifies that unordered packets are delivered in the order received:

```
cs7 sgmp 5000
 unordered-priority equal
```

Related Commands

Command	Description
cs7 sgmp	Establish an association to the mated signaling gateway and enters CS7 SGMP submode.

unordered-priority (cs7 sua)

To configure the priority of the 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 delivered in the order received.
----------	--

Command Modes	CS7 SUA
---------------	---------

Command History	Release	Modification
	12.2(4)MB5	This command was introduced.

Examples	<p>The following example specifies that unordered packets are delivered before any sequenced data:</p> <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

To enable unrouteable 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	No default behavior or values
-----------------	-------------------------------

Command Modes	CS7 linkset configuration
----------------------	---------------------------

Command History	Release	Modification
	12.2(25)SW	This command was introduced.

Examples	The following example enables unrouteable accounting in linkset1:
-----------------	---

```
cs7 linkset linkset1 2.2.2
unrouteable-accounting
```

Related Commands	Command	Description
	clear cs7 accounting	Clears unrouteable database.
	cs7 accounting global-unrouteable	Enables unrouteable accounting on all linksets.
	show cs7 accounting unrouteable	Displays accounting information about unroutable packets.

update (cs7 gtt address conversion)

To add, remove, or change a GTT address-conversion entry, use the **update in-address** 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*]

no update [**in-address** *in-address*] [**nai** *nai*] [**np** *np*] [**out-address** *out-address*] [**es** *es-val*]

Syntax Description

in-address	(Optional) Specifies the input address.
<i>in-address</i>	SCCP address. Valid numbers are between one and 15 digits long, in hex.
nai	(Optional) Specifies a new nature of address indicator.
<i>nai</i>	NAI value. Range is 0 through 127.
np	(Optional) Specifies a new numbering plan.
<i>np</i>	NP value. Range is 0 through 15.
out-address	(Optional) Specifies the output address.
<i>out-address</i>	SCCP address. Valid numbers are between one and 15 digits long, in hex.
es	(Optional) Specifies a specific encoding scheme for the address conversion result.
<i>es-val</i>	Encoding scheme value. Valid range is 0 through 2. 0 = unknown encoding scheme. 1 = bcd odd encoding scheme. 2 = bcd even encoding scheme.

Defaults

No default behavior or values

Command Modes

CS7 GTT address conversion submode

Command History

Release	Modification
12.2(4)MB2	This command was introduced.
12.2(25)SW1	The es keyword was added.

Examples

The following example specifies a new input address of 410123:

```
update in-address 410123
```

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	(Optional) Input GTI.
<i>gti-in</i>	Valid values are 2, 4
tt-in	(Optional) Input TT.
<i>tt-in</i>	Valid range 0 to 255. All TT match if not specified.
ssn-in	(Optional) Input SSN.
<i>ssn-in</i>	Valid range 0 to 255. All SSN match if not specified.
es-in	(Optional) 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	(Optional) 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	(Optional) 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	(Optional) Valid values are 2, 4.
<i>gti-out</i>	Valid values are 2, 4.
tt-out	Output TT.
<i>tt-out</i>	Valid range 0 to 255. TT unchanged if not specified.
ssn-out	(Optional) Output SSN.
<i>ssn-out</i>	Valid range 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.

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 per instance conversion rule.
<i>addr-conv</i>	Address conversion table name.

Defaults

No default behavior or values

Command Modes

CS7 SCCP GTI Conversion submode

Command History

Release	Modification
12.2(20)SW	This command was introduced.

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. The user specifies 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 converts all MSUs with GTI 2 to GTI 4 and sets the Encoding Scheme to 2, Numbering Plan to 1, and Nature of Address to 3, while leaving the TT, and SSN unchanged:

```
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*]

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 would be /24. For ITU the alternate specification of the default would be /14.
linkset	Specifies the linkset.
<i>ls-name</i>	Name of the previously created linkset.
priority	(Optional) Configure route priority.
<i>priority-value</i>	Priority of the route to the destination. Valid range is 1 through 9. The default is 5. The smaller the number the higher the priority. Two routes to the same destination using two different linksets but equal priority form a combined linkset.
qos-class	(Optional) Specifies the QoS class assigned to the destination.
<i>class</i>	QoS class. Valid range is 1 through 7.

Defaults

The default *priority-value* is 5.

Command Modes

Route-table submode

Command History

Release	Modification
12.2(1)MB	This command was introduced.

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 in the *priority-value* means the route has a higher priority.

Use of priority value 9 is not recommend. 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 is assigned on a destination point code basis. 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 the 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 will be changed to the default priority of 5.

Examples

The following two examples are both acceptable ways to create a route to destination 1.50.2 using linkset nyc and default priority:

```
update route 1.50.2 255.255.255 linkset nyc
```

```
update route 1.50.2/24 linkset nyc
```

The following example creates 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 creates 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 creates 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 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 it is important to note that if the qos-class 3 parameter was omitted from alternate route LSC, qos functionality would be disabled for destination 1.50.3. If some other qos-class was specified on the alternate route LSC instead of qos-class 3, the qos-class specified on alternate route LSC would be assigned to both the primary route LSA and the 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 it is important to note that if the priority 3 parameter is omitted when adding the qos-class 2 parameter, the priority of the route will be changed to the default priority of 5.

Related Commands

Command	Description
cs7 route-table	Specifies a route table for an instance.
show cs7 route	Displays the ITP routing table.

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 the 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.

Defaults

No default behavior or values

Command Modes

CS7 profile configuration

Command History

Release	Modification
12.2(4)MB	This command was introduced.

Examples

The following example indicates 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 links in a linkset.
hsl	Configure 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 the command.

variant jt1

no variant jt1

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Controller configuration

Command History

Release	Modification
12.2(25)SW6	This command was introduced.

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 Impedence	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 enables 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.



ITP Debug Commands

- `debug cs7 gws`
- `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 sgmp`
- `debug cs7 snmp`
- `debug cs7 sua`
- `debug cs7 tcap`



Note

Enabling debugging during periods of heavy traffic can cause link failure.

debug cs7 gws

To display debug information for 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	(Optional) Display detailed packet tracing.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

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 Technical Assistance Center.

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(1)MB	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(4)MB5	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(4)MB	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(1)MB	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

<i>error</i>	<ul style="list-style-type: none"> • all All management events • llsc Link Set Control • lsac Link Activity Control • lsda Data Link Allocation • lsla Link Activation • lslr Link Restoration • rca 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 • sr All Route Management errors • stm All Traffic Management errors • tc Changeback Control • tcoc Changeover Control • tcrc Controlled Rerouting Control • tfrc Forced Rerouting Control • tlac Link Availability Control • tp Signaling Point Restart • trcc Signaling Route Congestion Control • tsfc Signaling Traffic Control • tsrc Signaling Routing Control
event	MTP3 MGMT events.

<i>event</i>	<ul style="list-style-type: none"> • 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(1)MB	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>	(Optional) An existing CS7 linkset for which packet debugging is intended. If no linkset is specified packet debugging is implemented on all linksets.
incoming	(Optional) Perform debugging on incoming MSUs. If neither incoming nor outgoing is specified, debugging is performed on both incoming and outgoing MSUs.
outgoing	(Optional) 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>	(Optional) 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	(Optional) 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(4)MB	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	(Optional) 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	(Optional) 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: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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 • SUA-API • TCAP-API
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 sgmp

To display debug messages for SGMP, use the **debug cs7 sgmp** EXEC command.

debug cs7 sgmp {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	SGMP Events
mgmt	Management events.
packet	SGMP packet tracing to the mated SG.
sctp	SGMP SCTP API events for the mated SG.
state	SGMP management state machine events.
timers	SGMP timer events.

Defaults

No default behavior or values.

Command History

Release	Modification
12.2(4)MB5	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(4)MB5	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(4)MB7	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-SCCPPCUNAV: 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.

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](#)
- [CS7ADDRBL Messages](#)
- [CS7CDR Messages](#)
- [CS7CHKPT Messages](#)
- [CS7GROUP Messages](#)
- [CS7HSL Messages](#)
- [CS7M2PA Messages](#)
- [CS7MAPUA Messages](#)
- [CS7MLR Messages](#)
- [CS7MONITOR 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-CDRSERQFULL: 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-SYCNFAILURE: 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.

CS7MAPUA Messages

Error Message

%CS7MAPUA-5-AUTHNOCLIENT: Client ([IP_address]:[dec]) unavailable for authentication

Explanation An authentication request failed because a map client defined with the ip and port could not be found.

Recommended Action Verify the client is defined with the correct ip and port parameters.

Error Message

%CS7MAPUA-5-AUTHREQNOATTR: Authen request for client ([IP_address]:[dec]) missing ([chars]) attribute

Explanation An authentication request failed because the request was missing required attributes.

Recommended Action Verify the sender of the authentication request supports the required attributes.

Error Message

%CS7MAPUA-5-AUTHREQPAKDROPP: Authentication request packet dropped for ip = [IP_address] port = [dec]

Explanation An authentication request was dropped because a map user defined with the ip and port could not be found or the map user is shutdown.

Recommended Action Verify the map user is defined with the correct ip and port parameters. Verify the map user is not shutdown.

Error Message

%CS7MAPUA-5-AUTHRESPDROPP: Authentication response dropped, bad [chars] descriptor

Explanation An authentication response was dropped because the descriptor associated with the authentication response was invalid

Recommended Action This problem could be caused by the deleting of the map user while there was outstanding authentication requests. If any of these messages recur, call your technical support representative for assistance.

Error Message

%CS7MAPUA-5-CLRMAPUA: MAPUA stats cleared by [chars]

Explanation MAPUA stats cleared.

Recommended Action No action is required.

Error Message

%CS7MAPUA-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

%CS7MAPUA-5-NOSOCKET: A socket could not be opened for MAP user ([IP_address]:[dec])

Explanation The software failed to open a socket for the specified MAP user.

Recommended Action

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.

CS7MONITOR Messages

Error Message

%CS7MONITOR-6-CONNECTED: [chars] ([IP_address]/[dec] -> [IP_address]/[dec])

Explanation Report active session connection.

Recommended Action No action is required.

Error Message

%CS7MONITOR-3-CS7VARIANT: CS7 variant has already been configured (CS7 monitor cannot be configured).

Explanation The CS7 monitor feature cannot be configured if the ITP is already configured for CS7 routing.

Recommended Action Remove CS7 variant configuration and re-configure as monitor.

Error Message

%CS7MONITOR-6-DISCONNECTED: [chars] ([IP_address]/[dec] -> [IP_address]/[dec])

Explanation Report disconnect of session connection.

Recommended Action No action is required.

Error Message

%CS7MONITOR-3-ENCAPSFAILURE: Interface [chars] could not be configured for monitoring.

Explanation The interface encapsulation command for cs7monitor failed.

Recommended Action No action is required.

Error Message

%CS7MONITOR-3-ERROR: [chars]

Explanation Report internal error.

Recommended Action If problem persists call your Cisco technical support representative and provide the representative with the gathered information.

Error Message

%CS7MONITOR-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 monitoring will exceed the maximum allowed number for the port adapter.

Recommended Action Configure monitoring on a different port adapter.

Error Message

%CS7MONITOR-3-NOTSUPPORTED: Interface [chars] is not supported for monitoring

Explanation The interface is not supported by the CS7 Monitor.

Recommended Action No action is required.

Error Message

%CS7MONITOR-6-TCPCONGESTION: [dec]/[IP_address]/[dec] -> congestion [chars]

Explanation Report congestion onset/abatement on TCP connection.

Recommended Action No action is required.

Error Message

%CS7MONITOR-6-TCPCONNECTED: [dec]/[IP_address]/[dec]

Explanation Report active TCP session connection.

Recommended Action No action is required.

Error Message

%CS7MONITOR-6-TCPFAILURE: [dec]/[IP_address]/[dec] -> [chars] (errno=[dec])

Explanation Report failure of TCP session connection.

Recommended Action No action is required.

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-BUFPKDROP: 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-CLRACT: 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-CLRACTCHKPT: 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-CLRAL: 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-CLRALCHKPT: 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-CNVTNOALIAS: 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 RSP 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 RSP 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 VIP 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 RSP. 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 RSP. The Standby RSP 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 VIP in slot [dec]

Explanation Non Stop operation is in process. The VIP in slot [dec] is ready to be resynchronized with the RSP.

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 RSP 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 RSP. The Standby RSP 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 RSP 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-NOEVENTQELEM: 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-NORSP: [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-GTTIFSPARSEWARN: 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-SCCPRPTTERM: 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-SCCPGTTDBCHANGED: SCCP GTT database changed during read

Explanation A read of cs7:ggt-tables/ggt_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: SCCP 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: SCCP 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-SCCPPCUNAV: 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 support.

Error Message

%CS7SCCP-5-UPU: SCCP at [chars] is unavailable.

Explanation A 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 A UPU (user part unavailable) message with cause code of <<missing text>>

Recommended Action No action is required.

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 GSMMAP msc-proxy-addr lookup failed. MSC PC [chars] is not defined in msc-proxy-addr table.

Explanation A SMS GSMMAP 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 GSMMAP 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-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-CLRASPSTAT: 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 RSP on VIP slot [dec]

Explanation RSP was unable to send configuration or status information update to the specified VIP, 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 VIP. Issue CS7 show commands on the RSP 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 VIP. Issue CS7 show commands on the RSP 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 VIP to be inconsistent with the RSP. 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 VIP. Issue CS7 show commands on the RSP 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 VIP [dec]

Explanation CS7 has exhausted all error recovery procedures on the specified VIP. All MTP3 links on the VIP 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 VIP, 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-DCS7RELDVIP: CS7 is reloading microcode on VIP in slot [dec]. Reason: [chars]

Explanation If the reason is fatal errors, it means CS7 has exhausted all error recovery procedures on the specified VIP. The IOS image will be reloaded on the VIP 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 [taps://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl](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](https://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](https://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 VIP [dec] due to fatal error

Explanation MTP3 offload has been restarted on the VIP due to a fatal error reported in an earlier error message. All links on the VIP will be shut and re-started after the CS7 configuration has been downloaded to the VIP.

Recommended Action Issue CS7 show commands on the RSP 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 VIP in slot [dec]

Explanation CS7 has detected a loss of MTP3 configuration or status update message on the specified VIP. This indicates that the MTP3 data on the VIP (for example, route, link, linkset) is inconsistent with the master copy on the RSP.

Recommended Action No action is required. The ITP will automatically perform error recovery and re-start the links on the VIP. Issue CS7 show commands on the RSP 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-DCS7XDRLLEN: 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 VIP. Issue CS7 show commands on the RSP 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 VIP. Issue CS7 show commands on the RSP 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 VIP. Issue CS7 show commands on the RSP 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 VIP. Issue CS7 show commands on the RSP 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 VIP slot [dec] is in progress

Explanation MTP3 offload has been enabled on the VIP.

Recommended Action No action is required.

Error Message

%DCS7-6-MTP3OFFLDRESP: MTP3 offload has been [chars] on VIP slot [dec]. [chars]

Explanation MTP3 offload has been enabled on the VIP.

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 VIP [dec]

Explanation An enable/disable MTP3 offload command was not acknowledged by the specified VIP. The system will resend the command. The VIP 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] - VIP Expected [dec], received [dec]

Explanation The CS7 software on the VIP encountered loss of message(s) from the RSP. This indicates the configuration and status on the VIP may be out of sync with that on the RSP. The configuration will be reloaded on the VIP.

Recommended Action No action is required. The ITP will automatically perform error recovery and re-start the links on the VIP. Issue CS7 show commands on the RSP 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-RSPIPCERR: IPC error. [chars] RC = [hex]

Explanation CS7 encountered an error with the IPC component on the RSP. This will prevent exchange of configuration and status information between the RSP and the VIP. 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 VIP. Issue CS7 show commands on the RSP 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 VIP's is in progress

Explanation SLM offload has been enabled or disabled on all the VIP's.

Recommended Action No action is required.

Error Message

%DCS7-1-SLMOFFLDVIP: SLM offload has been [chars] on VIP slot [dec]. [chars]

Explanation SLM offload has been enabled or disabled on the VIP.

Recommended Action No action is required.

Error Message

%DCS7-3-VIPERR: [chars]. VIP in slot [dec]

Explanation CS7 encountered an abnormal error related to the specified VIP. This will prevent exchange of configuration and status information between the RSP and the VIP. 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 VIP. Issue CS7 show commands on the RSP 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.