



Cisco BTS 10200 Softswitch Operations and Maintenance Guide, Release 6.0.3

August 10, 2011

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

Text Part Number: OL-25015-01

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.

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

Cisco BTS 10200 Softswitch Operations and Maintenance Guide, Release 6.0.3

Copyright © 2011, Cisco Systems, Inc.

All rights reserved.



CONTENTS

Preface ix

Introduction iii-ix

CHAPTER 1

Starting and Shutting Down the BTS 1-1

Introduction 1-1

Meeting Power Requirements 1-1

Starting BTS Hardware 1-1

Shutting Down BTS Hardware 1-2

Starting BTS Software 1-2

CHAPTER 2

Managing BTS Users and Commands Using EMS 2-1

Introduction 2-1

Logging into the EMS Using CLI 2-1

Managing Users 2-2

Managing Commands 2-5

Adapter and User Security 2-6

Solaris OS Security and BTShard Package 2-7

Operator Interface 2-10

Vulnerabilities in H.323 Message Processing 2-11

Authentication, Authorization and Accounting Support 2-11

Pluggable Authentication Module Support 2-12

User Security Account Management 2-12

Sun Microsystems Configurations 2-12

Solaris OS Patches 2-14

Trace Normal Forms (TNF) Support 2-14

XML Libraries 2-15

Device GLM Patch 2-15

Security CE Patch 2-15

Security Bad_Trap Patch 2-15

Java SDK Patches 2-15

CHAPTER 3

Monitoring and Backing Up the BTS 3-1

- Introduction **3-1**
- Detecting and Preventing BTS Congestion **3-1**
- Monitoring BTS Hardware **3-1**
- Checking BTS System Health **3-2**
 - Using BTS System-Health Reports **3-3**
 - Checking BTS System Time **3-4**
 - Checking the OS Log of Each Host Machine **3-4**
 - Checking Disk Mirroring on Each Host Machine **3-5**
 - CA/FS Side A **3-5**
 - CA/FS Side B **3-5**
 - EMS Side A **3-6**
 - EMS Side B **3-6**
 - Auditing Databases and Tables **3-7**
- Exporting Provisioned Data **3-8**
 - Limitations **3-10**
 - Creating Numbering Resource Utilization/Forecast (NRUF) Reports **3-10**
 - Creating Reports for Nonrural Primary and Intermediate Carriers **3-11**
 - Creating Reports for Rural Primary and Intermediate Carriers **3-12**
- Backing Up the Software Image **3-15**
 - Full Database Auditing **3-16**
 - Checking Shared Memory **3-16**
 - From CA/FS Side A **3-16**
 - From CA/FS Side B **3-17**
 - Backing Up the Full BTS **3-18**
 - Backing Up the CA/FS **3-18**
 - Backing up the EMS/BDMS **3-19**
- Backing up the EMS Database **3-20**
 - Using FTP to Setup File Transfer **3-21**
 - Using SFTP to Setup File Transfer **3-22**
- Archiving Your Database **3-24**
 - Examining Heap Usage **3-25**
 - Checking the DNS Server **3-25**
- Log Archive Facility (LAF) **3-26**
 - Secure Transfer of Files **3-26**
 - Other Capabilities **3-27**
 - Provisioning LAF **3-27**
 - Enabling LAF Process **3-27**
 - Setup Non-Interactive SSH Login to External Archive Server **3-28**

LAF Alarm Information	3-29
Moving Core Files	3-29

CHAPTER 4

Operating the BTS	4-1
Introduction	4-1
Managing Subscribers	4-2
Viewing Calls	4-6
Using Status and Control Commands	4-7
Using Show and Change Commands	4-9
Using ERAC Commands	4-9
Managing Transactions	4-12
Scheduling Commands	4-13
Limitations	4-13

CHAPTER 5

Managing External Resources	5-1
Introduction	5-1
Viewing BTS System-Wide Status	5-1
Managing Trunk Groups and Trunks	5-3
Managing Subscriber Terminations	5-12
Managing Gateways	5-16
Managing Other External Resources	5-18
Learning External Resource Dependencies	5-20
GigE Support	5-28
Prerequisites	5-28
Provisioning the GigE Interface	5-28

CHAPTER 6

Using BTS Measurements	6-1
Introduction	6-1
Using Measurements	6-1
Learning the Measurement Types	6-2
ISDN Measurements	6-2
Call Processing Measurements	6-5
MGCP Adapter Measurements	6-12
DQoS Measurements	6-13
SIP Measurements	6-13
Service Interaction Manager Measurements	6-16
POTS Local FS Measurements	6-16

POTS Application Server Measurements	6-22
POTS Miscellaneous FS Measurements	6-22
POTS Class of Service FS Measurements	6-24
POTS Screen List Editing FS Measurements	6-25
POTS Customer Originated Trace FS Measurements	6-25
POTS Automatic Callback, Recall, and Call Return Measurements	6-26
POTS Limited Call Duration (Prepaid/Postpaid) with RADIUS Interface to AAA Measurements	6-28
POTS Call Forwarding Combination Measurements	6-28
AIN Services FS Measurements	6-29
SCCP Protocol Measurements	6-31
TCAP Protocol Measurements	6-33
SUA Measurements	6-37
M3UA Protocol Measurements	6-39
SCTP Measurements	6-41
IUA Measurements	6-44
ISUP Measurements	6-46
ISUP (ANSI) Measurements	6-52
ISUP (France) Measurements	6-55
ISUP (Poland) Measurements	6-55
ISUP (ITU-China) Measurements	6-55
ISUP (ITU-Mexico) Measurements	6-58
ISUP (ITU-HongKong) Measurements	6-60
Audit Measurements	6-62
SIP Interface Adapter Measurements	6-62
Call Detail Block Measurements	6-64
Event Messaging Measurements	6-66
Dynamic QoS Measurements	6-66
PCMM Measurements	6-67
SNMP Protocol Measurements	6-67
Trunk Group Usage Measurements	6-68
Announcement Measurements	6-71
H.323 Protocol Measurements	6-71
Call Tools Measurements	6-75
AIN Tools Measurements	6-75
PCT Tools Measurements	6-75
CPU Usage Measurements	6-76
Memory Usage Measurements	6-76
Network I/O Usage Measurements	6-76
Disk Usage Measurements	6-76
System Load Usage Measurements	6-78

Disk I/O Usage Measurements	6-78
ENUM Measurements	6-78
Diameter Message Counters	6-79
Single Number Reach Counters	6-80

CHAPTER 7**Using the BTS SNMP Agent 7-1**

Introduction	7-1
Managing User Access to the SNMP Agent	7-1
Viewing SNMP Trap Reports	7-2
Viewing and Managing BTS Components	7-4
Querying the SNMP Agent	7-6
Enabling NMS to Query/Poll Solaris SNMP Agent	7-6

APPENDIX A**Feature Tones A-1**

Introduction	A-1
Tones per Feature	A-1
Tone Frequencies and Cadences	A-6

APPENDIX B**FIM/XML B-1**

Understanding the Configurable FIM/XML Feature	B-1
Advantages of the FIM/XML Tool	B-2
Tool Requirements	B-2
Writing an External FIM/XML File	B-3
Defining Features	B-3
Elements in the External FIM/XML File	B-3
Define Element	B-4
Precedence-Exception Element	B-4
Inhibit Others Element	B-5
Inhibit Me Element	B-5
Response Profile Element	B-5
Installing the FIM/XML File Using the Offline FIM/XML Tool	B-7
FIM/XML File and Shared iFC File	B-9
Features Defined in FIM/XML and Shared iFC	B-9
Provisioning iFC	B-10
Defining a New feature as the Originating Feature	B-10
Defining a VSC	B-10
Defining the SIP Trigger Profile	B-10

Feature Configuration **B-10**
Subscriber-Sip-Trigger-Profile **B-11**
Service-Id **B-11**
Subscriber-Service-Profile **B-11**
Feature Restrictions and Limitations **B-11**



Preface

Revised: August 10, 2011, OL-25015-01

Introduction

This document is the *Operations and Maintenance Guide* for the Cisco BTS 10200 Softswitch, Release 6.0.3.

Organization

This guide has the following chapters:

- [Chapter 1, “Starting and Shutting Down the BTS”](#)—Tells you how to start up and shut down the BTS
- [Chapter 2, “Managing BTS Users and Commands Using EMS”](#)—Describes operator interfaces to the BTS and how to manage access and users
- [Chapter 3, “Monitoring and Backing Up the BTS”](#)—Includes overall BTS maintenance strategies
- [Chapter 4, “Operating the BTS”](#)—Tells you how to operate the BTS
- [Chapter 5, “Managing External Resources”](#)—Tells you how to manage external resources provisioned on the BTS using administrative (ADM) commands
- [Chapter 6, “Using BTS Measurements”](#)—Describes BTS traffic measurements and tells you how to use them
- [Chapter 7, “Using the BTS SNMP Agent”](#)—Explains how to use the Simple Network Management Protocol (SNMP) agent
- [Appendix A, “Feature Tones”](#)—Explains special tones the BTS supports for subscriber and operator features
- [Appendix B, “FIM/XML”](#)—Explains the Feature Interaction Module/Extensible Markup Language (FIM/XML) feature.

Document Change History

This table provides the revision history for the *Cisco BTS 10200 Softswitch Operations and Maintenance Guide, Release 6.0.3*.

Table 1 **Revision History**

Version Number	Issue Date	Status	Reason for Change
OL-25015-01	August 10, 2011	Initial	Initial document for Release 6.0.3.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

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

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.



CHAPTER 1

Starting and Shutting Down the BTS

Revised: August 10, 2011, OL-25015-01

Introduction

This chapter tells you how to start up and shut down the BTS.

Meeting Power Requirements

To meet high availability requirements:

- Do *not* have common parts in the power feeds to the redundant hardware that could be a common single point of failure.
- Use uninterruptible power supply (UPS) for both AC and DC systems. It must be designed to support system operation through any possible power interruption. Power must have battery backup to maintain service in the event of commercial power failure (both power supplies of the redundant pair must be able to do this).
- For AC-powered installations have two separate (redundant) circuits. Source AC circuits from separate transformer phases on separate breakers so a single breaker trip does not disable both.
- For DC-powered installations have power from two separate dedicated DC branches (redundant A and B feeds) for each DC-powered BTS.

Starting BTS Hardware

The time it takes to complete this procedure varies with system type and database size. System types include:

- EMS—Element Management System
- BDMS—Bulk Data Management System
- CA—Call Agent
- FS—Feature Server

Step 1 Ensure all power cables connect to the correct ports.

- Step 2** Plug in Catalyst switch routers.
 - Step 3** Power on EMS/BDMS hosts A and B.
 - Step 4** Power on CA/FS hosts A and B.
-

Shutting Down BTS Hardware

- Step 1** Ensure CA side A and EMS side A are active.
 - Step 2** Ensure CA side B and EMS side B EMS are standby.
 - Step 3** Log into CA side A and B and EMS side A and B using Secure Shell (SSH).
 - Step 4** Shut down the system in order:
 1. EMS side B
 2. CA side B
 3. CA side A
 4. EMS side A
 - Step 5** To begin platform shutdown:


```
>platform stop all
```
 - Step 6** When #> returns, enter `nodestat` to ensure the operating system is ready for shutdown.
 - Step 7** To shut down the servers, enter one of the following commands for each node (Sun Microsystems recommends both as graceful shutdowns).


```
>shutdown -i5 -g0 -y
```

Or:

```
>sync;sync; init5
```
 - Step 8** To power off primary and secondary CAs and FSs find the switch to the left of the LEDs and flip it to OFF.
 - Step 9** When the fans stop, release the switch to neutral.
 - Step 10** To power off primary and secondary EMSs find the switch to the left of the LEDs and flip it to OFF.
 - Step 11** When the fans stop, release the switch to neutral.
 - Step 12** To power off the side, unplug them.
-

Starting BTS Software

BTS automatically starts when you power on the server. Repeat this procedure for each server.

- Step 1** Enter `nodestat`.
- Step 2** Log in as `root`.
- Step 3** Enter `platform start`.

Step 4 Once all components start, enter `noreset` to ensure proper startup.



CHAPTER 2

Managing BTS Users and Commands Using EMS

Revised: August 10, 2011, OL-25015-01

Introduction

This chapter describes operator interfaces to the BTS and how to manage access and users.

The Element Management System (EMS) database holds up to 256 logins and up to 50 active user sessions. Using the command line interface (CLI) you can locally connect to the EMS in an interactive session. The EMS system administrator can:

- Add a new user.
- Assign a user's privilege level—10 is for the system administrator. BTS has predefined user accounts:

Username		Permission
btsadmin	btsadmin	like MAINT shell user—MAINT shell is an enhanced CLI interface and does not log off an idle user)
secadmin	secadmin	like MAINT shell user
btsuser	btsuser	lower access permissions than btsadmin and secadmin, good for generic provisioning access

- Reset a user's password.
- Enter a description for each security class and privilege level.
- Manage security log reporting.

Logging into the EMS Using CLI

SSH is a way to access the BTS CLI or maintenance (MAINT) modes. SSH provides encrypted communication between a remote machine and the EMS/CA for executing CLI or MAINT commands. The SSH server runs on EMSs and CAs. To connect the client and server sides run the secure shell daemon (SSHD). With SSH, new users must enter a new password and reenter that password during the first login. In future logins they are prompted once for a password only.

The “ciscouser” login is a high-level security login for TAC and other BTS support personnel that restricts access to certain commands. Anyone else trying to execute such commands receives an error message.

After installation, on the EMS, the system prompts you to change the passwords of **root**, **btsadmin**, **btsuser** and **calea** if they have default passwords. On the CA, the system prompts you to change the passwords of **root** if it has default password. There are no default passwords for Operations, Administration and Maintenance applications.

When logging in for the first time system administrators log in as **btsadmin** (the default password is **btsadmin**). Change the password.

Step 1 To log in from the client side for the first time: `ssh btsadmin@<ipaddress>`.



Note If you are logged in to the system as **root**, enter: `btsadmin@0`

On the first SSH login from the client side, expect a message like this:

```
The authenticity of host [hostname] can't be established.
Key fingerprint is 1024 5f:a0:0b:65:d3:82:df:ab:42:62:6d:98:9c:fe:e9:52.
Are you sure you want to continue connecting (yes/no)?
```

Step 2 Enter `yes`.

The password prompt appears, now all communications are encrypted.

Step 3 Enter your password.

The system responds with a CLI> prompt. You can now send commands to the EMS.

Step 4 Enter provisioning commands.

Step 5 To log off, enter `exit`.

Managing Users

You must have a user privilege level of 9 or higher to add, show, change, or delete a user.



Caution

Do not add, change, or delete username **root**, this prevents proper EMS access.

Table 2-1 Managing Users

Task	Sample Command
Adding a user	<ol style="list-style-type: none"> <code>add user name=UserABC; command-level=9; warn=10; days-valid=30; work-groups=somegroup;</code> Supply a default password: <code>reset password name=<user name>; new-password=<user password>;</code>
Viewing a user	<code>show user name=UserABC;</code>

Table 2-1 Managing Users (continued)

Task	Sample Command
Viewing user activity	<code>show ems;</code>
Changing a user	<code>change user name=UserABC; command-level=1; work-groups=somegroup;</code>
Deleting a user	<code>delete user name=UserABC;</code> You cannot delete <code>optiuser</code> .
Changing a user's password	<code>reset password name=username; days-valid=<number of days the new password will be valid>; warn=<number of days before password expiration to warn user>;</code> <code>reset password name=username; days-valid=30; warn=4;</code> A password must: <ul style="list-style-type: none"> • Have 6-8 characters • Have at least two alphabetic characters • Have at least one numeric or special character • Differ from the user's login name and any combination of the login name • Differ from the old password by at least three characters Change the password for user <code>optiuser</code> on each BTS.
Adding a new work-group	<code>change command-table noun=mgw; verb=add; work-groups=latex;</code>
Adding a user to a work-group	<code>change user name=trs80nut; work-groups=+rubber;</code>
Removing a user from a work-group	<code>change user name=trs80nut; work-groups=-latex;</code>
Viewing all currently active users	<code>show session</code>
Viewing an active user	<code>show session terminal</code>

Table 2-1 Managing Users (continued)

Task	Sample Command
Blocking an active user	<p>1. Select operation mode:</p> <ul style="list-style-type: none"> • MAINTENANCE—(default) for regular maintenance • UPGRADE—for upgrades <p>2. <code>block session terminal=USR16;</code></p> <p>Note You cannot block the session of a user with higher privileges than yours.</p> <p>Prevent BTS provisioning during an upgrade or maintenance window from the following interfaces:</p> <ul style="list-style-type: none"> • CLI • FTP • CORBA • SNMP <p>Note The software will support blocking HTTP interfaces in a future release.</p> <p>If you block provisioning before performing an SMG restart or EMS reboot, blocking is still enforced when these applications return to in-service state.</p> <p>There are two levels of blocking:</p> <ul style="list-style-type: none"> • PROVISION—Prevents all provisioning commands from executing • COMPLETE—Prevents all commands from executing <p>Only terminal type MNT users can use these blocking and unblocking commands. MNT users are never blocked. MNT users issue these commands from either active or standby EMS.</p> <p>A blocking command applies to all non-MNT users on terminals on either active or standby EMS. Commands do not execute for:</p> <ul style="list-style-type: none"> • Logged-in users • Users who login after the block command <p>Commands are not queued for execution after unblock. The CLI user prompt changes when blocked, notifying the user their commands will not execute.</p>
Unblocking a user	<p><code>unblock session terminal=USR16;</code></p> <p>Note You cannot unblock the session of a user with higher privileges.</p>
Resetting a user's idle time	<p>Idle time is how many minutes (1-30) a user can be idle before being logged off the BTS.</p> <p><code>change session idle-time=30;</code></p>
Stopping a user's session	<p><code>stop session terminal=USR16;</code></p>

**Note**

All commands should be assigned to a work-group. If a command is not assigned to a work-group, a user will be able to execute that command, which is not recommended. You can also assign users and the commands to multiple work-groups.

Managing Commands

Each command (verb-noun combination) has a security class of 1-10; 1 is lowest, 10 is highest. Each time a user enters a command, the system compares the user's privilege level to the command's security class. EMS denies the command if the user level is less than the command level.

The Command Level (command-level) table shows the 10 command security classes. BTS has the following presets:

- 1 (lowest level)
- 5 (mid-level)
- 10 (highest level)—These commands require a system administrator with a security level of 10 to execute.

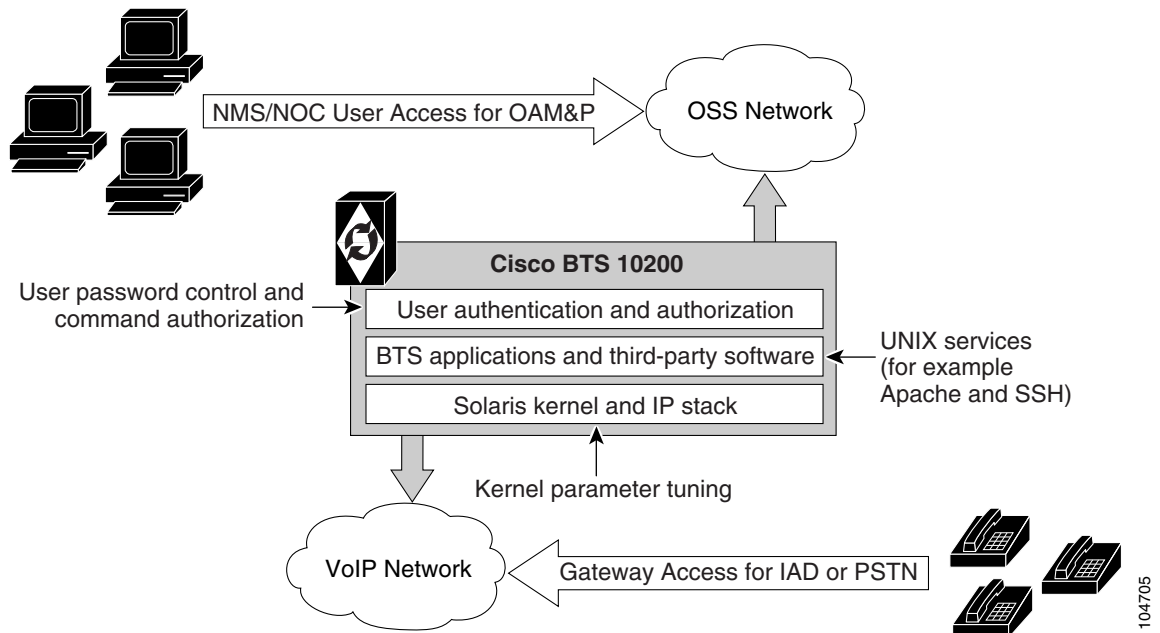
Table 2-2 Managing Commands

Task	Sample Command
Viewing a command's security class	<code>show command-level id=10;</code>
Adding a description to a command's security class	<code>change command-level id=10; description=This is the highest level administration access;</code>
Changing a command's privilege level	<code>change command-table noun=mgw; verb=add; sec-level=9;</code>
Resetting a command's privilege level	<code>reset command-table noun=mgw; verb=add;</code>
Viewing all executed commands	<code>show history;</code>
Sending all executed commands to a report file	<code>report history;</code> Note Results may take a few minutes to display.
Viewing the report of all executed commands	<ol style="list-style-type: none"> 1. In a web browser enter <code>http://server name</code>. 2. Click Reports. 3. Click <code>history.html</code>.
Viewing a security summary	<code>report security-summary start-time=2002-09-26 00:00:00; end-time=2002-09-27 00:00:00; source=all;</code> Note Results may take a few minutes to display.
Viewing security summary reports	In a web browser enter <code>https:// <ems ip addr></code> .

This chapter details the behaviors and attributes of the various security packages in the BTS 10200. The sources for the items are derived from many dynamic sources. Included in these sources are security bulletins from third-party vendors to the BTS 10200 as well as security agencies and open source organizations.

Security is an important part of the BTS 10200. The BTS 10200 has interfaces to customer premise equipment (CPE) as well as northbound Operations Support System (OSS) interfaces. All of these interfaces are subject to attacks. In addition, users who are allowed onto the BTS 10200 can also find ways to exploit applications that can lead to service-affecting situations. Therefore, many precautions are taken to ensure the solidity of the BTS 10200 defenses while avoiding a system that is difficult to manage.

Figure 2-1 *BTS 10200 Access and Related Security*



Adapter and User Security

This section describes requirements that generally involve adapter and user level of security. In the BTS 10200, adapters are any external, northbound interfaces of the BTS 10200. However, some extrapolated requirements involve adapter technology based on the current deployment:

- Support termination of a session once a provisionable inactivity timeout has occurred. An event report is issued upon each timeout expiry. The inactivity time ranges from 10 to 30 minutes.
- Restrict access as “root” to the BTS 10200 in all cases except Cisco TAC and customer “administrator”. This is a broad statement that includes the addition of command-line interface (CLI) commands to help manage the system. In addition, UNIX services are restricted to harden the operating system (OS). The service restriction is listed in the [Solaris OS Security and BTShard Package](#) section. The process of restricting root access is an ongoing process.
- Use of “sudo” is acceptable and the formal Sun-built and packaged version is located in `/opt/sfw/bin/`.

Solaris OS Security and BTShard Package

This section details the security packages for the BTS 10200 OS. These packages are automatically installed at installation. These packages are derived from both Sun Microsystems security bulletins and Cisco internal policies for safety of the OS and its applications. All services can be reactivated for the lifetime of the current kernel instance. All settings are reset on reboot of the kernel. These settings are contained in the BTShard Solaris package delivered with the BTS 10200.

- Remove unnecessary UNIX systems services. These services are listed below. Management of these facilities must allow for each service to be enabled or disabled on an individual basis. This service management must also be accomplished through the BTS 10200 adapter interface.
 - FTP—FTP server is disabled and SFTP (Secure FTP) should be used. This impacts the Bulk Data Provisioning interface. It does not impact the Billing Bulk Data transfer. The FTP client code will still be available on the EMS node.
 - Telnet—This terminal protocol is disabled and SSH (Secure Shell) should be used. The telnet server and client code are still available on the EMS node.
 - Echo—This service is to be disabled. This capability has been replaced with Internet Control Message Protocol (ICMP) “ping” facilities.
 - Discard—This service is to be disabled.
 - Printer—This service is to be disabled. No printer services are supplied in the BTS 10200 product description.
 - Daytime—This service is to be disabled.
 - Chargen—This service is to be disabled.
 - SMTP—This service is to be disabled.
 - Time—This service is to be disabled.
 - Finger—This service is to be disabled. No network user facilities are required. The BTS 10200 tracks users internally and on a single BTS basis.
 - Sun RPC—This service is to be disabled. This may be enabled in a lab environment for Tooltalk usage in debugging application programs.
 - Exec—This service is to be disabled.
 - Login—This service is to be disabled.
 - Shell—This service is to be disabled. This may be required for some lab activity; however, there is no field usage for rlogin, rcp, and rsh facilities.
 - UUCP—This service is to be disabled.
 - NFS—This service is to be disabled.
 - Lockd—This service is to be disabled.
 - X11—This service is available for the near term *only*.
 - DTSCP—This service is to be disabled.
 - Font-services—This service is to be disabled.
 - HTTP—This service is to be enabled. This is used by the BTS 10200 to offer results of report generation. This will migrate to HTTPS.

- The following UNIX accounts are to be LOCKED but not removed from the system: lp, uucp, nuucp, nobody, listen, and any other Cisco support accounts not used in the normal course of field operation. Services managed by root are the only accounts allowed to utilize one of these identities. This is the default behavior.
- Modifications to the Solaris kernel parameters were made to close potential breeches in the OS. These types of security precautions are most often geared toward “denial of service” attacks. These types of attacks create situations that degrade the performance of a system and as a result, prohibit the critical applications from delivering the service they are designed to provide.
- The TCP protocol uses random initial sequence numbers.
- All failed login attempts are logged.
- The following users are not allowed direct FTP access to the machine: root, daemon, bin, sys, adm, nobody, and noaccess.
- A root user cannot telnet directly to the machine. Direct root user access is granted to the console only. A user who wants to access the root account must use the **su** command from a nonprivileged account.
- The break key (<STOP> <A>) on the keyboard is disabled.
- **IP_FORWARD_DIRECTED_BROADCASTS**—This option determines whether to forward broadcast packets directed to a specific net or subnet, if that net or subnet is directly connected to the machine. If the system is acting as a router, this option can be exploited to generate a great deal of broadcast network traffic. Turning this option off helps prevent broadcast traffic attacks. The Solaris default value is 1 (True). For example:

```
ip_forward_directed_broadcasts=0
```
- **IP_FORWARD_SRC_ROUTED**—This option determines whether to forward packets that are source routed. These packets define the path the packet should take instead of allowing network routers to define the path. The Solaris default value is 1 (True). For example:

```
ip_forward_src_routed=0
```
- **IP_IGNORE_REDIRECT**—This option determines whether to ignore the ICMP packets that define new routes. If the system is acting as a router, an attacker may send redirect messages to alter routing tables as part of sophisticated attack (man-in-the-middle attack) or a simple denial of service. The Solaris default value is 0 (False). For example:

```
ip_ignore_redirect=1
```
- **IP_IRE_FLUSH_INTERVAL**—This option determines the period of time at which a specific route will be kept, even if currently in use. Address Resolution Protocol (ARP) attacks may be effective with the default interval. Shortening the time interval may reduce the effectiveness of attacks. The default interval is 1200000 milliseconds (20 minutes). For example:

```
ip_ire_flush_interval=60000
```
- **IP_RESPOND_TO_ADDRESS_MASK_BROADCAST**—This option determines whether to respond to ICMP netmask requests, typically sent by diskless clients when booting. An attacker may use the netmask information for determining network topology or the broadcast address for the subnet. The default value is 0 (False). For example:

```
ip_respond_to_address_mask_broadcast=0
```

- **IP_RESPOND_TO_ECHO_BROADCAST**—This option determines whether to respond to ICMP broadcast echo requests (ping). An attacker may try to create a denial of service attack on subnets by sending many broadcast echo requests to which all systems will respond. This also provides information on systems that are available on the network. The Solaris default value is 1 (True). For example:

```
ip_respond_to_echo_broadcast=1
```

- **IP_RESPOND_TO_TIMESTAMP**—This option determines whether to respond to ICMP timestamp requests, that some systems use to discover the time on a remote system. An attacker may use the time information to schedule an attack at a period of time when the system may run a cron job (or other time-based event) or otherwise be busy. It may also be possible predict ID or sequence numbers that are based on the time of day for spoofing services. The Solaris default value is 1 (True). For example:

```
ip_respond_to_timestamp=0
```

- **IP_RESPOND_TO_TIMESTAMP_BROADCAST**—This option determines whether to respond to ICMP broadcast timestamp requests, that are used to discover the time on all systems in the broadcast range. This option is dangerous for the same reasons as responding to a single timestamp request. Additionally, an attacker may try to create a denial of service attack by generating many broadcast timestamp requests. The default value is 1 (True). For example:

```
ip_respond_to_timestamp_broadcast=0
```

- **IP_SEND_REDIRECTS**—This option determines whether to send ICMP redirect messages, that can introduce changes into the routing table of the remote system. It should only be used on systems that act as routers. The Solaris default value is 1 (True). For example:

```
ip_send_redirects=0
```

- **IP_STRICT_DST_MULTIHOMING**—This option determines whether to enable strict destination multihoming. If this is set to 1 and `ip_forwarding` is set to 0, then a packet sent to an interface from which it did not arrive will be dropped. This setting prevents an attacker from passing packets across a machine with multiple interfaces that is not acting a router. The default value is 0 (False). For example:

```
ip_strict_dst_multihoming=1
```

- **TCP_CONN_REQ_MAX_Q0**—This option determines the size of the queue containing half-open connections. This setting provides protection from SYN flood attacks. Solaris 2.6 and 7 (and 2.5.1 with patch 103582-12 and higher) include protection from these attacks. The queue size default is adequate for most systems but should be increased for busy web servers. The default value is 1024. For example:

```
tcp_conn_req_max_q0=4096
```

- The following startup files are removed from the level “3” runtime environment of the BTS 10200. These services can still be started manually if required in laboratory circumstances. They are not required for field operations.
 - S71rpc
 - S73cachefs.daemon
 - S73nfs.client
 - S74autofs
 - S80lp
 - S80spc

- S88sendmail
- S93cacheos.finish
- S99dtlogin

Operator Interface

Additional commands have been added to manage the UNIX services in the BTS 10200. These commands are available from the CLI/MAINT interface. In addition, these same commands are also available from the CORBA and bulk-provisioning interface. There are no schemas and tables associated with these commands. They directly control the UNIX services. These services are only enabled for the lifetime of the current kernel instance. They are reset to the installed defaults when a kernel reboot is performed.

Table 2-3 describes the system services available using the node command.

Table 2-3 Node Command for UNIX Services

Noun	Verb	Options	Description
Node	Change	SERVICE [Required] Must be one of the following: FTP, TELNET, ECHO, DISCARD, PRINTER, DAYTIME, CHARGEN, SMTP, TIME, FINGER, SUNRPC, EXEC, LOGIN, SHELL, UUCP, NFS, LOCKD, X11, DTSCP, FONT-SERVICES, HTTP.	Defines the service to change.
Node	Change	ENABLE [Required]	A Boolean flag [Y/N] that indicates whether to turn this service on or off.
Node	Change	NODE [Required]	The node name in the BTS 10200 where the service is managed.

Table 2-3 Node Command for UNIX Services (continued)

Noun	Verb	Options	Description
Node	Show	SERVICE [Required] Must be one of the following: FTP, TELNET, ECHO, DISCARD, PRINTER, DAYTIME, CHARGEN, SMTP, TIME, FINGER, SUNRPC, EXEC, LOGIN, SHELL, UUCP, NFS, LOCKD, X11, DTSCP, FONT-SERVICES, HTTP.	Defines the service to display.
Node	Show	Node [Required]	Defines the node to display for the state of the service.

Vulnerabilities in H.323 Message Processing

During 2002 the University of Oulu Security Programming Group (OUSPG) discovered a number of implementation-specific vulnerabilities in the Simple Network Management Protocol (SNMP). Subsequent to this discovery, the National Infrastructure Security Coordination Centre (NISCC) performed and commissioned further work on identifying implementation specific vulnerabilities in related protocols that are critical to the United Kingdom Critical National Infrastructure. One of these protocols is H.225, that is part of the H.323 family and is commonly implemented as a component of multimedia applications such as Voice over IP (VoIP).

OUSPG produced a test suite for H.225 and employed it to validate their findings against a number of products from different vendors. The test results have been confirmed by testing performed by NISCC and the affected vendors contacted with the test results. These vendors' product lines cover a great deal of the existing critical information infrastructure worldwide and have therefore been addressed as a priority. However, the NISCC has subsequently contacted other vendors whose products employ H.323 and provided them with tools with which to test these implementations.

Authentication, Authorization and Accounting Support

These extensions represent modifications to the current scheme of user account management on the system. It includes support for the following two protocols; these protocols are not required to be mutually inclusive.

- Radius Protocol
- Lightweight Directory Access Protocol (LDAP)

Prior to Release 4.4, user account management for the BTS 10200 used the standard Solaris password management facilities without the use of the Authentication Dial-In User Service Network Information Service (NIS). All accounts are stored locally and referenced locally. This security feature begins support for a complete AAA model for user account management. This model impacts several internal subsystems of the BTS 10200 Element Management System (EMS) application. It also impacts the core login support on the other nodes of the BTS 10200.

Pluggable Authentication Module Support

The BTS 10200 deploys a Secure Shell (SSH) package with Pluggable Authentication Module (PAM) support. The package includes the PAM support required to utilize the Radius and LDAP servers.

The supporting configuration allows local accounts to fall through if the Radius and LDAP servers are not available. These default local accounts for the BTS 10200 are the `btsuser`, `btsadmin` and `secadmin` accounts. These are the standard default accounts provided in the base product and use the native password management.

A UNIX-based user provides access to the operating system on all nodes. The `oamp` user is defined for package management purposes. The account is locked and no password is available. However, to grant UNIX access to all nodes of the BTS 10200, a default password is provided.

When PAM support is used, SSH transfers the control of authentication to the PAM library, that then loads the modules specified in the PAM configuration file. Finally, the PAM library tells SSH whether the authentication was successful. SSH is not aware of the details of the actual authentication method employed by PAM. Only the final result is of interest.

User Security Account Management

The BTS 10200 EMS contains an application program known as User Security Management (USM). This program determines if an account is local or off-board. Password management facilities are disabled for all accounts on the BTS 10200 when an AAA deployment is configured. The AAA deployment transfers the responsibility for these existing facilities to the end-user AAA servers. These facilities include the following attributes:

- Password aging, warning, and expiration
- Password reset and automatic account locking
- Local account management (password and shadow files) for new accounts

Sun Microsystems Configurations

Table 2-4 lists the Solaris 10 architecture-specific or hardware specific packages for certain Sun Microsystems configurations.

Table 2-4 Solaris Architectural- or Hardware-Specific Optional Package List

Package	Description	Type	Status
SMEvplr	SME platform links	SYSTEM	—
SMEvplu	SME usr/platform links	SYSTEM	—
SUNWaudd	Audio drivers	SYSTEM	—
SUNWauddx	Audio drivers (64-bit)	SYSTEM	—
SUNWced	Sun GigaSwift Ethernet Adapter (32-bit driver)	SYSTEM	—
SUNWcedx	Sun GigaSwift Ethernet Adapter (64-bit driver)	SYSTEM	—
SUNWcg6	GX (cg6) device driver	SYSTEM	—
SUNWcg6x	GX (cg6) device driver (64-bit)	SYSTEM	—
SUNWcsd	Core Solaris devices	SYSTEM	—

Table 2-4 *Solaris Architectural- or Hardware-Specific Optional Package List (continued)*

Package	Description	Type	Status
SUNWdfb	Dumb Frame Buffer device drivers	SYSTEM	—
SUNWensqr	Ensoniq ES1370/1371/1373 Audio device driver (32-bit) (Root)	SYSTEM	—
SUNWensqx	Ensoniq ES1370/1371/1373 Audio device driver (64-bit) (Root)	SYSTEM	—
SUNWeridx	Sun RIO 10/100 Mb Ethernet drivers (64-bit)	SYSTEM	—
SUNWfcip	Sun FCIP IP/ARP over FibreChannel device driver	SYSTEM	—
SUNWfcipx	Sun FCIP IP/ARP over FibreChannel device driver (64-bit)	SYSTEM	—
SUNWfcp	Sun FCP SCSI device driver	SYSTEM	—
SUNWfcpx	Sun FCP SCSI device driver (64-bit)	SYSTEM	—
SUNWfctl	Sun Fibre Channel Transport layer	SYSTEM	—
SUNWfctlx	Sun Fibre Channel Transport layer (64-bit)	SYSTEM	—
SUNWfruid	FRU ID prtfru Command and libfru library	SYSTEM	—
SUNWfruip	FRU ID Platform Data module and Access libraries	SYSTEM	—
SUNWfruix	FRU ID library (64-bit)	SYSTEM	—
SUNWged	Sun Gigabit Ethernet Adapter driver	SYSTEM	—
SUNWglmr	rasctrl environment monitoring driver for i2c (Root) (32-bit)	SYSTEM	—
SUNWglmx	rasctrl environment monitoring driver for i2c (Root) (64-bit)	SYSTEM	—
SUNWi2cr	device drivers for I2C devices (Root, 32-bit)	SYSTEM	—
SUNWi2cx	device drivers for I2C devices (Root, 64-bit)	SYSTEM	—
SUNWidecr	IDE device drivers	SYSTEM	—
SUNWidecx	IDE device drivers (Root) (64bit)	SYSTEM	—
SUNWider	IDE device driver (Root)	SYSTEM	—
SUNWkmp2r	PS/2 Keyboard and Mouse device drivers (Root) (32-bit)	SYSTEM	—
SUNWkmp2x	PS/2 Keyboard and Mouse device drivers (Root) (64-bit)	SYSTEM	—
SUNWmdr	Solstice DiskSuite drivers	SYSTEM	Required by the BTS 10200
SUNWmdx	Solstice DiskSuite drivers(64-bit)	SYSTEM	Required by the BTS 10200
SUNWmdi	Sun Multipath I/O drivers	SYSTEM	—
SUNWmdix	Sun Multipath I/O drivers (64-bit)	SYSTEM	—
SUNWpd	PCI drivers	SYSTEM	—

Table 2-4 *Solaris Architectural- or Hardware-Specific Optional Package List (continued)*

Package	Description	Type	Status
SUNWpdx	PCI drivers (64-bit)	SYSTEM	—
SUNWpiclh	PICL Header files	SYSTEM	—
SUNWpiclr	PICL Framework (Root)	SYSTEM	—
SUNWpiclu	PICL libraries and Plugin modules (Usr)	SYSTEM	—
SUNWpiclx	PICL libraries (64-bit)	SYSTEM	—
SUNWqfed	Sun Quad FastEthernet Adapter driver	SYSTEM	—
SUNWqfedx	Sun Quad FastEthernet Adapter driver (64-bit)	SYSTEM	—
SUNWqlc	Qlogic ISP 2200/2202 Fiber Channel device driver	SYSTEM	—
SUNWqlcx	Qlogic ISP 2200/2202 Fiber Channel device driver (64-bit)	SYSTEM	—
SUNWses	SCSI Enclosure Services device driver	SYSTEM	—
SUNWsesx	SCSI Enclosure Services device driver (64-bit)	SYSTEM	—
SUNWsior	SuperIO 307 (plug-n-play) device drivers (Root)	SYSTEM	—
SUNWsiox	SuperIO 307 (plug-n-play) device drivers (Root) (64-bit)	SYSTEM	—
SUNWssad	SPARCstorage Array drivers	SYSTEM	—
SUNWssadx	SPARCstorage Array drivers (64-bit)	SYSTEM	—
SUNWssaop	Administration Utilities and Firmware for SPARCStorage Array	SYSTEM	—
SUNWuau	USB Audio drivers	SYSTEM	—
SUNWuau	USB Audio drivers (64-bit)	SYSTEM	—
SUNWusb	USB device drivers	SYSTEM	—
SUNWusbx	USB device drivers (64-bit)	SYSTEM	—
SUNWxwdv	X Windows System Window drivers	SYSTEM	—
SUNWxwdvx	X Windows System Window drivers (64-bit)	SYSTEM	—

Solaris OS Patches

This chapter describes the BTS 10200 Solaris OS patches.

Trace Normal Forms (TNF) Support

The TNF package provides the Solaris tool suite with enhanced debugging capabilities of applications as they execute in the target environment. TNF supports program execution traces at both the user and kernel level. The package includes the following:

- SUNWtnfc—Utilities needed to enable probe points, in the kernel and in applications, that can generate TNF records in a trace file.

- SUNWtnfd—Utilities needed by developers using TNF facilities.
- SUNWtnfx—The 64-bit utilities needed to enable probe points, in the kernel and in applications, that can generate TNF records in a trace file.

XML Libraries

The Sun VTS software requires the use of the XML libraries on the BTS 10200. These are in the supplemental part of the Solaris distribution with the VTS packages. These XML libraries and tools for 32 and 64 bit usage are listed as follows:

- SUNWxmlS
- SUNWlxml
- SUNWlxmlx

Device GLM Patch

The 109885-16 patch corrects several open bug reports on the SCSI device driver GLM in the Solaris OS.

Security CE Patch

The 111883-24 patch corrects Sun GigaSwift Ethernet 1.0 driver.

Security Bad_Trap Patch

The 117000-05 patch is a new generic kernel patch that cumulates many kernel level bug fixes into a single patch. This supersedes the older generic patch 108528-29.

Java SDK Patches

The upgraded version of Java requires some additional patches to the kernel and system libraries to support the required functionality. The patches are listed below. These are the relevant patches from the recommended cluster of patches as produced by Sun Microsystems.

- 109147-30—The SunOS 5.8: linker patch.
- 111308-05—The SunOS 5.8: /usr/lib/libmtmalloc.so.1 patch.
- 112438-03—The SunOS 5.8: /kernel/drv/random patch.
- 108434-17—The SunOS 5.8: 32-Bit Shared library patch for C++.

**Note**

108435-17 is the corresponding 64-bit patch.

- 108435-17—The SunOS 5.8: 64-Bit Shared library patch for C++ Note: 108434-17 is the corresponding 32-bit patch.
- 111111-04—The SunOS 5.8: /usr/bin/nawk patch.

- 108993-38—The SunOS 5.8: LDAP2 client, libc, libthread and libnsl libraries patch.
- 109326-16—The SunOS 5.8: libresolv.so.2 and in.named patch.
- 110615-13—The SunOS 5.8: sendmail patch.



CHAPTER 3

Monitoring and Backing Up the BTS

Revised: August 10, 2011, OL-25015-01

Introduction

This chapter includes overall BTS maintenance strategies.

Detecting and Preventing BTS Congestion

When congested the BTS automatically does the following:

- Detects internal messaging congestion caused by traffic overload or other extraordinary events.
- Takes preventive action to avoid system failure (including shedding of traffic).
- Generates alarms when it detects internal messaging.
- Clears the alarms when congestion abates.
- Places the access control list (ACL) parameter (indicating congestion) into release messages sent to the SS7 network when the BTS internal call processing engine is congested.
- Routes emergency messages. Exact digit strings for emergency calls differ, specify up to ten digit strings (911 and 9911 are included by default). Contact Cisco TAC to do this, it involves a CA restart.
- Generates a SS7 termination cause code 42 for billing.
- Generates the cable signaling stop event with cause code “resource unavailable” for billing.

See the *Cisco BTS 10200 Softswitch Troubleshooting Guide, Release 6.0.3* for congestion alarms.



Monitoring BTS Hardware

BTS tracks devices and facilities that exceed their settings.

- A process exceeds 70 percent of the CPU.
- The Call Agent CPU is over 90 percent busy (10 percent idle).
- The load average exceeds 5 for at least a 5-minute interval.
- Memory is 95 percent exhausted and swap is over 50 percent consumed.

- Partitions consumed:
 - A partition 70 percent consumed generates a minor alarm.
 - A partition 80 percent consumed generates a major alarm.
 - A partition 90 percent consumed generates a critical alarm.

Table 3-1 Managing Hardware

Task	Sample Command
Running node reports	<code>report node node=prica42;</code> Note Results may take a few minutes to display.
Viewing nodes	<code>status node node=prica42;</code>
Rebooting the host machines	<code>control node node=prica42; action=REBOOT;</code>  Caution Use this command with extreme caution.
Setting the host machine for maintenance	<code>control node node=prica42; action=HALT;</code>  Caution Use local console access or a power cycle to restart the node.

Checking BTS System Health

Do the following tasks as listed or more frequently if your system administrator recommends it.

Table 3-2 BTS System Health Checklist

Tasks	Frequency
<input type="checkbox"/> Moving Core Files	as alarms are received
<input type="checkbox"/> Using BTS System-Health Reports	Daily
<input type="checkbox"/> Checking BTS System Time	Daily
<input type="checkbox"/> Checking Traffic Measurements See Chapter 6, “Using Measurements.”	Daily
<input type="checkbox"/> Checking Event and Alarm Reports See <i>Cisco BTS 10200 Softswitch Troubleshooting Guide, Release 6.0.3</i> .	Daily
<input type="checkbox"/> Checking the OS Log of Each Host Machine	Daily
<input type="checkbox"/> Backing up the EMS Database	Daily
<input type="checkbox"/> Checking Disk Mirroring on Each Host Machine	Weekly

Table 3-2 *BTS System Health Checklist (continued)*

<input type="checkbox"/>	Auditing Databases and Tables	Monthly
<input type="checkbox"/>	Cleaning Filters See equipment manufacturer's documentation.	Monthly
<input type="checkbox"/>	Archiving Your Database	See your system administrator
<input type="checkbox"/>	Backing Up the Software Image	Monthly
<input type="checkbox"/>	Examining Heap Usage	Quarterly
<input type="checkbox"/>	Running Diagnostic Procedures on Trunk Groups See Chapter 5, "Managing External Resources"	Quarterly
<input type="checkbox"/>	Running Diagnostic Procedures on Subscriber Terminations See Chapter 5, "Managing External Resources"	Quarterly
<input type="checkbox"/>	Running Network Loopback Tests for NCS/MGCP Endpoints See equipment manufacturer's documentation.	Quarterly
<input type="checkbox"/>	Creating Numbering Resource Utilization/Forecast (NRUF) Reports	Biannually

Using BTS System-Health Reports

The BTS allows you to gather data and create a report on its overall state. Use this data to find problems like hardware failures or traffic congestion.

Table 3-3 *Using BTS System-Health Reports*

Task	Sample Command
Viewing scheduled reports	<code>show scheduled-command verb=report; noun=system_health</code>
Viewing reports by ID number	<code>show scheduled-command ID=1</code>
Scheduling reports	<pre>add scheduled-command verb=report; noun=system_health; start-time=2003-10-01 12:22:22; recurrence=DAILY; keys=period; key-values=<1 ... 720>;</pre> <p>where:</p> <p>start-time—When BTS creates report, yyyy-mm-dd hh:mm:sss.</p> <p>recurrence—How often to run report (none (only once), daily, weekly, monthly)</p> <p>keys=period; key-values=<1 ... 720>;—How many hours back to collect data. If not specified, BTS uses default of 24 (last 24 hours worth of data).</p>
Changing reports	<code>change scheduled-command id=881958666704177006; start-time=2003-10-01 14:14:14; recurrence=DAILY; keys=period; key-values=24;</code>

Table 3-3 Using BTS System-Health Reports (continued)

Task	Sample Command
Deleting reports	<code>delete scheduled-command id=881958666704177006;</code>
Viewing completed reports	In a web browser enter <code>https://<active EMS IP addr or FQDN>:/report/system_health</code>
Generating a report immediately	<code>report system-health period=<1 ... 720>;</code> Note Results may take a few minutes to display.

Checking BTS System Time

BTS clocks must be accurate to 2 seconds.



Caution

Do not change the date or time in your BTS host machines while CA, FS, EMS, and BDMS are running. Instead allow the Solaris OS to get the time automatically through NTP services.

-
- Step 1** Log in to the primary and secondary EMSs as `root`.
 - Step 2** Enter `<hostname># date`.
 - Step 3** On each EMS ensure the following are correct:
 - a. The time does not deviate more than +/- 2 seconds.
 - b. Day, month, year, time zone
 - Step 4** Log in to both the primary and secondary CA as `root`.
 - Step 5** Enter `<hostname># date`.
 - Step 6** On each CA ensure the following are correct:
 - a. The time is accurate to within +/-2 seconds of the correct time.
 - b. Day, month, year, time zone
-

Checking the OS Log of Each Host Machine

Monitor the OS logs on all four host machines (primary and secondary EMS, primary and secondary CA) for errors or warnings. This report shows you recent messages like memory hits, disk errors, and frequent process restarts.

-
- Step 1** Log in as `root`.
 - Step 2** Enter `dmesg`.
 - Step 3** For more history edit the `/var/adm/messages` file.
-

Checking Disk Mirroring on Each Host Machine

Each procedure takes about 30 minutes.

CA/FS Side A

Before doing this procedure, ensure your BTS platform is connected to controller 1 or controller 0.

Step 1 Log in as `root` to CA/FS side A using telnet.

Step 2 Enter one of the following:

```
<hostname># metastat | grep c0
```

Or:

```
<hostname># metastat | grep c1
```

Step 3 Verify the return matches the following:

```
c1t0d0s1      0      No      Okay   Yes
c1t1d0s1      0      No      Okay   Yes
c1t0d0s5      0      No      Okay   Yes
c1t1d0s5      0      No      Okay   Yes
c1t0d0s6      0      No      Okay   Yes
c1t1d0s6      0      No      Okay   Yes
c1t0d0s0      0      No      Okay   Yes
c1t1d0s0      0      No      Okay   Yes
c1t0d0s3      0      No      Okay   Yes
c1t1d0s3      0      No      Okay   Yes
c1t1d0      Yes   id1,sd@SSEAGATE_ST373307LSUN72G_3HZ9JG7800007518H8WV
c1t0d0      Yes   id1,sd@SSEAGATE_ST373307LSUN72G_3HZ9JC9N00007518Y15K
```

If the results differ synchronize the disk mirroring:

```
<hostname># cd /opt/setup
<hostname># sync_mirror
```

Verify the results using Step 1 through Step 3.



Caution

In case of a mismatch, synchronize once. If the mismatch continues, contact Cisco TAC.

CA/FS Side B

Step 1 Log in as `root` to CA/FS side B using telnet.

Step 2 Enter `<hostname># metastat | grep c0`.

Step 3 Verify the return matches the following:

```
c0t0d0s6 0 No Okay
c0t1d0s6 0 No Okay
c0t0d0s1 0 No Okay
c0t1d0s1 0 No Okay
c0t0d0s5 0 No Okay
c0t1d0s5 0 No Okay
```

```

c0t0d0s7 0 No Okay
c0t1d0s7 0 No Okay
c0t0d0s0 0 No Okay
c0t1d0s0 0 No Okay
c0t0d0s3 0 No Okay
c0t1d0s3 0 No Okay

```

If the results differ synchronize the disk mirroring:

```

<hostname># cd /opt/setup
<hostname># sync_mirror

```

Verify the results using Step 1 through Step 3.



Caution

In case of a mismatch, synchronize once. If the mismatch continues contact Cisco TAC.

EMS Side A

Step 1 Log in as `root` to EMS side A using telnet.

Step 2 Enter `<hostname># metastat | grep c0`.

Step 3 Verify the return matches the following:

```

c0t0d0s6 0 No Okay
c0t1d0s6 0 No Okay
c0t0d0s1 0 No Okay
c0t1d0s1 0 No Okay
c0t0d0s5 0 No Okay
c0t1d0s5 0 No Okay
c0t0d0s7 0 No Okay
c0t1d0s7 0 No Okay
c0t0d0s0 0 No Okay
c0t1d0s0 0 No Okay
c0t0d0s3 0 No Okay
c0t1d0s3 0 No Okay

```

If the results differ synchronize the disk mirroring:

```

<hostname># cd /opt/setup
<hostname># sync_mirror

```

Verify the results using Step 1 through Step 3.



Caution

In case of a mismatch, synchronize once. If the mismatch continues contact Cisco TAC.

EMS Side B

Step 1 Log in as `root` to EMS side B using telnet.

Step 2 Enter `<hostname># metastat | grep c0`.

Step 3 Verify the return result matches the following:

```
c0t0d0s6 0 No Okay
c0t1d0s6 0 No Okay
c0t0d0s1 0 No Okay
c0t1d0s1 0 No Okay
c0t0d0s5 0 No Okay
c0t1d0s5 0 No Okay
c0t0d0s7 0 No Okay
c0t1d0s7 0 No Okay
c0t0d0s0 0 No Okay
c0t1d0s0 0 No Okay
c0t0d0s3 0 No Okay
c0t1d0s3 0 No Okay
```

If the results differ synchronize the disk mirroring:

```
<hostname># cd /opt/setup
<hostname># sync_mirror
```

Verify the results using Step 1 through Step 3.



Caution

In case of a mismatch, synchronize once. If the mismatch continues contact Cisco TAC.

Auditing Databases and Tables

Audit either the complete database or entries in every provisionable table in both the Oracle database and shared memory. See the *Cisco BTS 10200 Softswitch Troubleshooting Guide, Release 6.0.3*.



Caution

Audits are time-intensive. Do only during a maintenance window. Completion time varies with database or table entries.

Table 3-4 Auditing Databases and Tables

Task	Sample Command
Auditing individual tables	<code>audit trunk type=row-count;</code>
Auditing every entry in each provisionable table	<code>audit database;</code>
Auditing provisionable tables based on type	<code>audit database type=row-count;</code> Note type defaults to <code>full</code>
Auditing provisionable tables based on platform state	<code>audit database platform-state=active;</code> Note <code>platform-state</code> defaults to <code>active</code>

Table 3-4 Auditing Databases and Tables (continued)

Task	Sample Command
Auditing mismatches across network elements	<ol style="list-style-type: none"> 1. Log in as <code>root</code>. 2. Enter: <pre>bts_audit -ems priems01 -ca prica01 -platforms CA146,FSAIN205 -tables SUBSCRIBER,MGW_PROFILE</pre> <p>Note <code>bts_audit</code> cannot work in certain scenarios, for example, when a termination record points to an invalid <code>mgw</code></p>
Resolving mismatches across network elements	<p>If a table references a missing row, the mismatch is not resolved. Only synchronize data mismatches between active network elements.</p> <ol style="list-style-type: none"> 1. Audit mismatches using <code>bts_audit</code>. 2. Enter: <pre>bts_sync /opt/ems/report/Audit_CA146_root.sql</pre> <p><code>bts_sync</code> applies updates directly to the databases.</p>

Exporting Provisioned Data

The CLI Native Data Export feature enables the export of all provisioning data from the BTS 10200 system by the use of a CLI command. Execution of the CLI command stores the exported data in a user-named output file in text format in the export directory. The exported file contains all provisioning data from the BTS 10200. The provisioning data is written into the export file using **add** and **change** commands for all supported nouns.

The key attributes of the CLI Native Data Export feature are

- The user can run the CLI command to export the BTS 10200 provisioning data.
- The provisioning data for all the nouns, which enables the use of verbs as “add” and “change” is exported in text format.
- The list of all the nouns related to provisioning is kept in an input file (xml format). Upon execution of the **export** command, the xml input file reads the nouns and their corresponding verbs (operation type, whether add or change), and exports the provisioning data from the BTS 10200.

The CLI export command is:

```
CLI > export database outfile = <whatever>
```

Where the noun is `database` and the verb is `export`. Execution of the command exports all of the provisioning data from the BTS 10200. All of the exported data is written in the output file as specified by the user. The output file contains all the **add** and **change** commands for the existing native data in the BTS 10200. The exported output file is stored in the `/opt/ems/export` directory.

The result of the **export** command is a text file that contains add/change CLI commands. The following is an example output text file:

```
# BTS Config Export
# EMS Server: priems26-ora
# User: optiuser
# Export Start Time : Tue Jan 22 17:23:54 CST 2008

#####
##### Add clli_code #####
```

```

#####
add clli_code ID=ABCD1234567;

#####
#### Add call_agent ####
#####
add call_agent id=CA146;tsap_addr=CA146.A.12345678901234567890123456789012345678
901234567890123456;mgw_monitoring_enabled=N;clli=ABCD1234567;

#####
#### Add feature_server ####
#####
add feature_server ID=FSAIN205;TSAP_ADDR=FSAIN.A.1234567890123456789012345678901
2345678901234567890123456;TYPE=AIN;DESCRIPTION=123456789012345678901234567890123
456789012345678901234567890ABCD;EXTERNAL_FEATURE_SERVER=N;
add feature_server ID=FSPTC235;TSAP_ADDR=FSPTC.A.1234567890123456789012345678901
2345678901234567890123456;TYPE=POTS;DESCRIPTION=12345678901234567890123456789012
3456789012345678901234567890ABCD;EXTERNAL_FEATURE_SERVER=N;

#####
#### Change billing_acct_addr ####
#####

#####
#### Change billing_alarm ####
#####

#####
#### Change report_properties ####
#####
change report_properties TYPE=EVENT_LOGSIZE;VALUE=30000;
change report_properties TYPE=ALARM_LOGSIZE;VALUE=30000;
change report_properties TYPE=EVENT_LEVEL;VALUE=INFO;

#####
#### Change sup_config ####
#####
change sup_config TYPE=refresh_rate;VALUE=86400;
change sup_config TYPE=priority;VALUE=5;
change sup_config TYPE=subterm_mgw_block;VALUE=5;
change sup_config TYPE=subterm_block_pause;VALUE=9000;
change sup_config TYPE=subterm_status_pause;VALUE=0;
change sup_config TYPE=trunkterm_tg_block;VALUE=5;
change sup_config TYPE=trunkterm_block_pause;VALUE=9000;
change sup_config TYPE=trunkterm_status_pause;VALUE=0;
change sup_config TYPE=trunkterm_range_block;VALUE=1000;
change sup_config TYPE=trunkterm_range_pause;VALUE=20000;

```

```
#####
#### Change command_throttle_threshold ####
#####
change command_throttle_threshold SESSION_TYPE=CLI;THRESHOLD=100;ENABLE=Y;
change command_throttle_threshold SESSION_TYPE=CORBA;THRESHOLD=100;ENABLE=Y;
change command_throttle_threshold SESSION_TYPE=FTP;THRESHOLD=1000;ENABLE=Y;
change command_throttle_threshold SESSION_TYPE=MNT;THRESHOLD=100;ENABLE=Y;
change command_throttle_threshold SESSION_TYPE=SNMP;THRESHOLD=100;ENABLE=Y;
change command_throttle_threshold SESSION_TYPE=SOAP;THRESHOLD=100;ENABLE=Y;

#####
#### Change config_interval ####
#####
change config_interval CONFIG_TYPE=THROTTLE;INTERVAL=15;

# Export End Time : Tue Jan 22 17:24:14 CST 2008
```

Limitations

Currently the **export** command is supported only from the CLI interface. The **export** command is currently not supported from other interfaces such as CORBA and SOAP.

There is a limitation on the size of the /opt/ems/export directory. Currently the size of the export directory is defined in /opt/ems/etc/bts.properties as 7500000 ~ 700 MB. During the first run of the **export** command, if the size of the export file is beyond the threshold limit, a warning message is shown to the user after export is finished. The warning message indicates that the export file size has exceeded the threshold and that the user needs to clean up the export directory before running the command again. During additional runs of the **export** command, if the export directory size is more than the threshold size, a warning is shown to the user that the space of export directory is insufficient for the export and that the user has to clear the export directory before rerunning the **export** command.

Creating Numbering Resource Utilization/Forecast (NRUF) Reports

The North American Numbering Plan Association (NANPA) collects, stores, and maintains how telephone numbers are used by 19 countries. Companies, like carriers, that hold telephone numbers must report to NANPA twice a year using the NRUF report. Go to <http://www.nanpa.com> for more information and job aids on submitting reports.

The BTS creates an NRUF report using the Number Block table. This table:

- Is a single table that is the sole reference for NANPA audits
- Can be customized
- Can be updated from data imported from other tables, changes from office-code updates, or manually
- Has the following fields:
 - Number Block: NPA to NPA-NXX-XXXX—For FCC-required NANPA audit compliance, the report input is NPANXX. In markets outside of NANPA, the input can be based on either the combination of the national destination code (NDC) and the exchange code (EC), or just the EC.
 - Code Holder = Y/N
 - Block Holder = Y/N
 - Native = Y/N

- Non-Native = Y/N

To generate the following reports, use `report dn-summary`:

- All DNs in NDC and EC
- Thousands group in NDC and EC
- Operating company number (OCN)
- Switch Common Language Location Identifier (CLLI) code
- OCN + CLLI code—entries must match LERG data

Creating Reports for Nonrural Primary and Intermediate Carriers

NRUF reporting for nonrural primary and intermediate carriers:

- Occurs at a thousands-block level (NPA-NXX-X)
- Applies only to NANP

The report returns the following based on the DN2SUBSCRIBER table's STATUS token:

Table 3-5 NRUF Report Data for Nonrural Carriers

Data Groups	Matching Data from the DN2SUBSCRIBER Table
Assigned DNs	<ul style="list-style-type: none"> • Individual DNs: <pre>ndc=<npa>; ec=<nxx>; DN=[0-9][0-9][0-9]; (status=assigned) AND ADMIN-DN=N ndc=<npa>; ec=<nxx>; DN=[0-9][0-9][0-9]; (status=ported-out) AND ADMIN-DN=N</pre> • DID DNs: <pre>ndc=<npa>; ec=<nxx>; DN=xxxx; (status=assigned) AND ADMIN-DN=N; X 1000 ndc=<npa>; ec=<nxx>; DN=xxxx; (status=ported-out) AND ADMIN-DN=N; X 1000 ndc=<npa>; ec=<nxx>; DN=[0-9]xxx; (status=assigned) AND ADMIN-DN=N; X 1000 ndc=<npa>; ec=<nxx>; DN=[0-9]xxx; (status=ported-out) AND ADMIN-DN=N; X 1000 ndc=<npa>; ec=<nxx>; DN=[0-9][0-9]xx; (status=assigned) AND ADMIN-DN=N; X 100 ndc=<npa>; ec=<nxx>; DN=[0-9][0-9]xx; (status=ported-out) AND ADMIN-DN=N; X 100 ndc=<npa>; ec=<nxx>; DN=[0-9][0-9][0-9]x; (status=assigned) AND ADMIN-DN=N; X 10 ndc=<npa>; ec=<nxx>; DN=[0-9][0-9][0-9]x; (status=ported-out) AND ADMIN-DN=N; X 10</pre> • PORTED-OUT DNs
Intermediate Telephone Directory Numbers	0
Reserved DNs	0

Table 3-5 NRUF Report Data for Nonrural Carriers (continued)

Data Groups	Matching Data from the DN2SUBSCRIBER Table
Aging DNs	<ul style="list-style-type: none"> • DISC DNs: <code>ndc=<npa>; ec=<nxx>; DN=[0-9][0-9][0-9][0-9]; (status=DISC)</code> • Changed Number DNs: <code>ndc=<npa>; ec=<nxx>; DN=[0-9][0-9][0-9][0-9]; (status=CN)</code> • DISC DID DNs: <code>ndc=<npa>; ec=<nxx>; DN=xxxx; (status=DISC) X 10000</code> <code>ndc=<npa>; ec=<nxx>; DN=[0-9]xxx; (status=DISC) X 1000</code> <code>ndc=<npa>; ec=<nxx>; DN=[0-9][0-9]xx; (status=DISC) X 100</code> <code>ndc=<npa>; ec=<nxx>; DN=[0-9][0-9][0-9]x; (status=DISC) X 10</code> • Changed Number DID DNs: <code>ndc=<npa>; ec=<nxx>; DN=xxxx; (status=CN) X 10000</code> <code>ndc=<npa>; ec=<nxx>; DN=[0-9]xxx; (status=CN) X 1000</code> <code>ndc=<npa>; ec=<nxx>; DN=[0-9][0-9]xx; (status=CN) X 100</code> <code>ndc=<npa>; ec=<nxx>; DN=[0-9][0-9][0-9]x; (status=CN) X 10</code>
Administrative DNs	<ul style="list-style-type: none"> • Administrative DNs: <code>ndc=<npa>; ec=<nxx>; status=LRN;</code> <code>ndc=<npa>; ec=<nxx>; status=CLRN</code> <code>ndc=<npa>; ec=<nxx>; status=RACF-DN;</code> <code>ndc=<npa>; ec=<nxx>; status=ANNC;</code> <code>ndc=<npa>; ec=<nxx>; status=TEST-LINE;</code> <code>ndc=<npa>; ec=<nxx>; (ADMIN-DN=Y AND (status=ASSIGNED))</code> <code>ndc=<npa>; ec=<nxx>; (ADMIN-DN=Y AND (status=PORTED-OUT))</code> • Administrative DID DNs: <code>ndc=<npa>; ec=<nxx>; DN=xxxx; (ADMIN-DN=Y AND (status=ASSIGNED)) X 10000</code> <code>ndc=<npa>; ec=<nxx>; DN=xxxx; (ADMIN-DN=Y AND (status=PORTED-OUT)) X 10000</code> <code>ndc=<npa>; ec=<nxx>; DN=[0-9]xxx (ADMIN-DN=Y AND (status=ASSIGNED)) X 1000</code> <code>ndc=<npa>; ec=<nxx>; DN=[0-9]xxx (ADMIN-DN=Y AND (status=PORTED-OUT)) X 1000</code> <code>ndc=<npa>; ec=<nxx>; DN=[0-9][0-9]xx; (ADMIN-DN=Y AND (status=ASSIGNED)) X 100</code> <code>ndc=<npa>; ec=<nxx>; DN=[0-9][0-9]xx; (ADMIN-DN=Y AND (status=PORTED-OUT)) X 100</code> <code>ndc=<npa>; ec=<nxx>; DN=[0-9][0-9][0-9]x; (ADMIN-DN=Y AND (status=ASSIGNED)) X 10</code> <code>ndc=<npa>; ec=<nxx>; DN=[0-9][0-9][0-9]x; (ADMIN-DN=Y AND (status=PORTED-OUT)) X 10</code> • Changed Number administrative DNs

Creating Reports for Rural Primary and Intermediate Carriers

This section identifies the DN information that is reported at the NPA-NXX level when the service provider is a code holder. NRUF reporting at the “ndc, ec” level includes dn-groups of varying length. Some countries might support dn-groups of length 1, 2, 3 or 4.

- The Rural Primary Carrier (U2 form) NPA-NXX report has:
 - NPA-NXX (input as ndc, ec)
 - Rate Center (read from LERG)
 - State (read from LERG)
 - Number of Assigned DNs
 - Number of Intermediate DNs
 - Number of Reserved DNs
 - Number of Aging DNs
 - Number of Administrative DNs
 - Donated to Pool (always 0)

- The Rural Intermediate Carrier (U4 form) report has:
 - NPA-NXX (input as ndc, ec)
 - Rate Center (read from LERG)
 - State (read from LERG)
 - Number of Assigned DNs
 - Number of Intermediate DNs
 - Number of Reserved DNs
 - Number of Aging DNs
 - Number of Administrative DNs
 - Numbers Received (always 0)

The report returns the following based on the DN2SUBSCRIBER table's STATUS token:

Table 3-6 NRUF Report Data for Rural Carriers

Data Groups	Matching Data from the DN2SUBSCRIBER Table
Assigned DNs	<ul style="list-style-type: none"> • Individual DNs: <pre>ndc=<npa>; ec=<nxx>; DN=[0-9][0-9][0-9]; (status=assigned) AND ADMIN-DN=N ndc=<npa>; ec=<nxx>; DN=[0-9][0-9][0-9]; (status=ported-out) AND ADMIN-DN=N</pre> • DID DNs: <pre>ndc=<npa>; ec=<nxx>; DN=xxxx; (status=assigned) AND ADMIN-DN=N; X 10000 ndc=<npa>; ec=<nxx>; DN=xxxx; (status=ported-out) AND ADMIN-DN=N; X 10000 ndc=<npa>; ec=<nxx>; DN=[0-9]xxx; (status=assigned) AND ADMIN-DN=N; X 1000 ndc=<npa>; ec=<nxx>; DN=[0-9]xxx; (status=ported-out) AND ADMIN-DN=N; X 1000 ndc=<npa>; ec=<nxx>; DN=[0-9][0-9]xx; (status=assigned) AND ADMIN-DN=N; X 100 ndc=<npa>; ec=<nxx>; DN=[0-9][0-9]xx; (status=ported-out) AND ADMIN-DN=N; X 100 ndc=<npa>; ec=<nxx>; DN=[0-9][0-9][0-9]x; (status=assigned) AND ADMIN-DN=N; X 10 ndc=<npa>; ec=<nxx>; DN=[0-9][0-9][0-9]x; (status=ported-out) AND ADMIN-DN=N; X 10</pre>
Intermediate Telephone Directory Numbers	0
Reserved DNs	0

Table 3-6 NRUF Report Data for Rural Carriers (continued)

Data Groups	Matching Data from the DN2SUBSCRIBER Table
Aging DNs	<ul style="list-style-type: none"> • DISC DNs: <code>ndc=<npa>; ec=<nxx>; DN=[0-9][0-9][0-9][0-9]; (status=DISC)</code> • Changed Number DNs: <code>ndc=<npa>; ec=<nxx>; DN=[0-9][0-9][0-9][0-9]; (status=CN)</code> • DISC DID DNs: <code>ndc=<npa>; ec=<nxx>; DN=xxxx; (status=DISC) X 10000</code> <code>ndc=<npa>; ec=<nxx>; DN=[0-9]xxx; (status=DISC) X 1000</code> <code>ndc=<npa>; ec=<nxx>; DN=[0-9][0-9]xx; (status=DISC) X 100</code> <code>ndc=<npa>; ec=<nxx>; DN=[0-9][0-9][0-9]x; (status=DISC) X 10</code> • Changed Number DID DNs: <code>ndc=<npa>; ec=<nxx>; DN=xxxx; (status=CN) X 10000</code> <code>ndc=<npa>; ec=<nxx>; DN=[0-9]xxx; (status=CN) X 1000</code> <code>ndc=<npa>; ec=<nxx>; DN=[0-9][0-9]xx; (status=CN) X 100</code> <code>ndc=<npa>; ec=<nxx>; DN=[0-9][0-9][0-9]x; (status=CN) X 10</code>
Administrative DNs	<ul style="list-style-type: none"> • Administrative DNs: <code>ndc=<npa>; ec=<nxx>; status=LRN;</code> <code>ndc=<npa>; ec=<nxx>; status=CLRN</code> <code>ndc=<npa>; ec=<nxx>; status=RACF-DN;</code> <code>ndc=<npa>; ec=<nxx>; status=ANNC;</code> <code>ndc=<npa>; ec=<nxx>; status=TEST-LINE;</code> <code>ndc=<npa>; ec=<nxx>; (ADMIN-DN=Y AND (status=ASSIGNED))</code> <code>ndc=<npa>; ec=<nxx>; (ADMIN-DN=Y AND (status=PORTED-OUT))</code> • Administrative DID DNs: <code>ndc=<npa>; ec=<nxx>; DN=xxxx; (ADMIN-DN=Y AND (status=ASSIGNED)) X 10000</code> <code>ndc=<npa>; ec=<nxx>; DN=xxxx; (ADMIN-DN=Y AND (status=PORTED-OUT)) X 10000</code> <code>ndc=<npa>; ec=<nxx>; DN=[0-9]xxx (ADMIN-DN=Y AND (status=ASSIGNED)) X 1000</code> <code>ndc=<npa>; ec=<nxx>; DN=[0-9]xxx (ADMIN-DN=Y AND (status=PORTED-OUT)) X 1000</code> <code>ndc=<npa>; ec=<nxx>; DN=[0-9][0-9]xx; (ADMIN-DN=Y AND (status=ASSIGNED)) X 100</code> <code>ndc=<npa>; ec=<nxx>; DN=[0-9][0-9][0-9]xx; (ADMIN-DN=Y AND (status=PORTED-OUT)) X 100</code> <code>ndc=<npa>; ec=<nxx>; DN=[0-9][0-9][0-9]x; (ADMIN-DN=Y AND (status=ASSIGNED)) X 10</code> <code>ndc=<npa>; ec=<nxx>; DN=[0-9][0-9][0-9]x; (ADMIN-DN=Y AND (status=PORTED-OUT)) X 10</code>

Backing Up the Software Image

To back up the software image do the following three procedures:

1. [Full Database Auditing, page 3-16](#)
2. [Checking Shared Memory, page 3-16](#)
3. [Backing Up the Full BTS, page 3-18](#)

Full Database Auditing

-
- Step 1** Log in as CLI user on EMS side A.
 - Step 2** Enter `audit database type=full;`.
 - Step 3** Check the audit report and verify that there is no mismatch or error. If errors are found, try to correct the errors. If you cannot make the correction, contact Cisco TAC.
-

Checking Shared Memory

This task checks shared memory to detect potential data problems.

From CA/FS Side A

-
- Step 1** Log in as `root`.
 - Step 2** Enter:


```
<hostname># cd /opt/OptiCall/CAxxx/bin
<hostname># ca_tiat data
```

Press **Enter**.

The result should match the following:

```
All tables are OK.
For details, see ca_tiat.out
```



Caution If the result is not “All tables are OK”, stop and contact Cisco TAC. If the result is “All tables are OK”, go to [Step 3](#).

- Step 3** Enter:


```
<hostname># cd /opt/OptiCall/FSPTCzzz/bin <Return>
<hostname># potsctx_tiat data <Return>
```

Press **Enter**.

The result should match the following:

```
All tables are OK.
For detail, see potsctx_tiat.out
```



Caution If the result is not “All tables are OK”, stop and contact Cisco TAC. If the result is “All tables are OK”, go to [Step 4](#).

- Step 4** Enter:


```
<hostname>#cd /opt/OptiCall/FSAINyyy/bin
<hostname>#ain_tiat data
```
- Step 5** Press **Enter**.

The result should match the following:

```
All tables are OK.
For detail, see ain_tiat.out
```



Caution If the result is not “All tables are OK”, stop and contact Cisco TAC.

From CA/FS Side B

Step 1 Log in as `root`.

Step 2 Enter:

```
<hostname>#cd /opt/OptiCall/CAxxx/bin
<hostname>#ca_tiat data
```

Step 3 Press `Enter`.

The result should match the following:

```
All tables are OK.
For detail, see ca_tiat.out
```



Caution If the result is not “All tables are OK”, stop and contact Cisco TAC. If the result is “All tables are OK”, go to [Step 3](#).

Step 4 Enter:

```
<hostname>#cd /opt/OptiCall/FSPTCzzz/bin
<hostname>#potsctx_tiat data
```

Step 5 Press `Enter`:

The result match the following:

```
All tables are OK.
For detail, see potsctx_tiat.out
```



Caution If the result is not “All tables are OK”, stop and contact Cisco TAC. If the result is “All tables are OK”, go to [Step 6](#).

Step 6 Enter:

```
<hostname>#cd /opt/OptiCall/FSAINyyy/bin
<hostname>#ain_tiat data
```

Step 7 Press `Enter`:

The result should match the following:

```
All tables are OK.
For detail, see ain_tiat.out
```

**Caution**

If the result is not “All tables are OK”, stop and contact Cisco TAC.

Backing Up the Full BTS

Do this before and after software upgrades or as routine, always during a maintenance window. Before starting the provisioning process ensure you have the following:

Pre-Provisioning Checklist

- | | |
|--------------------------|-----------------------------------|
| <input type="checkbox"/> | NFS server hostname or ip address |
| <input type="checkbox"/> | Shared directory from NFS server |
| <input type="checkbox"/> | Root user access |
| <input type="checkbox"/> | Provisioning blocked |

Backing Up the CA/FS

Perform the following steps to back up the secondary CA/FS. Then repeat the procedure on the primary CA/FS.

-
- Step 1** Log in as **root** on the secondary CA/FS.
- Step 2** Verify all platforms are in STANDBY mode, enter `<hostname>#nodestat`.
- Step 3** Remove unnecessary files or directories like `/opt/Build` and application tar files.
- Step 4** Mount the NFS server to the `/mnt` directory, enter `<hostname>#mount <nfs server ip or hostname>:/<share dire> /mnt`.
- Step 5** Stop all platforms; enter `<hostname>#platform stop all`.
- Step 6** Save all platforms data directory (shared memory) to nfs server

```
<hostname>#tar -cf - /opt/OptiCall/CAxxx/bin/data |gzip -fast - > /mnt/data.<hostname>.CA
<<hostname>#tar -cf - /opt/OptiCall/CAxxx/bin/data |gzip --fast - >
/mnt/data.<hostname>.CA.gz
<hostname>#tar -cf - /opt/OptiCall/FSAINxxx/bin/data |gzip --fast - >
/mnt/data.<hostname>.FSAIN.gz
<hostname>#tar -cf /opt/OptiCall/FSPTCxxx/bin/data |gzip --fast - >
/mnt/data.<hostname>.FSPTC.gz
```

where xxx is the instance number

- Step 7** Start all platforms by entering `<hostname>#platform start`.
- Step 8** Verify all platforms are in STANDBY mode, enter `<hostname>#nodestat`.
- Step 9** Create an excluded directories file for the flash archive, enter:

```
<hostname>#vi /tmp/excluded_dir
/opt/OptiCall/CAxxx/bin/data
/opt/OptiCall/CAxxx/bin/logs
```



```

/opt/OptiCall/FSAINxxx/bin/data
/opt/OptiCall/FSAINxxx/bin/logs
/opt/OptiCall/FSPTCxxx/bin/data
/opt/OptiCall/FSPTCxxx/bin/logs

```

where xxx is the instance number

Step 10 Back up the system, enter:

```

<hostname>#mv /bin/date /bin/date.archive
<hostname>#mv /bin/.date /bin/date
<hostname>#flarcreate -n <hostname> -X /tmp/excluded_dir -c /mnt/<hostname>.archive
<hostname>#mv /bin/date /bin/.date
<hostname>#mv /bin/date.archive /bin/date

```

Step 11 Unmount the NFS server, enter:

```

<hostname>#umount /mnt

```

Step 12 From the active EMS switch over all platforms, enter:

```

<hostname>#ssh optiuser@<hostname>
cli>control feature-server id=FSAINxxx;target-state=standby-active;
cli>control feature-server id=FSPTCxxx;target-state=standby-active;
cli>control call-agent id=CAxxx;target-state=standby-active;

```

where xxx is the instance number of each platform

Step 13 Repeat this procedure for the primary CA/FS.

Backing up the EMS/BDMS

Do the following to back up the STANDBY EMS/BDMS system.

Step 1 Log in as root.

Step 2 Verify all platforms are in STANDBY mode, enter `<hostname>#nodestat`.

Step 3 Remove unnecessary files or directories like /opt/Build and application tar files.

Step 4 Mount the NFS server to the /mnt directory, enter `<hostname>#mount <nfs server ip or hostname>:<share dire> /mnt`.

Step 5 Stop all platforms, enter `<hostname>#platform stop all`.

Step 6 Save the Oracle database and MySQL directories, enter:

```

<hostname>#tar -cf - /data1/oradata |gzip --fast - >/mnt/oradata.<hostname>.gz
<hostname>#tar -cf - /opt/ems/db |gzip --fast - >/mnt/db.<hostname>.gz

```

Step 7 Create an excluded directories file for the flash archive, enter:

```

<hostname>#vi /tmp/excluded_dir
/data1/oradata

```

Step 8 Start all platforms `<hostname>#platform start`.

Step 9 Verify all platforms are in STANDBY mode, enter `<hostname>#nodestat`.

Step 10 Back up the system, enter:

```

<hostname>#mv /bin/date /bin/date.archive
<hostname>#mv /bin/.date /bin/date

```

```
<hostname>#flarccreate -n <hostname> -X /tmp/excluded_dir -c /mnt/<hostname>.archive
<hostname>#mv /bin/date /bin/.date
<hostname>#mv /bin/date.archive /bin/date
```

Step 11 Unmount the NFS server, enter `<hostname>#umount /mnt`.

Step 12 From the active EMS switch over all platforms, enter:

```
<hostname>#ssh optiuser@<hostname>
cli>control bdms id=BDMS01;target-state=standby-active;
cli>control element-manager id=EM01;target-state=standby-active;
```

Step 13 Repeat the procedure starting with Step 3 to back up the PRIMARY EMS/BDMS.

Backing up the EMS Database

This procedure is for experienced UNIX users. It tells you how to save the provisioning database from the EMS to a remote server. The remote server must be:

- Connected to a corporate LAN.
- Backed up daily by default, the daily hot backup is not turned on at installation

The back up processes:

- `ora_hot_backup.ks`—Backs up database data files, control files, and archive logs
- `ora_arch_backup.ksh`—Backs up archive logs

The target backup directory on both primary and secondary EMS systems is `/opt/oraback`. Backup files in `/opt/oraback` directory are later transferred to the `/opt/backup` directory in a remote archive site. After the files are transferred, they are purged from `/opt/oraback`.

Step 1 Cross check the databases on the primary and secondary EMSs before backing up.



Caution Cross check before `ora_hot_backup.ksh` and `ora_arch_backup.ksh` are scheduled. This validates database and archived log files for RMAN processes.

- Log in as `oracle`, or `su - oracle`.
- Enter `dbadm -E backup_crosscheck..`
- Ensure the log file has no errors (except the “validation failed for archived log” messages). Ignore these messages of the `/data1/arch/opticalx_yyy.arc` files because the validation directs RMAN not to look for `*.arc` files. `ora_purge_archlog.ksh` purges `*.arc` files.

```
RMAN-06157: validation failed for archived log
RMAN-08514: archive log filename=/data1/arch/optical1_25.arc recid=1 stamp=461878656
```

Step 2 Remove the archive log purge process and schedule the backup processes.



Note Do this on the primary and secondary EMSs.

- Disable the `ora_purge_archlog.ksh` process.
- Enable the `ora_hot_backup.ksh` process.

- c. Optional: Enable the `ora_arch_backup.ksh` process.
- d. Log in as `oracle`, or `su - oracle`.
- e. Enter `crontab -e`.
- f. Modify the crontab file as follows. This is on the primary EMS site, database name *optical1*.

```
# Daily Oracle Hot backup - this also include archive log backup
#     Note: Set hot backup process to run at 2:00am every day.
#
0 2 * * * /opt/oracle/admin/scripts/ora_hot_backup.ksh optical1 > /opt/oracle/t
mp/ora_hot_backup.log 2>&1
#
# Oracle archive log backups, in addition to daily hot backup.
#     Note: Set one additional archive log backup to run at 6:00pm every day.
#
0 18 * * * /opt/oracle/admin/scripts/ora_arch_backup.ksh optical1 > /opt/
oracle/tmp/ora_arch_backup.log 2>&1
#
# Purge archive log files
#     Note: Delete or uncomment this line to stop purging archive log files.
#
#0 1,3,...,23 * * * /opt/oracle/admin/scripts/ora_purge_archlog.ksh optical1 >
/opt/oracle/tmp/ora_purge_archlog.log 2>&1
```

- g. Repeat Step f by replacing *optical1* with *optical2* on the secondary EMS site.

- Step 3** To setup daily file transfer to the remote archive site using FTP, see [Using FTP to Setup File Transfer](#). To setup daily file transfer to the remote archive site using SFTP, see [Using SFTP to Setup File Transfer](#).

Using FTP to Setup File Transfer

- Step 1** Configure the remote site.

- a. Verify the oracle user access and create backup directory on FTP server site.

```
Primary EMS hostname:      priems
Secondary EMS hostname:    secems
FTP server hostname:       ftpserver
FTP server Oracle password: ora00
FTP server backup directory: /opt/backup
```

First, test the connection to the remote FTP server using the *oracle* user access. If the password of *oracle* is not 'ora00', update the `ORA_PW` variable in the `/opt/oracle/admin/etc/dba.env` file.

- b. Do this on the primary and secondary EMSs:


```
telnet ftpserver
```
- c. Log in as `oracle` and enter the password (in this case, `ora00`).
- d. Create the `/opt/backup` directory. Ensure the `oracle` user has write permission to this directory.

```
mkdir /opt/backup
```



Note It is your responsibility to archive backup files from the ftp server `/opt/backup` directory to a tape device or enterprise tape library.

Step 2 Schedule the FTP process.

a. Do this on the primary and secondary EMSs:

Log in as `oracle`, or `su - oracle` and enter the following command: `crontab -e`

b. Add the following line to the Oracle crontab on the primary EMS.

```
#
# FTP backup files from primary (optical1) to /opt/backup directory of ftpserver.
#
0 6 * * * /opt/oracle/admin/scripts/ora_ftp_backup.ksh optical1 ftpserver /opt/backup >
/opt/oracle/tmp/ora_ftp_backup.log 2>&1
```

c. Replace `ftpserver` with the correct host name of the remote FTP server. Replace `/opt/backup` with the correct target directory name, if they are different.



Note The `0 6 *** /opt/oracle/admin/scripts/ora_ftp_backup.ksh ora_ftp_backup.log 2>&1` are all typed in the same line.

d. Edit the oracle crontab on secondary EMS site by replacing `optical1` with `optical2`.

Step 3 Verify the backup files, enter:

```
cd /opt/oraback      | EMS systems
cd /opt/backup      | Remote FTP system
```

Using SFTP to Setup File Transfer

The following steps generate an SSH key from the primary EMS. Key files are copied to the secondary EMS and remote SFTP server. On the remote SFTP server the "oracle" user is created for login.

Step 1 Generate SSH secure key from primary EMS:

a. Login to the primary EMS:

```
# su - oracle
# /opt/BTSossh/bin/ssh-keygen -t rsa
```

b. Generating public/private rsa key pair.

c. Enter file in which to save the key (`/opt/orahome/.ssh/id_rsa`).

d. Enter passphrase (empty for no passphrase).

e. Enter same passphrase.

Your identification has been saved in `/opt/orahome/.ssh/id_rsa`.

Your public key has been saved in `/opt/orahome/.ssh/id_rsa.pub`.

The key fingerprint is: `d8:4f:b1:8b:f4:ac:2f:78:e9:56:a4:55:56:11:e1:40 oracle@priems79`

f. Enter:

```
# ls -l /opt/orahome/.ssh
-rw-----1 oracleorainst1675 Mar 10 15:42 id_rsa
-rw-r--r--1 oracleorainst397 Mar 10 15:42 id_rsa.pub
```

Step 2 From the secondary EMS, `sftp` both "id_ssa" and "id_rsa.pub" files from the primary EMS to the secondary EMS `/opt/orahome/.ssh` directory. Make the files with "oracle:orainst" ownership.

Step 3 Login to the secondary EMS:

```
# su - oracle
$ cd /opt/orahome/.ssh
$ sftp root@priems
sftp> cd /opt/orahome/.ssh
sftp> get id_rsa*
sftp> quit
$ ls -l /opt/orahome/.ssh/id_rsa*
-rw-----1 oracleorainst1675 Mar 10 15:42 id_rsa
-rw-r--r--1 oracleorainst397 Mar 10 15:42 id_rsa.pub
Now both primary and secondary EMSs have the same "id_rsa" and "id_rsa.pub" files in
/opt/orahome/.ssh directory.
```

Step 4 Create an oracle user and **/opt/backup** directory on the remote SFTP server.

- a. Login to remote SFTP server as root.
- b. Create a user "oracle" with group "orainst" and home directory "/opt/orahome".
- c. Create a repository directory "/opt/backup".

```
# mkdir -p /opt/orahome
# groupadd orainst
# useradd -g orainst -d /opt/orahome -s /bin/ksh oracle
# chown oracle:orainst /opt/orahome
# passwd oracle
New Password: <Enter password>
Re-enter new Password: <Re-enter password>
# mkdir -p /opt/backup
# chown oracle:orainst /opt/backup
# su - oracle
$ mkdir -p /opt/orahome/.ssh
$ chmod 700 /opt/orahome/.ssh
$ chown oracle:orainst /opt/orahome/.ssh
```

Step 5 Sftp the "id_rsa" and "id_rsa.pub" files generated in Step 1 to remote SFTP server /opt/orahome/.ssh directory. Make the file owned by "oracle:orainst" owner and group.

Login to remote SFTP server:

```
# su - oracle
$ cd .ssh
$ sftp root@priems
sftp> cd /opt/orahome/.ssh
sftp> get id_rsa*
sftp> quit
$ cat id_rsa.pub >> authorized_keys
$ chmod 600 id_rsa* authorized_keys
$ ls -l
-rw-----1 oraoragrp788 Mar 10 16:52 authorized_keys
-rw-----1 oraoragrp1675 Mar 10 16:48 id_rsa
```

```
-rw-----1 oraoragrp394 Mar 10 16:48 id_rsa.pub
```

Step 6 Sftp the "id_rsa" and "id_rsa.pub" files generated in Step 1 to remote SFTP server /opt/orahome/.ssh directory. Make the file owned by "oracle:orainst" owner and group.

Step 7 Test SSH and SFTP from both the primary and secondary EMSs to the remote SFTP server:

a. From BTS primary EMS:

```
# su - oracle
$ sftp_ping oracle SFTPserverName
Connecting to SFTPserverName...
sftp> quit
SFTP_PING=OK
```

**Note**

At the first login, the following message may display: "Warning: Permanently added the RSA host key for IP address '10.xx.xxx.xxx' to the list of known hosts."

Step 8 To schedule the ora_sftp_backup.ksh process to execute at 5:30am every day in oracle crontab on both the primary and secondary EMS:

a. Log in as oracle, or su - oracle and enter the following:

```
crontab -e
```

b. Add the following line to the Oracle crontab on the primary EMS:

```
#
# SFTP backup files from primary (optical1) to /opt/backup directory of SFTPserver.
#
0 6 * * * /opt/oracle/admin/scripts/ora_sftp_backup.ksh optical1 oracle SFTPserver
/opt/backup > /opt/oracle/tmp/ora_sftp_backup.log 2>&1
```

**Note**

Enter 0 6 *** /opt/oracle/admin/scripts/ora_sftp_backup.ksh...ora_sftp_backup.log 2>&1 in the same line.

Step 9 Replace SFTPserver with the correct host name of the remote SFTP server.

Step 10 Replace /opt/backup with the correct target directory name, if different.

Step 11 Edit the oracle crontab on secondary EMS site by replacing optical1 with optical2.

Archiving Your Database

Step 1 Log in as root.

Step 2 Stop all platforms. If this is a primary node, use the CLI command to control the standby forced active.

Step 3 Verify that /var/yp exists. Enter `ls -l /var/yp`.

If the result is no such file or directory, enter `mkdir -p /var/yp`

Step 4 Mount the NFS server. Enter `mount <nfserver hostname/ip>:<share directory> /mnt`. Example:

```
mount 10.89.183.253:/opt/archive /mnt
```

Step 5 Back up all interfaces. Enter `tar -cvf /mnt/<local_hostname>.tar host*`. Example:

```
<hostname>#tar -cvf bts-prica.tar host.*
```

Step 6 Restore the Solaris “**date**” command to create the system Flash Archive. Enter:

```
mv /bin/date /bin/date.orig
mv /bin/.date /bin/date
```

Step 7 Create the archive. Enter `<hostname>#flarcreate -n <archive name> -x /opt -S -c /mnt/<file name>`



Note Example archive name: `flarcreate -n CCPU-EMS -x /opt -S -c /mnt/secems04.archive`

Step 8 Back up the /opt directory. Enter `tar -cvf - /opt/* |gzip -c >/opt/<hostname_release>.tar.gz`

Step 9 Restore the original configuration. Enter:

```
mv /bin/date /bin/.date
mv /bin/date.orig /bin/date
```

Step 10 Unmount the NFS server. Enter `umount /mnt`

Examining Heap Usage

Heap is memory BTS reserves for data it creates as its applications execute. BTS audits heap usage of all the processes started by a platform, CA, AIN, POTS, EMS and BDMS. Heap auditing is added to the ADP process.

When heap usage of a process goes beyond certain threshold level, BTS generates an alarm. The alarm clears when heap usage goes below the threshold level.

Heap audit does the following:

- Monitors traces of heap usage in the last four periods for each process
- Measures heap usage of each process started by the platform once a day at 4 a.m
- Issues a minor alarm if the heap usage of a process exceeds 70% of its max heap size limit
- Clears a minor alarm if the heap usage of a process drops below 68% of its max heap size limit
- Issues a major alarm if the heap usage of a process exceeds 80% its max heap size limit
- Clears a major alarm if the heap usage of a process drops below 78% its max heap size limit
- Issues a critical alarm if the heap usage of a process exceeds 90% its max heap size limit
- Clears a critical alarm if the heap usage of a process drops below 88% its max heap size limit
- Reports, via trace logs, the last twenty heap measurements, including the time and the value for each process
- Clears heap usage alarms when process restarts

Checking the DNS Server

To check the DNS server, do this for all nodes.

-
- Step 1** Log in as **root** on the active CA.
- Step 2** Enter more `/etc/resolv.conf`.
- Note `nameserver <ip address>`
- Step 3** Enter `nslookup`
- This defaults to the first DNS server.
- Step 4** Enter a valid gateway name and press **Enter**.
- An IP address associated to gateway appears.
- Step 5** Enter `server <second dns server ip>`
- Step 6** Enter a valid gateway name and press **Enter**.
- An IP address associated to gateway appears.
- Step 7** Enter `exit` to quit.
-

Log Archive Facility (LAF)

The LAF process in Cisco BTS 10200 transports the trace log files to a remote archive server for storage. LAF is a continuously running daemon process on all nodes (components) of the BTS 10200. It wakes up every minute when active and checks if there are any new log files.

The service provider can specify the external archive system, the target directory, host directory, and the disk quota for each trace log directory in the system. If any new log files are in these trace log directories, LAF transfers them by Secure FTP (SFTP) to an external archive server specified by the service provider.

Secure Transfer of Files

BTS 10200 uses Secure FTP to transfer trace log files to the external server. LAF opens an SFTP connection when its ready to transfer log file to the remote server. This connection is not closed even after the transfer is complete. If for some reason the connection closes, the LAF process re-establishes the connection during the next transfer. The connection is persistent till the LAF feature is disabled.

LAF operates on a single SFTP connection and transfer of files occurs one file at a time (using the SFTP put operation). The same connection is used to transfer multiple files. When the LAF process detects a bad connection, it terminates the SFTP session by closing the socket used to talk to the archive server.

The LAF process maintains a linked list for the files that need to be transferred. If the connection is lost during a transfer, the LAF process moves the unsuccessfully transferred file to the end of the list and raises Maintenance Alarm 108.

A re-attempt on a failed file depends on the number of files in the list and the time taken to transfer those files. When there is no file to be transferred (i.e. the list is empty), then there is a gap of 30 seconds before processing the list again.

The LAF process increments a counter, which is specifically used for the number of times the transfer was attempted for this file. If a counter is more than three, the log file is deleted from the list. That is, upon three failed attempts on the same file, the file entry is deleted from the list.

Other Capabilities

This section lists the additional capabilities of the LAF process.

- It performs disk space management when 90% of the disk space quota specified for the target directory is reached.
- It gracefully recovers from any abnormal conditions and re-initiates the process to continue the transfer of files.
- It generates alarms when any unsuccessful scenarios are encountered. These alarms are listed in the *Cisco BTS 10200 Troubleshooting Guide*.

Provisioning LAF



Caution

The values provided by the user for the following parameters will be written into `/etc/opticall.cfg` file and transported to all the four BTS 10200 nodes.

The following parameters are associated with the LAF process. If they are left blank, the LAF process for a particular platform (such as, CA, FSPTC, FSAIN) is turned off.

To use this feature, you must provision the following parameters with the external archive system, the target directory, and the disk quota (in GB) for each platform.

CA_{xxx}_LAF_PARAMETER

FSPTC_{xxx}_LAF_PARAMETER

FSAIN_{xxx}_LAF_PARAMETER

Note that *xxx* must be replaced with each platform's instance number.

Example 1

```
CA146_LAF_PARAMETER="yensid /CA146_trace_log 20"
```

Example 2

```
FSPTC235_LAF_PARAMETER="yensid /FSPTC235_trace_log 20"
```

Example 3

```
FSAIN205_LAF_PARAMETER="yensid /FSAIN205_trace_log 20"
```

To enable Log Archive Facility (LAF) process, refer to [Enabling LAF Process](#) section.

Enabling LAF Process

To enable the Log Archive Facility (LAF) feature, you must set up the authorization for non-interactive SSH login to the external archive server for the Cisco BTS 10200 system to access and turn the LAF processes to active state. (Immediately after the fresh installation and platform start, the LAF process is in a dormant state).

The steps to set up the authorization in external archive server and turn the LAF processes to active is listed below:

Setup Non-Interactive SSH Login to External Archive Server



Note

The external archive system is recommended to be located such that it can be accessed by the management network. In such a case, the static routes in the CA system should be explicitly set so that the traffic to the external archive system is routed through the management network see section (“Adding Static Routes” section for more details). Otherwise, the traffic is routed through the default network (i.e. signaling network) and may not be able to reach the external archive system.

-
- Step 1** Log in to the Cisco BTS 10200 primary EMS as **root**.
 - Step 2** From the EMS, login to the external archive server via ssh to get the external archive server added to the */.ssh/known_hosts* file.
 - Step 3** Log off from the external archive server.
 - Step 4** While still logged in on the primary EMS as **root**, generate an SSH key.
 - a. Execute **cd /opt/BTSossh/bin**.
 - b. Execute **ssh-keygen -t rsa**.
 - c. Press Enter to accept the default file name for the key (*/.ssh/id_rsa*).
 - d. Enter **y** if prompted to choose whether to overwrite the existing file.
 - e. Press Enter when prompted to enter a passphrase (i.e. no passphrase).
 - f. Transfer the resulting file (*/.ssh/id_rsa.pub*) to a temporary location on the external archive server.
 - Step 5** Set up the external archive server with the key generated in Step 4.
 - a. Login to the external archive system as **root**.
 - b. If a */.ssh/authorized_keys* file does not exist on the external archive system, rename the **id_rsa.pub** file (copied from the Cisco BTS 10200 EMS) to */.ssh/authorized_keys*. If the file does exist, append the **id_rsa.pub** file to it.
 - Step 6** On the primary EMS, execute


```
ssh root@abcd
```

 where *abcd* is the IP address or fully-qualified domain name of the external archive server.
 - Step 7** Verify that login to the external archive server is successful and that no prompts for username or password are issued.
 - Step 8** Run **enableLAF** in EMS platform directories (i.e. */opt/ems/bin* and */opt/bdms/bin*)
 - Step 9** Repeat Steps 1-8 for the secondary EMS, primary CA and secondary CA. (In CA, the platform directories are */opt/OptiCall/CAxxx/bin*, */opt/OptiCall/FSPTCyyy/bin*, */opt/OptiCall/FSAINzzz/bin*).




Note

Billing has a similar mechanism/steps to SFTP their Call Detail Blocks (CDB) files to an external machine. If the LAF and Billing use the same target machine, then in both EMS, perform Steps 1-7 only once. You must still run Step 8 to enable LAF. And you must still run Steps 1 -9 in CA nodes.

Adding Static Routes

To add static routes to all Cisco BTS 10200 systems, perform the following steps:

-
- Step 1** From the shell or window of the primary call agent, change directory to */opt/utlils*.
- ```
cd /opt/utlils
```
- Step 2** Edit **S96StaticRoutes** using an editor.
- Step 3** Add the subnet of NTP server, DNS server, external archive server and any other machine to the file, which user wants to have access to Cisco BTS 10200 system in the following format:
- ```
route add -net <destination network> <network gateway>
```
-  **Note** All NTP, DNS traffic, traffic to external archive server, and traffic from other machine to Cisco BTS 10200 system (eg. login), should all go through management networks. (i.e. network gateway in management network). This is particularly important in CA system because CA has both management and signaling network. If user does not specify explicitly in this file, those traffic will be directed to signaling network, because signaling network is the default one in CA/FS.
-
- Step 4** Make sure there is a soft link pointing from */etc/rc3.d/S96StaticRoutes* to */opt/utlils/S96StaticRoutes*.
- ```
ls -l /etc/rc3.d/S96StaticRoutes
```
- Step 5** After editing, close the file, and run **S96StaticRoutes**.
- ```
/etc/rc3.d/S96StaticRoutes
```
- Step 6** Repeat Step 1 to Step 5 on the secondary CA.
- Step 7** Verify the connectivity by pinging the DNS server, NTP server, external archive server, or any machine that user just added in that file.
-

LAF Alarm Information

Refer to the following link to see the LAF alarm information.

Document Name	Link to the Document
Cisco BTS 10200 Troubleshooting Guide	http://www.cisco.com/en/US/docs/voice_ip_comm/bts/6.0.3/troubleshooting/guide/07tg01.html#wp1938289

Moving Core Files

BTS creates and stores core files in the bin directory for the binary executable that generated the core. Core files are large (2–4 GB) and eventually cause a disk full condition resulting in a switchover. When a BTS platform system generates a core file, the BTS creates an alarm. The Core File Present—Audit 25 (major) alarm indicates a core is present in the BTS. The primary cause of this alarm is that a network element process crashed.

The BTS automatically removes these core files when disk space is critically low or the core file has aged beyond a maximum allowable time. However, to ensure proper BTS performance move these core files off the BTS to another storage area as soon as they are generated. Refer to the Directory Containing Core Files dataword for the location of the core file.

Use the settings in the `cfm.cfg` file to configure how to monitor and manage core files.

Table 3-7 Core File Monitor Configuration File Parameters and Conditions

Parameter	Condition
CORE_FILE_MONITOR_DISABLE	If set to true, the core file monitor audit is not performed. Default setting is false.
CORE_FILE_ALARM_ENABLE	If set to false, the core file monitor alarm is not issued when a core file is found in the network element bin directory. Default setting is true.
CORE_FILE_MINIMUM_SPACE	This is the minimum free file space in megabytes which will trigger the automatic deletion of the oldest core files. Default is 5 GB.
CORE_FILE_AGE_TO_DELETE	This is the maximum time in hours that a core file can exist before it is automatically deleted. Default is 72 hours.
CORE_FILE_AGE_DELETE_ENABLE	If set to true, core files are deleted automatically when their maximum age is reached. Default is true.
CORE_FILE_SPACE_DELETE_ENABLE	If set to to true, the oldest core files are deleted when free file space is low. Default is true.



CHAPTER 4

Operating the BTS

Revised: August 10, 2011, OL-25015-01

Introduction

This chapter tells you how to operate the BTS. This chapter assumes the following are true:

- Connecting components have been correctly installed.
- Connecting components have been successfully started.
- You are a system administrator with past BTS experience.

Managing Subscribers

Table 4-1 Managing Subscribers

Task	Sample Command
Activating added subscribers	<pre>control subscriber-termination id=<subscriber id>; target-state=INS; mode=FORCED;</pre> <p>Ensure you specify <code>mode=FORCED;</code> when assigning a DN to a ported-out subscriber.</p>
Deactivating subscribers	<p>Force the subscriber OOS:</p> <pre>control subscriber-termination target-state=oos; mode=forced; id=<subscriber id>;</pre> <p>Force the subscriber's MTA OOS:</p> <pre>control mgw id=<mgw-id>; target-state=oos; mode=forced;</pre> <p>Disassociate the subscriber from VoIP service:</p> <pre>delete subscriber-service-profile sub-id=<subscriber id>; service-id=1;</pre> <p>Remove the subscriber from the BTS database:</p> <pre>delete subscriber id=<subscriber-id>;</pre> <p>Remove VoIP service from the subscriber's MTA:</p> <pre>delete termination prefix=aaln/; port-start=1; port-end=2; mgw_id=<mgw-id>;</pre> <p>Remove the subscriber's MTA from the BTS:</p> <pre>delete mgw id=<mgw-id>;</pre>
Bypassing LNP queries for ported-in numbers	<p>After activating a ported-in number, update the BTS so calls to this number from MTAs on the BTS directly route to the MTA associated with the ported-in number:</p> <pre>change dn2subscriber office-code-index= <office-code-index of ported TN's NPA-NXX>; dn=<XXXX of the ported TN>; lnp-trigger=N;</pre>
Ensuring LNP queries for ported-out numbers	<p>Update the BTS so calls to this number perform an LNP query:</p> <pre>change dn2subscriber office-code-index= <office-code-index of ported TN's NPA-NXX>; dn=<XXXX of the ported TN>; lnp-trigger=y;</pre>
Assigning a DN ported-out status	<p>Note Wait for the CLEC to confirm the transfer before changing the DN status on the BTS. Initially, calls to the DN may have to route to the porting-out subscriber's MTA using LNP.</p> <p>Ensure you specify <code>mode=FORCED;</code> when assigning a DN to a ported out subscriber.</p> <pre>change dn2subscriber office-code-index= <office-code-index of porting TN's NPA-NXX>; dn=<XXXX of the porting TN>; status=ported-out; sub-id=null;</pre>
Disconnecting service to ported subscribers	<ol style="list-style-type: none"> 1. Assign time and date to disconnect service. 2. Send service disconnection notice to NPAC SMS. 3. NPAC SMS broadcasts this to all service providers. 4. NPAC SMS removes the ported number from its database. 5. All service providers remove the number from their LNP databases. 6. Calls to the number route as if it was non-porting.

Table 4-1 Managing Subscribers (continued)

Task	Sample Command
Viewing subscribers voice mail indicator (VMI) status	<pre>status subscriber ID=278-222-1917</pre> <p>Note For MGCP subscribers only.</p>
Resetting subscribers voice mail waiting indicator (VMWI)	<pre>control subscriber ID=278-222-1917; mwi=on</pre> <p>or</p> <pre>control subscriber ID=278-222-1917; mwi=off</pre>
Reporting all subscribers that use “best effort” (non DQoS) calls in the network having or not having a specific aggr id	<pre>report subscriber id=%; oper-status=qos-best-effort; aggr-id=aggr1; start_row=1; limit=5;</pre> <p>Displays the output as CLI as the output-type has not been mentioned</p> <p>or</p> <pre>report subscriber id=215-222-0502; oper-status=qos-best-effort; aggr-id=%; output-type=xml; start_row=1; limit=5; output=report;</pre> <p>Displays the output in the specific format (CSV/XML) based on the output-type specified</p> <p>Note The output displays only NCS subscribers.</p>
Changing subscribers ring and call waiting tone	<pre>change dn2subscriber DN=4692553010; RING_TYPE=4; CWT_TYPE=4;</pre> <p>Note The CWT_TYPE has no effect on SIP subscribers. Their IP phones control how they receive call waiting tones.</p>
Deleting subscribers secondary DNs	<p>Delete one secondary DN for a subscriber:</p> <pre>delete dn2subscriber FDN=4692553010;</pre> <p>Delete all secondary DNs for a subscriber:</p> <pre>delete dn2subscriber SUB_ID=SUBSCRIBER_1; VIRTUAL_DN=Y;</pre>

Table 4-1 *Managing Subscribers (continued)*

Task	Sample Command
Changing subscribers announcements	Delete the changed-number entry. <code>delete changed-number old-DN=<old-DN>;</code> Change the status of the old DN to DISC in the dn2subscriber table. <code>change dn2subscriber DN=<old-DN>; status=DISC;</code>

Table 4-1 Managing Subscribers (continued)

Task	Sample Command
Changing subscribers DNs	<p>Change the subscriber DN to the new DN.</p> <pre>change sub id=<id>; dn1=<new-DN>; CN-REFERRAL=Y;</pre> <p>Example:</p> <pre>change sub id=sub1; dn1=206-222-1841; CN-REFERRAL=Y;</pre> <p>The CN-REFERRAL token adds an entry in the changed-number table for the changed subscriber DN. By default, the CN-REFERRAL token is set to Y. If the CN-REFERRAL token is set to N, the changed-number table is not updated with the changed number information.</p> <p>Use the show subscriber command to verify the new DN.</p> <pre>show sub id=<id></pre> <p>Example:</p> <pre>show sub id=sub1; Dn1 indicates 206-222-1841</pre> <p>Verify that the changed number (old DN) of the subscriber is being tracked in the changed-number table.</p> <pre>show changed-number old-dn=<old-dn></pre> <p>Example:</p> <pre>show changed-number OLD-DN=206-222-2345</pre> <p>Use the dn2subscriber table to verify that the old DN is in CN state and new DN is in assigned state. Check if the status of the old DN is CN.</p> <pre>show dn2subscriber FDN=<old-DN>;</pre> <p>Example:</p> <pre>show dn2subscriber FDN=206-222-2345;</pre> <p>Check if the status of the new DN is assigned.</p> <pre>show dn2subscriber FDN=<new-DN>;</pre> <p>Example:</p> <pre>show dn2subscriber FDN=206-222-1841;</pre> <p>Place an incoming call to the new DN and verify the call is setup successfully.</p> <p>Place an incoming call to the old DN and verify that the announcement played is "<old DN> has been changed to <new DN>."</p> <p>If an announcement is not played, do the following:</p> <p>Verify if the release cause id maps to annc-id=118.</p> <pre>show release-cause id=22;</pre> <p>Verify if the announcement id maps to announcement-number 301.</p> <pre>show annc id=118;</pre> <p>Note If there is no referral number (that is, when CN-REFERRAL is set to N where the new number is private), the BTS 10200 plays a generic announcement indicating that the number has changed. No further information is provided on the new number.</p>

Viewing Calls

These tasks allow you to view information related to call forwarding features.

If A calls B and the call is forwarded to C:

- Querying A shows A is connected to C and provide C's information.
- Querying C shows C is connected to A and provide A's information.
- Querying B shows A is calling C and the call is forwarded through B.
- Even when the call is forwarded through B, B can originate another call. B can also forward multiple calls.

When viewing Three-Way Call and Call Waiting calls remember the output shows both calls.

Table 4-2 Viewing Calls


Task	Sample Command
Viewing active calls	<code>query call-trace subscriberDN/FQDN/NPA-NXX-****/aaln/*@*</code>
Viewing call trace summaries, started when subscriber presses *57	<code>report call-trace-summary</code> Note The report appears on the screen and it does not generate in HTML.

Using Status and Control Commands

Table 4-3 *Using Status and Control Commands*

Task	Sample Command
Viewing BTS system status	<code>status system;</code>
Viewing component states	<p data-bbox="638 495 1047 525"><code>status element-manager id=EM01;</code></p> <p data-bbox="638 535 808 564">Possible states:</p> <ul data-bbox="651 579 1503 1472" style="list-style-type: none"> <li data-bbox="651 579 1503 646">• STARTUP—During platform startup, the two sides are communicating to determine which side will come up active. <ul data-bbox="699 657 1503 800" style="list-style-type: none"> <li data-bbox="699 657 1503 724">– INIT-NORMAL—primary will be active, secondary will be standby; switchover allowed. <li data-bbox="699 735 1503 800">– INIT-FORCED—primary will be forced to active or standby, secondary will be forced to standby or active; no switchover allowed. <li data-bbox="651 810 1503 877">• ACTIVE-NORMAL—primary is active, secondary is standby; switchover allowed. <li data-bbox="651 888 1503 955">• ACTIVE-FORCED—primary or secondary has been forced to active; no switchover allowed. <li data-bbox="651 966 1503 1033">• STANDBY-NORMAL—primary should be active, secondary should be standby; switchover allowed. <li data-bbox="651 1043 1503 1110">• STANDBY-FORCED—primary or secondary has been forced to standby; no switchover allowed. <li data-bbox="651 1121 1503 1188">• TRANSITION-TO-ACTIVE-NORMAL—primary is going to active, secondary is going to standby; switchover allowed. <li data-bbox="651 1199 1503 1291">• TRANSITION-TO-ACTIVE-FORCED—primary has been forced to active or standby; secondary has been forced to standby or active; no switchover allowed. <li data-bbox="651 1302 1503 1369">• TRANSITION-TO-STANDBY-NORMAL—primary is going to standby, secondary is going to standby; switchover allowed. <li data-bbox="651 1379 1503 1472">• TRANSITION-TO-STANDBY-FORCED—primary has been forced to active or standby; secondary has been forced to standby or active; no switchover allowed. <p data-bbox="638 1482 1357 1522">Tip Use <code>status application</code> for more detailed information.</p>

Table 4-3 Using Status and Control Commands (continued)

Task	Sample Command
Changing states of component pairs (EMS, BDMS, CA, and FS)	<pre>control call-agent id=CA146; target-state=FORCED-STANDBY-ACTIVE;</pre> <p>Possible states:</p> <ul style="list-style-type: none"> • ACTIVE_STANDBY • STANDBY_ACTIVE • NORMAL—Primary is active and secondary is standby. • FORCED-ACTIVE-STANDBY—Primary has been forced to active and secondary is standby. • FORCED-STANDBY-ACTIVE—Primary has been forced to standby and secondary is active.
Viewing component application states	<pre>status application id=CA146;</pre>
Changing component applications states (in-service or OOS)	<pre>control application id=CA146; action=star;node=prica06</pre> <p> Caution This negatively impacts the performance of the BTS host.</p>
Activating media gateways	<p>Ensure the MG exists, then enter:</p> <pre>control mgw id=<mgw-id>; target-state=ins; mode=forced;</pre> <p>where</p> <ul style="list-style-type: none"> • mgw id—the voice port on the subscriber's MTA (the voice port's MAC address without hyphens) • target-state—ins to show in service for all activations • mode—forced for all activations
Setting subsystem groups/OPC in or OOS	<pre>control subsystem_grp id=CNAM; mode=forced; target_state=UOS;</pre> <p>This sets the state of the individual subsystems within the subsystem group as well. If a subsystem/OPC combination is taken OOS individually, the state of the subsystem group may be in service while some members of the group are out of service.</p>
Viewing subsystem groups/OPC status	<pre>status subsystem_grp id=CNAM</pre>

Using Show and Change Commands

Table 4-4 Using Show and Change Commands

Task	Sample Command
Viewing subscriber-related batch data: subscribers, terminations, subscriber service profiles	<pre>show subscriber limit=1000; start_row=<next page value>;display=id,sub_service_profile; order=id;</pre> <p>Where</p> <ul style="list-style-type: none"> • limit—Page size for the maximum number of rows (or lines) to display • start_row—Which page to display first • display=id—Sorts data by id column • order=id—Provides a key for ordering or sorting the data
Viewing database usage statistics	<pre>show db-usage table-name=dial_plan;</pre> <p>Note Do not use hyphens in table names; instead use underscores.</p> <p>or</p> <ol style="list-style-type: none"> 1. Go to http://www.cisco.com/en/US/docs/voice_ip_comm/bts/6.0.3/command/CLI/CLI_Database.zip 2. From the first drop-list, select "Table Sizing Configuration".
Changing database usage statistics	<pre>change db-usage table-name=dial-plan; minor-threshold=70;major-threshold=80; critical-threshold=95;</pre>

Using ERAC Commands

Using prepared SQL statements Extended Read Access Commands (ERAC) commands perform a complex read against the BTS database. This SQL optimization and multitable and nested SELECT(s) quickly return data that would otherwise take several database dips and a lot of back end data post processing. Use the following interfaces to access ERAC:

- CLI and MAINT shells
- CORBA/XML adapters
- EPOM (uses CORBA/XML)
- SPA

Directory number (DN) and telephone number (TN) refer to the same BTS entity but with different sources:

- TN—EC database value + the Office Code table's NDC field
- DN—DN2 Subscriber table's DN field

The TN/DN is a concatenation of 14 (or less) digits. Commands fail if a partial TN is supplied.



Note

Commands allow for wild card support. When you enter a subscriber, subscriber account code, or DN, the value can have the wild card percent (%) search criteria.

These are standard commands and their parameters. Several are associated with BTS tables. However, several parameters are derived from multiple sources and do not map directly to a table. They may have real database representation but be modified for ease of use or readability.

Tasks	Descriptions	Examples
Viewing account IDs	An account id can be assigned to one or more subscribers. An account id is used only for identification purposes. The account id is not associated with feature grouping behavior during call processing. The account id is included in billing record. This is for operational identification purpose only. This is an optional field of 1-20 text characters.	<code>account-id=ABC123456789;</code>
Viewing DNs	The DN is the telephone number. This number is a derived value composed of the office-code.ndc, office-code.ec and the dn2subscriber.dn fields. It is a concatenation to provide a consistent view of the primary directory number for a subscriber. It is 1-14 numbers.	<code>show 4692550529</code>
Viewing DNs by subscriber	This command returns a list of all DNs associated with a specified subscriber or account id. In this command, the subscriber id field or the new account-id field determines the DN(s) to list. Each row of data represents a DN entry. The additional data is supplied to provide further information about the DN.	<code>show sub-dn-list sub-id=foo_123; account-id=ABC123456789;</code>
Viewing line features by DN	This command returns a list of all features associated with a specified DN. In this command the DN is supplied to qualify the data search. The data returned is not in the form of services and service packages. This query dips into the service packages and finds the actual features associated with each service assigned to the DN and its subscriber.	<code>show dn-line-feat dn=4692550529; sub-id=foo_123; account-id=-ABC123456789;</code>
Viewing feature summaries by DN	This command returns the list of all features associated with a specified entity. In this command the DN, Subscriber ID or Account ID is supplied to qualify the data search. The command returns the list of all the services of the associated subscriber or DN and all features associated with each specific service package. This also includes the service profiles association.	<code>show dn-feat-list dn=4692550529; sub-id=foo_123; account-id=ABC123456789;</code>

Tasks	Descriptions	Examples
Viewing speed dial settings by DN	This command returns a list of all speed dial telephone numbers by the specified DN or primary subscriber directory number. All one digit speed dial values are returned as well as the feature state of speed dial. Only a single row is returned with the complete list of speed dial numbers. If a number is not defined, it is left blank.	<pre>show dn-sd-list dn=4692550529; sub-id=foo_123; account-id=ABC123456789;</pre>
Viewing domestic long distance blocking by subscriber or account id	This command returns the cos-restrict information for a specified subscriber. In this command the subscriber ID field or the new account-id field determines the subscriber. This command keys on the use of the Nature of Dial (NOD) means for restricting subscriber activity.	<pre>show sub-id-block sub-id=foo_123; account-id=ABC123456789;</pre>
Viewing international long distance blocking settings by subscriber or account id	This command returns the COS_RESTRICT information for all DN(s) associated with a specified subscriber or account. In this command the subscriber ID field or the new ACCOUNT_ID field determines the subscriber. This command keys on the use of the NOD as the means for restricting subscriber activity.	<pre>show sub-intl-block sub-id=foo-123; account-id=ABC123456789;</pre>
Viewing DA blocking by subscriber or account id	This command returns the cos-restrict information a specified subscriber or account. In this command the subscriber id field or the new account_id field determines the subscriber. This command keys on the use of the NOD as the means for restricting subscriber activity.	<pre>show sub-da-block sub-id=foo-123; account-id=ABC123456789;</pre>
Viewing OA blocking by subscriber or account id	This command returns the Operator assistance blocking information for a specified subscriber or account. In this command the subscriber ID field or the new ACCOUNT_ID field determines the subscriber. One row of data exists for each actual BTS 10200 subscribers.	<pre>show sub-oper-block sub-id=foo-123; account-id=ABC123456789;</pre>
Viewing call hunt groups by subscriber or account id	This command returns the list of one or more hunt groups associated with a specified subscriber. In this command the subscriber Id field or the new account_id field determines the subscriber. Each row of data represents a hunt group membership.	<pre>show hg-dn-listdn=4692550529; sub-id=foo-123; account-id=ABC123456789;</pre>
Viewing sequence by hunt group	This command returns the hunt sequence as a list of telephone numbers (TNs) associated with a specified Hunt Group. Each row of data equates to a relative terminal in the hunt group. This avoids static lists with a fixed number of terminals.	<pre>show hg-sequence mlhg-id=foo-123; account-id=ABC123456789;</pre>

Tasks	Descriptions	Examples
Viewing list DNs that not in a hunt group	This command returns a list of all DNs associated with a specified subscriber and that are not associated with a hunt group. Under the present definition, the list can be long. Each row of the data indicates a TN with a free association. It is strongly recommended that some qualifications are provided to narrow the scope of the command. For example, list all free DNs in a particular account where the account ID is some specific value.	<pre>show sub-dn-find account-id=ABC1234%; sub-id=foo-123;</pre>
Viewing Outbound Caller ID with Name Value by DN	This command returns the caller ID and NAME for a specified TN. Each row of data represents a separate subscriber TN. The read is based on the actual TN of a subscriber.	<pre>show sub-cid sub-id=foo-123; account-id=ABC123456789;</pre>

Managing Transactions

The Transaction Queue tracks updates to EMS database, and the shared memory of the CAs and FSs. Entries should remain in the transaction queue for a few seconds, unless an EMS, CA, or FS in an error state. In case of an error state, the transaction queue to stores entries for later updates.

Table 4-5 Viewing and Deleting Transactions


Task	Sample Command
Viewing transaction queue entries	<pre>show transaction-queue target=CA146; status=pending;</pre> <p>Following is an example of the system response to this command.</p> <pre>TRANSACTION_ID=901208641475967405 USER_ID=optiuser TERMINAL_ID=USR1 SEQUENCE_NUM=0 TARGET=CA146 STATEMENT=INSERT INTO CARRIER (ID) VALUES ("3434") TIMESTAMP=2006-11-10 11:36:41 ACTIVE_TARGET=Y STATUS=PENDING</pre>
Deleting transaction queue entries	<pre>delete transaction-queue target=CA146</pre> <p> Caution This command causes a database inconsistency. Call TAC before using it.</p>
Viewing maximum download capacity for transaction queuing	<pre>show queue-throttle</pre>

Table 4-5 Viewing and Deleting Transactions (continued)

Task	Sample Command
Enabling/Disabling queue throttling	<ol style="list-style-type: none"> Go to the <code>bts.properties</code> file. <pre>/opt/ems/etc/bts.properties</pre> <ol style="list-style-type: none"> To enable throttling, set <code>throttleEnable</code> to <code>Y</code>. To disable throttling, set <code>throttleEnable</code> to <code>N</code>. <pre>throttleEnable=Y</pre> <ol style="list-style-type: none"> Restart the platform.
Viewing number of commands executed from CLI, MNT, FTP, CORBA, SNMP, or SOAP interfaces	<pre>show config-interval;</pre>
Setting number of commands executed from CLI, MNT, FTP, CORBA, SNMP, or SOAP interfaces	<pre>change command-throttle-threshold session-type=CORBA; threshold=2000;</pre> <pre>change command-throttle-threshold session=CORBA; enable=N;</pre>

Scheduling Commands

The Hour and Minute Command Scheduling feature allows you to schedule command execution for a specific hour and minute.

Using start-time and recurrence command tokens, schedule command time and frequency (hourly, daily, weekly, monthly, etc.). You can remove the command at any time; if it is recurring and currently executing, it completes and is removed.

Limitations

To prevent overload and subsequent EMS degradation, limit commands to 10, each taking less than a minute.

If you schedule a command to execute, but an earlier occurrence of that command is still executing, the second might fail.

Table 4-6 Scheduling Commands

Task	Sample Command
Adding scheduled commands using minutes	<pre>add scheduled_command verb=report;noun=system_health;keys=period;key_values=720;recurrenc e=MINUTE;on_minute=3,10,25,59;start_time=2007-11-08 00:00:00;</pre>
Adding scheduled commands using hours	<pre>add scheduled_command verb=report; noun=system_health;start_time=2007-06-30 00:00:00; key_values=720;keys=period; recurrence=HOURLY;</pre>

Table 4-6 Scheduling Commands (continued)

Task	Sample Command
Viewing scheduled commands	<code>show scheduled_command recurrence=HOURLY;key_values=720;</code>
Changing scheduled commands	<code>change scheduled_command id=3871788758088233209;recurrence=MINUTE;on_minute=19;</code>



CHAPTER 5

Managing External Resources

Revised: August 10, 2011, OL-25015-01

Introduction

This chapter tells you how to manage external resources provisioned on the BTS using administrative (ADM) commands. External resources have two service states:

- Administrative—State the BTS user provisions for the resource link
- Operational—Physical condition of the resource link or the resource)

The two types of service states are independent of each other, for example:

A user places an MGW link in-service; its administrative state is ADMIN_INS. But that link between the BTS and MGW is lost. The MGW link's operational state is MGW_STATUS_DOWN. A query of the MGW returns both the administrative state and operational state.

Viewing BTS System-Wide Status

BTSSTAT runs on any BTS host. Any valid UNIX user can enter `btsstat` from a UNIX shell to initiate it. This command returns the following for all BTS components:

- Component id
- Side
- Host name
- Version
- Replication status
- Redundancy status

To run BTSSTAT from a non-BTS host, the configuration file needs the information in following table. BTSSTAT ignores all other lines in the file.

Table 5-1 Using *BTSSTAT*

Task	Sample Command
Viewing status of entire BTS system (including components not on the same host)	<code>btsstat</code>
Viewing status of specific components	CA <code>btsstat -caport</code> FSAIN <code>btsstat -fsainport</code> FSPTC <code>btsstat -fsptcport</code> EMS <code>btsstat -emsport</code> BDMS <code>btsstat -bdmsport</code>
Running <i>BTSSTAT</i> from a non-BTS host (requires an SSL connection to the BTS)	<code>btsstat -f my_cfg_file</code> Specify BTS hosts in a configuration file: <ul style="list-style-type: none"> • CA_SIDE_A_HN = prica11 CA_SIDE_B_HN = secca11 • FSAIN_SIDE_A_HN = prica11 FSAIN_SIDE_B_HN = secca11 • FSPTC_SIDE_A_HN = prica11 FSPTC_SIDE_B_HN = secca11 • EMS_SIDE_A_HN = priems11 EMS_SIDE_B_HN = secems11 • BDMS_SIDE_A_HN = priems11 BDMS_SIDE_B_HN = secems11
Viewing BTS software version and installed patches	<code>nodestat</code>

Managing Trunk Groups and Trunks

Table 5-2 Managing Trunk Groups

Task	Sample Command
Viewing TG status	<pre>status trunk-grp id=2;</pre> <p>Possible operational states:</p> <ul style="list-style-type: none"> • in-service • out of service • manually busy • operate in wait state, operate in standby state • restore session request normal, restore session request switchover, restore session request maintenance, restore session fail normal, restore session fail switchover, restore session fail maintenance, restore establish request normal, restore establish request switchover, restore establish request maintenance, restore establish fail normal, restore establish fail switchover, restore establish fail maintenance • in maintenance state • down session set fail soft normal, down session set fail hard normal, down session set fail soft maintenance, down session set fail hard maintenance, down establish request soft normal, down establish request hard normal, down establish request soft maintenance, down establish request hard maintenance, down establish request hard normal, down establish request soft maintenance, down establish request hard maintenance, down establish fail soft normal, down establish fail hard normal, down establish fail soft maintenance, down establish fail hard maintenance • delete graceful • request remove release, request remove session set • remove graceful in-service and maintenance state • DPC is inaccessible
Viewing TGs with ISDN D channels	<pre>show isdn-dchan</pre>
Switching ISDN D channels	<pre>control isdn-dchan tgn-id=1;</pre> <p>This switches the active D channel to standby, and the standby D channel to active.</p>
Changing TGs states	<pre>control trunk-grp tgn-id=129; mode=forced; target-state=oos;</pre> <p>Note Before bringing an ISDN trunk in-service, put the connected media gateway in-service, see Changing media gateways status.</p>
Viewing trunk status	<pre>status trunk-termination tgn-id=2; cic=8;</pre>

Table 5-2 Managing Trunk Groups (continued)

Task	Sample Command
Resetting trunks	<pre>reset trunk-termination tgn-id=13; cic=1-6;</pre> <p>Resetting does the following:</p> <ul style="list-style-type: none"> • Clears all manual and blocked states • Clears active/transient calls on a trunk termination, with the exception of SS7 trunk terminations. • Brings trunks INS
Changing trunk states	<pre>control trunk-termination tgn-id=17; cic=1-23; target-state=ins; mode=forced;</pre> <pre>equip trunk-termination tgn-id=13; cic=all;</pre> <p>Changes trunks in UEQP to OOS</p> <pre>unequip subscriber-termination id=97_8@ipclab.cisco.com;</pre> <p>Changes OOS trunks to UEQP</p>
Forcing MAINT state	<p>SS7 trunks</p> <pre>control ss7-trunk-termination tgn-id=103; mode=forced; target-state=maint;</pre> <p>Note Set COT on the terminating gateway or switch to perform these tests. Otherwise, the test or tests fail.</p> <p>ISDN trunks</p> <pre>control isdn-trunk-termination tgn-id=17; mode=forced; target-state=maint;</pre> <p>CAS trunks</p> <pre>control cas-trunk-termination tgn-id=64; mode=forced; target-state=maint;</pre> <p>Announcement trunks</p> <pre>control annc-trunk-termination tgn-id=13; mode=forced; target-state=maint;</pre>

Table 5-2 *Managing Trunk Groups (continued)*

Task	Sample Command
Viewing test menus	SS7 trunks <code>diag ss7-trunk-termination test=<TAB></code> <code>diag ss7-trunk-termination test=<RETURN></code> ISDN trunks <code>diag isdn-trunk-termination test=<TAB></code> <code>diag isdn-trunk-termination test=<RETURN></code> CAS trunks <code>diag cas-trunk-termination test=<TAB></code> <code>diag cas-trunk-termination test=<RETURN></code> Announcement trunks <code>diag annc-trunk-termination test=<TAB></code> <code>diag annc-trunk-termination test=<RETURN></code>

Table 5-2 Managing Trunk Groups (continued)

Task	Sample Command
Testing trunks (place in MAINT state first)	<p>SS7 trunks</p> <pre>diag ss7-trunk-termination tgn-id=103; cic=13; test=1;</pre> <p>Test 1: SS7 MGCP Connectivity Test—tests if MGCP has access to the SS7 trunk termination</p> <p>Test 2: SS7 Termination Connection Test—tests if there is a path to the device (ping).</p> <p>Test 3: SS7 COT Test—tests the integrity of the SS7 Bearer Path.</p> <p>Test 4: SS7 CQM Test—queries the SS7 circuit (or group of circuits) status. A range of CICs can be specified (to a maximum of 24). Both remote and local trunk states are displayed in the results.</p> <p>Test 5: SS7 CVT Test—tests to ensure that each end of the circuit has sufficient and consistent information for using the circuit in call connections. CLLI names are included.</p> <p>Test 6: SS7 CIC Audit—returns status of CICs</p> <p>Test 0: ALL—performs tests 1 through 6.</p> <p>ISDN trunks</p> <pre>diag isdn-trunk-termination test=1; tgn-id=17; cic=1;</pre> <ol style="list-style-type: none"> 1. Tests if MGCP has access to the ISDN termination 2. Tests if there is a path to the device (ping) 3. Performs tests 1 and 2 <p>CAS trunks</p> <pre>diag cas-trunk-termination tgn-id=64;cic=1;test=1;</pre> <ol style="list-style-type: none"> 1. Tests if MGCP has access to the CAS termination 2. Tests if there is a path to the device (ping) 3. Performs tests 1 and 2 <p>Announcement trunks</p> <pre>diag annc-trunk-termination;test=1;tgn-id=13;cic=1</pre> <ol style="list-style-type: none"> 1. Tests if MGCP has access to the ANC termination 2. Tests if there is a path to the device (ping) 3. Performs tests 1 and 2

Table 5-3 Valid Normal Trunk Termination States

State/Token	ADMIN-STATE	OPER-STATE	STATIC-STATE	DYNAMIC-STATE
UNEQP	UNEQP	ANY	UEQP	IDLE
MANUALLY OOS	OOS	ANY	LBLK	IDLE
MANUALLY MAIN	MAINT	IDLE	LBLK	IDLE

Table 5-3 Valid Normal Trunk Termination States (continued)

State/Token	ADMIN-STATE	OPER-STATE	STATIC-STATE	DYNAMIC-STATE
IDLE	INS	IDLE	ACTV	IDLE
ACTIVE INCOMING	INS	IDLE	ACTV	IDLE
ACTIVE OUTGOING	INS	ACTIVE	ACTV	OBSY
TRANSIENT INCOMING	INS	ACTIVE	ACTV	IBY-TRNS
TRANSIENT OUTGOING	INS	BUSY	ACTV	OBSY-TRNS

If a TG or trunk command fails, it can return one of the following generic failure reasons, as well as ones specific to the command.

Table 5-4 Understanding Trunk Group and Trunk Generic Command Responses

Command Entered	Command Response	Possible Conditions
<code>status</code> or <code>control</code>	Failure	<p>TG or trunk database was not found in shared memory.</p> <p>Component is already in the requested state.</p> <p>Graceful mode only. Appears when a command is executed and operation is INS going OSS or INS going MAINT.</p> <p>A required resource is not available.</p> <p>For ISDN</p> <ul style="list-style-type: none"> - A trunk cannot be added unless both the MGW and TG are available. - A TG cannot be added unless the MGW is available, and vice versa. <p>For SS7, CAS, Announcement</p> <ul style="list-style-type: none"> - A trunk cannot be added unless both the MGW and TG are available. - A TG does not require the MGW to be available, and vice versa. <p>An associated resource of the database cannot be found.</p> <p>An assigned resource is not valid (supported).</p>

Table 5-4 Understanding Trunk Group and Trunk Generic Command Responses (continued)

Command Entered	Command Response	Possible Conditions
any	Failure	<ul style="list-style-type: none"> • Found no failure • TG(s) cannot be found, trunk(s) cannot be found, no TG(s) found in trunking gateway, no trunk(s) found in TG • Fail while in termination table, fail while in TG table, fail while in trunk table, fail while looking to find trunk index, fail while getting TG administration state • Failed to allocate IPC message(s), failed to dispatch IPC message(s) • Operational state invalid, administration state invalid • Trunk(s) state change and pending • Found TG type invalid, found TG state invalid, found TG admin state not ready • Entity in desired state • Not allow trunk to reset • Change to out-of-service state required, change to request graceful mode error • Found entity unequipped in initial state • Operation not allowed because D Channel(s) is down • Found unknown failure reason(s)

Table 5-4 Understanding Trunk Group and Trunk Generic Command Responses (continued)

Command Entered	Command Response	Possible Conditions
Trunk Termination commands	Failure	<ul style="list-style-type: none"> • The transaction could not be executed due to a transient error, the endpoint is unknown, the endpoint is not ready, endpoint does not have enough resources available, a protocol error was detected, the command contained an unrecognized extension, the endpoint is restarting. • Invalid conn identifier, invalid call ID. • Unsupported mode or invalid mode, unsupported or unknown package. • Endpoint does not have a digit map, endpoint redirected to another Call Agent, endpoint malfunctioning, endpoint taken out of service. • No such event or signal. • Unknown action or illegal combination of actions. • Internal consistency in local connection options, unknown extensions in local connection options, unsupported values on local connection options. • Insufficient bandwidth. • Missing remote connection descriptor. • Incompatible protocol version. • Internal hardware failure. • CAS signaling protocol error. • Failure of a group of trunks. • Response too big. • Loss of lower connectivity. • No fault reason available.

Table 5-4 Understanding Trunk Group and Trunk Generic Command Responses (continued)

Command Entered	Command Response	Possible Conditions
Trunk commands	Failure	<ul style="list-style-type: none"> • NON-FAULTY—Not blocked, available for service. • MAINT-OOS—Trunk-termination is manually controlled OOS. • MAINT-BUSY—Trunk-termination is in maintenance state; controlled to MAINT. • TERM-FAULT—Bearer termination is in faulty condition. • SIGNALLING-FAULT—Signaling link (for example, SS7 link, or ISDN D channel) is faulty. • MAINT-BLOCK—Trunk-termination is manually controlled OOS (controlled mode=GRACE). • HARDWARE-BLOCK—Trunk-termination is manually controlled OOS (controlled mode=FORCED). • OUTGOING_RESTRICTED—The outgoing call is not allowed • DPC_INACCESSIBLE—The DPC is not accessible. • ACL_CONGESTION_LEVEL_1—Automatic Congestion Level (ACL) congestion is at level 1. • ACL_CONGESTION_LEVEL_2—ACL congestion is at level 2. • ACL_CONGESTION_LEVEL_3—ACL congestion is at level 2. • TFC_CONGESTION_LEVEL_1—Transfer Controlled (TFC) congestion is at level 1. • TFC_CONGESTION_LEVEL_2—TFC congestion is at level 2. • TFC_CONGESTION_LEVEL_3—TFC congestion is at level 3.

Table 5-4 Understanding Trunk Group and Trunk Generic Command Responses (continued)

Command Entered	Command Response	Possible Conditions
SS7 trunk commands	Failure	<ul style="list-style-type: none"> • ACT_LOC_INIT_RESET—Reset circuit at startup. • ACT_LOC_MML_RESET—Craft reset request. • ACT_LOC_QUERY—Circuit query. • ACT_LOC_UPU—Action to perform user part unavailable. • ACT_LOC_VALIDATE—Circuit validation. • ACT_LOC_COTTEST—COT test. • ACT_LOC_STOP—Action to stop the call. • BLK_LOC_UPU—Trunk is blocked because user part is unavailable. • DES_LOC_GRACE—Local hardware RSIP graceful. • DES_LOC_SIG—SS7 signaling fault (link fail). • DES_LOC_FORCE—Local hardware RSIP forced. • DES_LOC_MML—MML; also used for unsolicited blocks from MDL due to circuit query reservation (CQR). • DES_LOC_UPU—Trunk needs to be blocked because of user part unavailability. • JOB_PENDING—Ongoing job in progress. • JOB_REC—Job was received by the MDL component and is being processed. • OPER_ACTIVE—Trunk is available for calls. • REMOTE_GRACE—Trunk is blocked remotely because of a CLI command on the remote switch. • REMOTE_FORCE—Trunk is blocked remotely because of a hardware failure on the remote switch. • RESERVE_SPARE1—Reserved for future use. • RESERVE_SPARE2—Reserved for future use. • TERM_GRACE—Trunk is gracefully blocked because of an RSIP graceful from the MGW.

Managing Subscriber Terminations

Table 5-5 *Managing Subscriber Terminations*

Task	Sample Command
Checking subscriber status	<pre>status subscriber-termination id=ubr204_1;</pre> <p>Possible states:</p> <ul style="list-style-type: none"> • ADMIN-UEQP—Unequipped. <ul style="list-style-type: none"> – Newly-provisioned subscriber terminations are UEQP – Place a subscriber termination in UEQP before deleting it • ADMIN-INS—In-service • ADMIN-OOS—Out of service • ADMIN-MAINT—Maintenance Mode • ADMIN-OOS-PENDING—Transitioning to out of service • ADMIN-MAINT-PENDING—Transitioning to Maintenance Mode
Checking subscriber status in detail	<pre>status subscriber-termination id=@ubr235; oper-state=FA;ISDN Administrative and Operational Maintenance States for a Trunking Gateway</pre> <p>For more information use one of the following for oper-state:</p> <ul style="list-style-type: none"> • FA—Faulty • NF—Not faulty • IDLE—Termination idle • ACTIVE—Termination active • DOWN—Termination down • TERM-FA—Termination fault • TEMP-DOWN—Termination temporarily down • UNREACH—Termination unreachable • INT-MAINT—Termination internal maintenance • UEQP—Termination unequipped • ALL—All states, same as executing command without oper-state token

Table 5-5 *Managing Subscriber Terminations (continued)*

Task	Sample Command
Changing subscriber termination states	<pre>control subscriber-termination id=*c3810_167; mode=forced; target-state=INS;</pre> <p>Possible states:</p> <ul style="list-style-type: none"> • INS—In-service • OOS—Out of service • MNT—Maintenance mode <pre>control subscriber-termination id=sub2-ctx2; mode=forced; target-state=maint;</pre> <p>Forces MAINT state, do this before testing</p> <pre>equip subscriber-termination id=97_8@ipclab.cisco.com;</pre> <p>Changes OOS subscriber terminations to UEQP</p> <pre>unequip subscriber-termination id=97_8@ipclab.cisco.com;</pre> <p>Changes INS subscriber terminations and puts them in UEQP, subscriber terminations state must be UEQP before you can delete them.</p>
Viewing test menus	<pre>diag subscriber-termination; test=<TAB></pre> <pre>diag subscriber-termination; test=<RETURN></pre>
Testing subscriber terminations (place subscriber terminations in MAINT state first)	<pre>diag subscriber-termination id=sub-ubr3-1@cisco.com; test=3; ring-duration=10;</pre> <p>Note Ring-duration values are 0–999 (Default = 5). Maximum ring time is 30 seconds regardless of whether the duration is set higher than or equal to 31.</p> <ol style="list-style-type: none"> 1. Tests if MGCP has access to the termination 2. Tests if there is a path to the device (ping) 3. Tests if the subscriber can be rung 4. Performs tests 1 through 3

If a subscriber termination command fails, it can return one of the following generic failure reasons, as well as ones specific to the command.

Table 5-6 Understanding Subscriber Command Responses

Command Entered	Command Response	Possible Conditions
<code>status</code> or <code>control</code>	Failure	<ul style="list-style-type: none"> • Subscriber database was not found in shared memory. • Component is already in the requested state. • Graceful mode only, this appears when a command is executed and operation is INS going OSS or INS going MAINT. • A required resource is not available. For example: The MGW for a subscriber is down, the subscriber cannot be added. • An associated resource of the database cannot be found. • An assigned resource is not valid (supported). For example, a subscriber is assigned to a PBX and the PBX is not supported.

Table 5-6 Understanding Subscriber Command Responses (continued)

Command Entered	Command Response	Possible Conditions
Any	failure	<ul style="list-style-type: none"> • Found no failure, subscriber category invalid, entity unequipped in initial state, unknown failure reason(s). • Subscriber(s) cannot be found, subscriber(s) state change and pending. • No termination(s) found in MGW. • Fail while in termination table. • Administration state invalid, operational state invalid. • Failed to allocate IPC message(s), failed to dispatch IPC message(s). • Entity in desired state. • Not allow subscriber to reset. • Change to out-of-service state required.
Subscriber commands	Failure	<ul style="list-style-type: none"> • The media gateway is down, unreachable, in a faulty state, transitioning to another state. • The transaction could not be executed because the endpoint is unknown, the endpoint is not ready, the endpoint does not have enough resources available, the endpoint is restarting, the command contained an unrecognized extension, the gateway is not equipped to detect one of the requested events, the gateway is not equipped to generate one of the requested signals, the gateway cannot send the specified announcement. • Invalid conn identifier, invalid call ID. • Unsupported mode or invalid mode, unsupported or unknown package. • Endpoint does not have a digit map, endpoint redirected to another Call Agent, endpoint malfunctioning, endpoint taken out of service. • No such event or signal. • Unknown action or illegal combination of actions. • Internal consistency in local connection options, unknown extensions in local connection options, unsupported values on local connection options. • Insufficient bandwidth. • Missing remote connection descriptor. • Incompatible protocol version. • Response too big. • Loss of lower connectivity. • No fault reason available.

Managing Gateways

Table 5-7 Managing Gateways

Task	Sample Command
Viewing H.323 gateways	<pre>status h323-gw id=CHINA-1;</pre> <p>Possible RAS states:</p> <ul style="list-style-type: none"> • CCH323_RAS_STATE_NONE—operational state is ADMIN OOS • CCH323_RAS_STATE_GRQ—Gatekeeper Discovery state • CCH323_RAS_STATE_RRQ—Gateway Registration state • CCH323_RAS_STATE_IDLE—ready for calls • CCH323_RAS_STATE_URQ—Un-registration state.
Setting the state of H.323 gateways	<pre>control h323-gw id=CHINA_1; target-state=INS;</pre>
Viewing signaling gateway processes (SGPs)	<pre>status sgp id=sgp1;</pre>
Viewing media gateways status	<pre>status mgw id=c5300_197;</pre> <p>Possible states:</p> <ul style="list-style-type: none"> • ADMIN-INS—In-service • ADMIN-OOS—Out of service • ADMIN-MAINT—Maintenance Mode • ADMIN-OOS-PENDING—Transitioning to out of service • ADMIN-MAINT-PENDING—Transitioning to Maintenance Mode
Reporting all MTAs that use “best effort” (non DQoS) calls in the network having or not having a specific aggr id	<pre>report mgw id=%; oper-status=qos-best-effort; aggr-id=aggr1; start_row=1; limit=5;</pre> <p>Displays the output as CLI as the output-type has not been mentioned</p> <p>or</p> <pre>report mgw id=%; oper-status=qos-best-effort; aggr-id=%; output-type=xml; start_row=1; limit=5; output=report;</pre> <p>Displays the output in the specific format (CSV/XML) based on the output-type specified</p> <p>Note The output displays only those mgws that use NCS variant.</p>

Table 5-7 *Managing Gateways (continued)*

Task	Sample Command
Changing media gateway status	<pre>control mgw id=c5300_162; mode=forced; target-state=INS;</pre> <p>Modes can be forced or graceful. Forced tears down all calls immediately; graceful allows calls in progress to complete before teardown.</p> <p>Note Rules for changing an MGW states are in Figure 5-1.</p> <pre>control mgw id=c2421.65; mode=forced; target-state=maint;</pre> <p>Forces MAINT state, do this before testing</p>
Viewing media gateway test menus	<pre>diag mgw test= <TAB></pre> <p>or</p> <pre>diag mgw test= <RETURN></pre>
Testing media gateways (place gateways in MAINT state first)	<pre>diag mgw id=ubr-03; test=1;</pre>

If a gateway command fails, you might receive one of the following generic failure reasons, or one specific to the command.

Table 5-8 Understanding Gateway Command Responses

Command Entered	Command Response	Possible Conditions
<code>status</code> or <code>control</code>	Failure	<ul style="list-style-type: none"> Media gateway database was not found in shared memory. Component is already in the requested state. Graceful mode only. Appears when a command is executed and operation is INS going OSS or INS going MAINT. A required resource is not available. An associated resource of the database cannot be found. An assigned resource is not valid (supported).
any	Failure	<ul style="list-style-type: none"> Found no failure. MGW(s) cannot be found, no termination(s) found in MGW, MGW(s) state change and pending, found MGW admin state not ready. No TG(s) found in trunking gateway. Fail while getting MGW administration state, fail while looking for MGW index. Administration state invalid. Failed to allocate IPC message(s), failed to dispatch IPC message(s). Operational state invalid. Subscriber(s) state change and pending. Trunk(s) state change and pending. Found subscriber category invalid. Entity in desired state. Change to out-of-service state required. Change to request graceful mode error. Found entity unequipped in initial state. The H.323 Gateway was not found in DBM. Found unknown failure reason(s).

Managing Other External Resources


Table 5-9 Managing External Resources

Task	Sample Command
Viewing SIP phones	<code>status sip-reg-contact aor-id=4695551885@SYS44CA146.boston3.com;</code>
Viewing aggregation router status	<code>status aggr id=CMTS1</code>

Table 5-9 *Managing External Resources (continued)*

Task	Sample Command
Shows all CMTS (Aggr-ID) that are not referred by any Subnet.	<code>report aggr subnet=NONE;</code>
Viewing destination point codes (DPCs) status for availability and congestion	<code>status dpc id=dpc1;</code>
Viewing Stream Control Transmission Protocol (SCTP) associations	<code>status sctp-assoc id=sctpassoc1;</code>
Taking an SCTP association OOS	<code>control sctp-assoc id=sctpassoc1; target-state=INS; mode=FORCED;</code> Modes can be forced or graceful. Forced tears down all calls immediately; graceful allows calls in progress to complete before teardown.
Viewing subsystems	<code>show subsystem;</code>
Viewing subsystems status	<code>status subsystem id=LNP_SSN; opc_id=opc;</code>
Changing subsystem status	<code>control subsystem id=LNP_SSN; opc_id=opc; target-state=OOS; mode=FORCED;</code>
Viewing CA/FS status	<code>show sup-config</code>
Changing CA/FS status refresh rate	<code>change sup-config type= refresh-rate; value=600</code>
Changing NTP servers	<ol style="list-style-type: none"> 1. Modify 'server' line(s) in /etc/ntp.conf. 2. Modify 'NTP_SERVERS' in /etc/opticall.cfg 3. Restart daemon: <pre> /etc/init.d/xntp stop /etc/init.d/xntp start </pre> 4. Verify configuration change: <pre> /opt/BTSxntp/bin/ntpq -c peers" </pre>

Table 5-9 Managing External Resources (continued)

Task	Sample Command
Ensuring billing server receives Call Detail Blocks (CDBs)	<ol style="list-style-type: none"> 1. On both the primary and secondary EMS enter: <code>CLI>show billing-acct-addr</code> 2. Note the polling interval. 3. Log in to the billing server. 4. Ensure it receives billing files every XX minutes from the BTS, where XX = polling interval.
Clearing billing directory	<p> Caution Remove only transferred or secondary files. Never remove primary files, you need these to collect revenue.</p> <ol style="list-style-type: none"> 1. Check the default format secondary files: <code><billing-file-prefix>-<call-agent-id>-(0/1){+/-}HHMMSS- -yyyymmdd-hhmmss-<sequence-number>-<S></code> where s=secondary state 2. Check the PacketCable-specific format secondary files: <code><billing-file-prefix>_yyyymmddhhmmss_<priority>_<1>_<c ms-id>_<sequence-number>.ascii[.tmp]</code> where 1=secondary record-type 3. On the secondary EMS enter <code><hostname>#df -k</code> 4. Ensure the /opt directory is not more than 70% full. If the /opt directory is >70% full, remove obsolete scripting files and other user-generated files. Also remove obsolete files from the backup directory. For help call Cisco TAC.

Learning External Resource Dependencies

Table 5-10 RGW and Subscriber Termination States

RGW State	Allowed Subscriber Termination States
OOS	<ul style="list-style-type: none"> • OOS • UEQP

Table 5-10 *RGW and Subscriber Termination States (continued)*

RGW State	Allowed Subscriber Termination States
INS	<ul style="list-style-type: none"> • OOS • MAINT • INS • UEQP
MAINT	<ul style="list-style-type: none"> • OOS • MAINT • UEQP

Table 5-11 *ISDN TGW/TG State Relationships*

TGW State	Allowed TG States
INS	<ul style="list-style-type: none"> • OOS • MAINT • INS
MAINT	<ul style="list-style-type: none"> • OOS • MAINT

This table lists the administrative states BTS returns.

Table 5-12 *Returnable Administrative States*

State	Definition
ADMIN-INS	In service.
ADMIN-OOS	Out of service.
ADMIN-MAINT	Maintenance Mode.
ADMIN-OOS-Pending	Transitioning to out of service.
ADMIN-MAINT-Pending	Transitioning to Maintenance Mode.
ACL	Congestion is at level 1
ACL	Congestion is at level 2
ACL	Congestion is at level 3
TFC	Congestion is at level 1
TFC	Congestion is at level 2
TFC	Congestion is at level 3

Table 5-13 ISDN TGW/TG State Relationships

TGW State	Allowed TG States	Allowed Trunk States
INS	<ul style="list-style-type: none"> • OOS • MAINT • INS 	<ul style="list-style-type: none"> • UEQP OOS • UEQP OSS, MAINT • UEQP OOS, MAINT, INS
MAINT	<ul style="list-style-type: none"> • OOS • MAINT 	<ul style="list-style-type: none"> • UEQP OOS • UEQP OSS, MAINT

Table 5-14 Valid Normal Trunk Termination States

State/Token	ADMIN-STATE	OPER-STATE	STATIC-STATE	DYNAMIC-STATE
UNEQP	UNEQP	ANY	UEQP	IDLE
MANUALLY OOS	OOS	ANY	LBLK	IDLE
MANUALLY MAIN	MAINT	IDLE	LBLK	IDLE
IDLE	INS	IDLE	ACTV	IDLE
ACTIVE INCOMING	INS	IDLE	ACTV	IDLE
ACTIVE OUTGOING	INS	ACTIVE	ACTV	OBSY
TRANSIENT INCOMING	INS	ACTIVE	ACTV	IBY-TRNS
TRANSIENT OUTGOING	INS	BUSY	ACTV	OBSY-TRNS


**Note**

If a call termination attempt is made on a termination for which gateway is unreachable, the termination status will be updated as unreachable even if MGW keepalive is disabled.

Table 5-15 Returnable Operational States

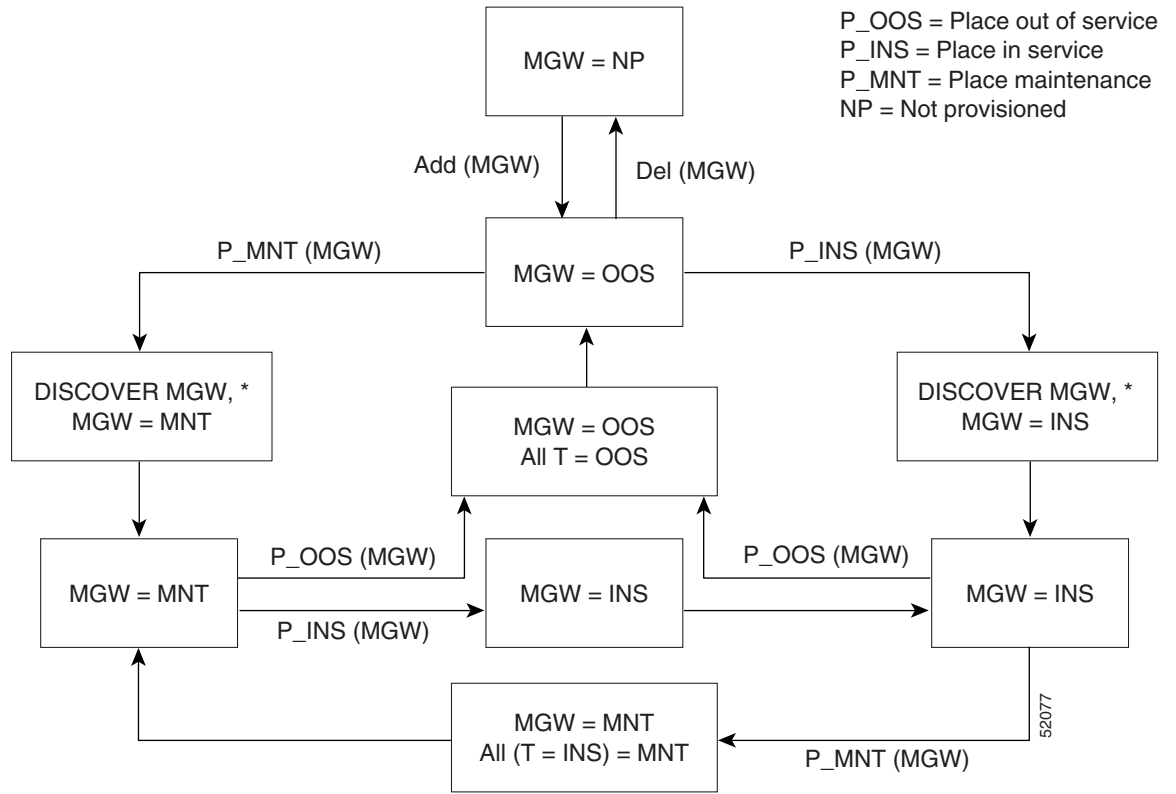
State	Definition
UNKNOWN	<ul style="list-style-type: none"> • The termination is not being audited for connectivity. • Capabilities, termination, and connection are not being synchronized with the termination. • When KEEPALIVE-METHOD=NONE in MGW-PROFILE, the termination status is UNKNOWN even if the transaction becomes UNREACHABLE. • Newly-provisioned terminations are in this state.
ACTIVE	<ul style="list-style-type: none"> • The termination is being audited for connectivity. • Capabilities, termination, and connection are being synchronized with the termination.

Table 5-15 Returnable Operational States (continued)

State	Definition
UNREACHABLE	<ul style="list-style-type: none"> The termination is unreachable. This occurs when MGW KEEPALIVE declares an MGW unreachable. This changes to ACTIVE when MGW KEEPALIVE detects an MGW is reachable or any termination previously UNREACHABLE starts sending MGCP messages (NTFY, RSIP).
FAULTY	<ul style="list-style-type: none"> The termination returned a permanent error code, making it unusable for future calls. <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p> Note The error code may occur only in certain circumstances and re-audit/auto-recovery may succeed. This does not mean the termination recovered from that condition.</p> </div> <ul style="list-style-type: none"> The flag MGCP-MAX-FAULT-COUNT controls how many times BTS tries to recover the fault (performing re-audit/auto-recovery) before putting it in this state.
MTRANS	<ul style="list-style-type: none"> Maintenance Transient, the termination is in the middle of an audit/re-audit/auto-recovery. This state may go along with other states (MTRANS-UNREACH).
IDLE	The termination is not involved in transient/active call
BUSY	<ul style="list-style-type: none"> The termination is involved in Active/Transient call. This state may go along with CTRANS state.
CTTRANS	<ul style="list-style-type: none"> Call Transient, the termination is involved in a Transient call. This state always goes with BUSY.
RESERVED	The termination is reserved for a call during Busy Line Verification
SERV_EFFC_TEST	The termination is in a Service Effecting Network loopback or Network Continuity test.
DOWN	This occurs when the MGW sends an RSIP down (graceful) message.

Source Token

Figure 5-1 Administrative and Operational Maintenance States for MGW



P_OOS = Place out of service
 P_INS = Place in service
 P_MNT = Place maintenance
 NP = Not provisioned

* "Discover" means to establish MGCP communication with MGW

52077

Figure 5-2 Administrative and Operational Maintenance States for Residential Gateways

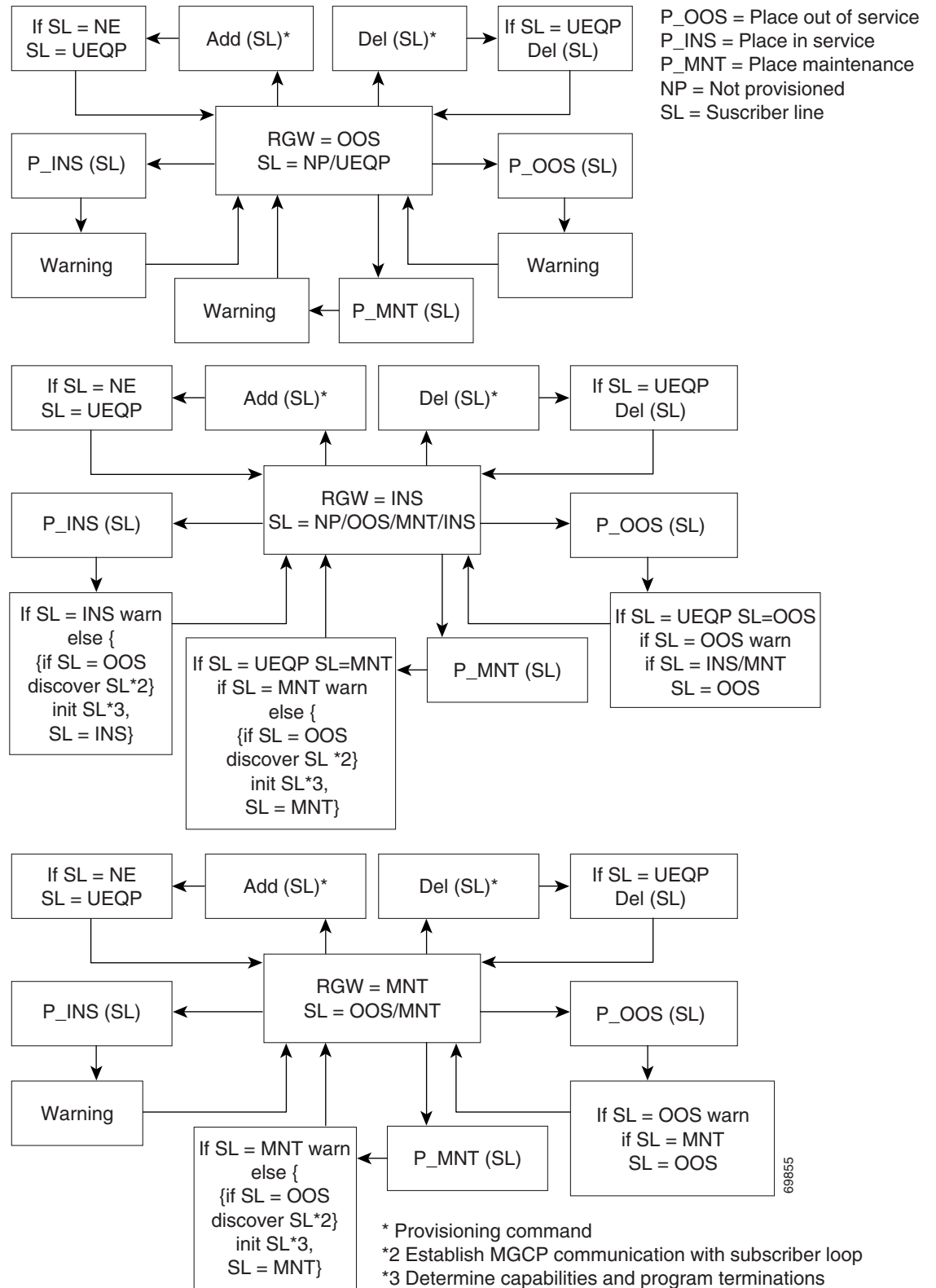
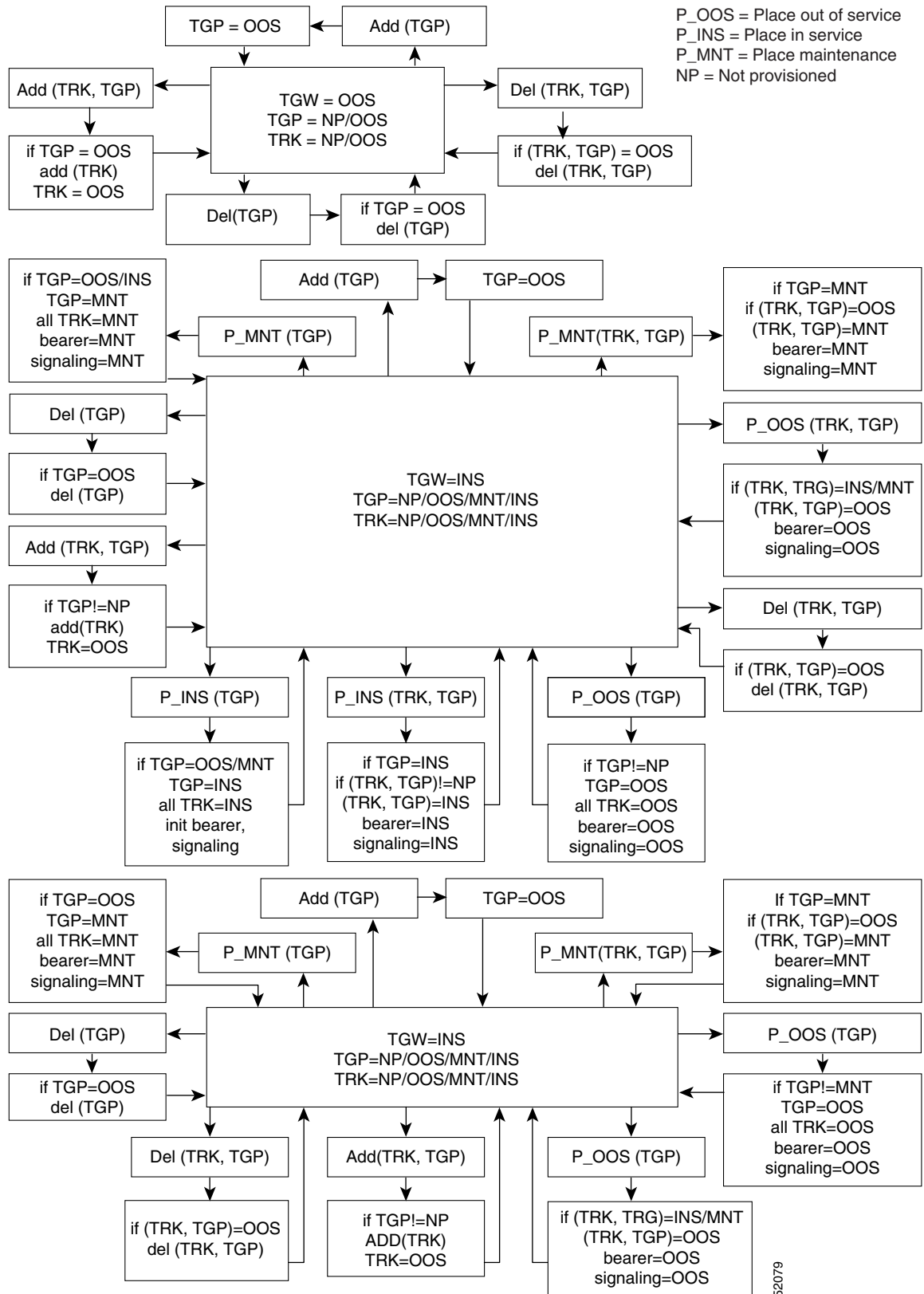
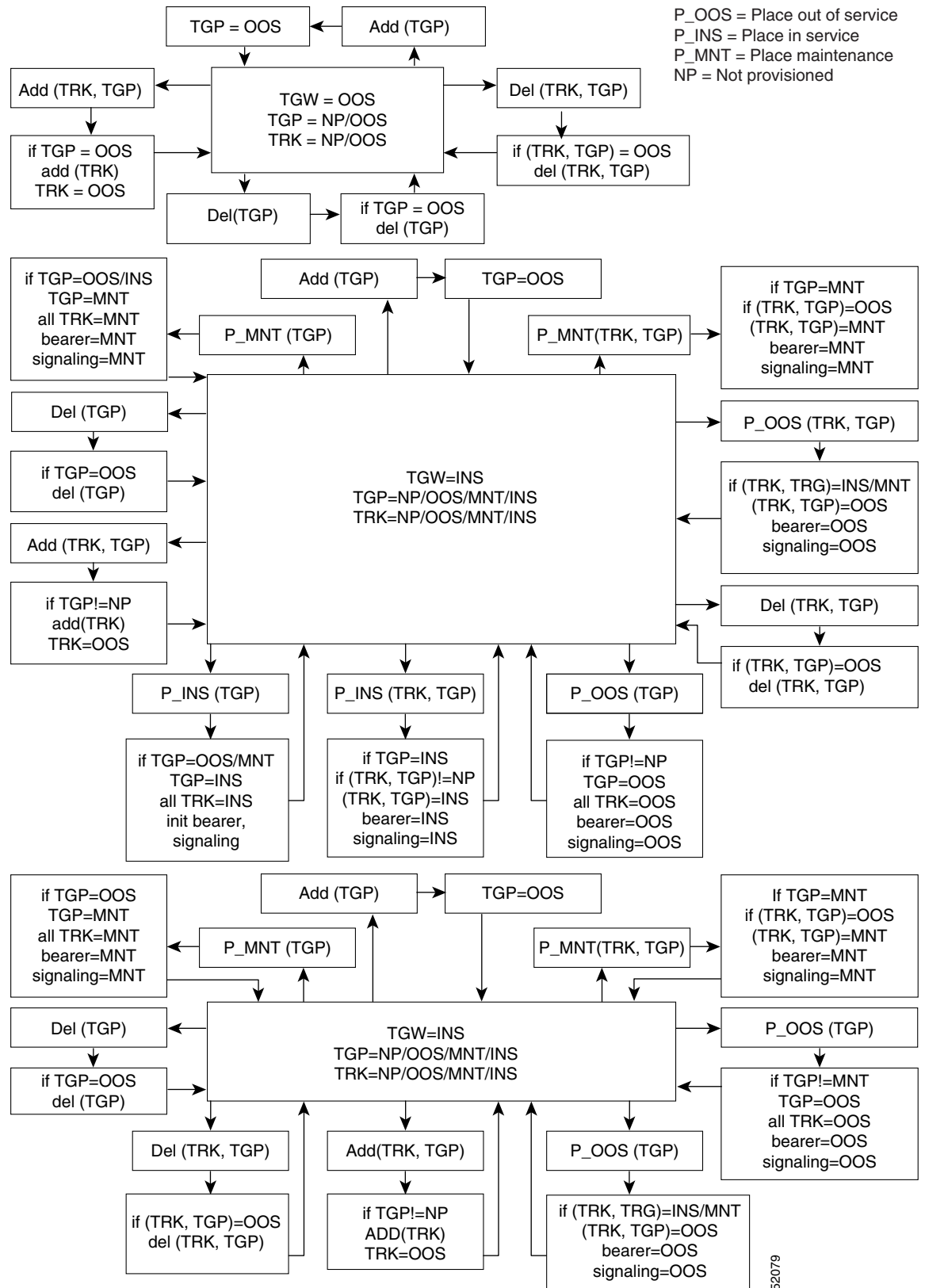


Figure 5-3 ISDN Administrative and Operational Maintenance States for a Trunking Gateway



52079



GigE Support

The purpose of implementing the GigE Support Feature provisioning is to increase the bandwidth between the network switches and the Cisco BTS 10200 from 100 Mbps to 1000 Mbps.

This section describes the steps needed to enable GigE support on the UNIX hosts of the Cisco BTS 10200 Softswitch. Use this procedure only after you upgrade to Cisco BTS 10200 Release 6.0(1) or later.



Caution

This is not an upgrade procedure. Performing the steps in this procedure will bring the Cisco BTS 10200 down on one side with temporary loss of redundancy. Do not start this procedure unless you have authorization from your supervisor. If you have questions, contact Cisco Technical Assistance Center (TAC).



Caution

Perform this procedure on one UNIX host at a time.



Caution

This procedure should be executed by a person very familiar with the operation and administration of the Cisco BTS 10200 and 29xx switches as well as the network and cabling of the Cisco BTS 10200.

Prerequisites

1. The Cisco BTS 10200 Softswitch Release 6.0(1) must already be installed.
2. The BTS 10200 UNIX host must have network interfaces capable of running at GigE speed (1000 Mbps).

Provisioning the GigE Interface

For each host in Cisco BTS 10200, perform the following steps:

- Step 1** Ensure that the targeted Cisco BTS 10200 applications are operating in standby mode. These applications include the Call Agent (CA), the Feature Server for POTS, Tandem, and Centrex services (FSPTC), the Feature Server for AIN services (FSAIN), the Element Management System (EMS), and the Bulk Data Management System (BDMS). If necessary, perform a switchover to ensure this is the case.
- Step 2** Use the **platform stop all** command to stop the targeted Cisco BTS 10200 applications running on the UNIX host.
- Step 3** Identify and note the Ethernet ports on the 29xx switches that connect to the Cisco BTS 10200 UNIX host.
- Step 4** Modify the configuration of the switch ports connected to the Cisco BTS 10200 UNIX host to auto negotiate. To do so, first log in to the 29xx switch through console access, change to the switch port, and modify the speed and duplex mode settings on each port using the following commands:

```
no speed 100
no duplex full
```

```
shut
no shut
```

Step 5 Save the switch configuration.

Step 6 Reboot the Cisco BTS 10200 host using the **shutdown -g0 -y -i6** command. We recommend that you execute the **shutdown** command using the console port to avoid loss of connectivity during the reboot. After the reboot, all the targeted Cisco BTS 10200 applications should automatically restart and go into standby state.

Step 7 Verify interface speed and duplex mode by executing the following command on the host:

```
dladm show-dev
```

Example output:

```
ca102> dladm show-dev
bge0 link: up speed: 1000 Mbps duplex: full
bge1 link: up speed: 1000 Mbps duplex: full
bge2 link: up speed: 1000 Mbps duplex: full
bge3 link: up speed: 1000 Mbps duplex: full
```

Step 8 Repeat for the other UNIX hosts in the Cisco BTS 10200 system.



CHAPTER 6

Using BTS Measurements

Revised: August 10, 2011, OL-25015-01

Introduction

This chapter describes BTS traffic measurements and tells you how to use them. BTS does the following:

- Collects statistics in 5-, 15-, 30-, or 60-minute intervals.
- Collects TG statistics at 100 second intervals.
- Clears measurements after each interval without loss of ongoing counts.
- Saves 48 hours of statistical data in 5-, 15-, 30-, or 60-minute increments in persistent store.
- Displays of summary report of past 48-hour period.
- Provides On-demand report queries keyed by collection interval.
- Issues events.

There are many measurement types, but they all have a similar format. Only titles and measurement labels differ. Each header tells you where the data is from and whether it is normal or suspect.

Access BTS measurements using the following:

- Command-line interface (CLI), which runs over a telnet or secure shell (SSH) session.
- Comma-separated value (CSV) or Extensible Markup Language (XML) format via FTP or SFTP interface.
- SNMP MIB (version v2c).

Measurements without data for the given interval do not appear in reports.


Using Measurements

When working with measurements watch for the following:

- rapid buildup of counts—Sometimes that means congestion or processing failures.
- disparity in measurement pairs that are normally equal—The greater the difference between the two, the more likely there is a problem. For example, successful incoming messages should be nearly equal to incoming messages:

SIP_TOTAL_INCOMING_MSG
and
SIP_TOTAL_SUCCESS_INCOMING_MSG

Table 6-1 Using Measurements

Task	Sample Command
Viewing measurement types	<code>show measurement-prov type=<type>;</code>
Enabling measurements	<code>change measurement-prov type=<type>; enable=<yes>; time-interval=<time interval>;</code>
Disabling measurements	<code>change measurement-prov type=<type>; enable=<no>; time-interval=<time interval>;</code>
Changing measurement intervals	<code>change measurement-prov type=<type>; enable=<yes>; time-interval=<5>;</code>
Viewing measurement summaries	<code>report measurement-isdn-summary start-time=<start time>; end-time=<end time>; call-agent-id=<CA ID>;</code> Note Results may take a few minutes to display.
Reporting historical measurements	<code>report measurement-sim-summary start-time=2003-03-27 10:00:00; end-time=2003-03-27 12:00:00; call-agent-id=CA146; output=sim-report; output-type=csv;</code> Create reports as either CSV or XML files. Then you can view or transfer them using FTP/SFTP. Note Results may take a few minutes to display.
Viewing in-progress measurements from the data source	<code>report measurement-isdn-summary call-agent-id=CA146; output=isdn-partial-report; output-type=csv; interval=current;</code> Note This is not supported for tg-usage measurements. Note Results may take a few minutes to display.
Clearing in-progress measurements from the data source	<code>clear measurement-isdn-summary call-agent-id=CA146;</code>  Caution This permanently erases in-progress measurements.

Learning the Measurement Types

These tables list the different measurement types the BTS collects.

ISDN Measurements

Table 6-2 ISDN Measurements

Measurement	Description (* = rapid count could mean a potential problem in the system)
ISDN_ALERTING_RX	ISDN ALERTING messages received.
ISDN_ALERTING_TX	ISDN ALERTING messages sent from the reporting CA.

Table 6-2 ISDN Measurements (continued)

Measurement	Description (* = rapid count could mean a potential problem in the system)
ISDN_CALL_PROCEED_RX	ISDN CALL PROCEED messages received.
ISDN_CALL_PROCEED_TX	ISDN CALL PROCEED messages sent from the reporting CA.
ISDN_CONG_CNTL_TX	ISDN Congestion Control messages sent from the reporting CA, this only applies to ETSI PRI.
ISDN_CONNECT_ACK_RX	ISDN CONNECT ACK messages received.
ISDN_CONNECT_ACK_TX	ISDN CONNECT ACK messages sent from the reporting CA.
ISDN_CONNECT_RX	ISDN CONNECT messages received.
ISDN_CONNECT_TX	ISDN CONNECT messages sent from the reporting CA.
ISDN_DISCONNECT_RX	ISDN DISCONNECT messages received.
ISDN_DISCONNECT_TX	ISDN DISCONNECT messages sent from the reporting CA.
ISDN_FACILITY_RX	ISDN FACILITY messages received.
ISDN_FACILITY_TX	ISDN FACILITY messages sent from the reporting CA.
ISDN_INFORMATION_RX	ISDN INFORMATION messages received.
ISDN_INFORMATION_TX	ISDN INFORMATION messages sent from the reporting CA.
ISDN_NOTIFY_RX	ISDN NOTIFY messages received.
ISDN_NOTIFY_TX	ISDN NOTIFY messages sent from the reporting CA.
ISDN_OC_SETUP_REJECTED	ISDN calls rejected due to system overload.
ISDN_PROGRESS_RX	ISDN PROGRESS messages received.
ISDN_PROGRESS_TX	ISDN PROGRESS messages sent from the reporting CA.
ISDN_RELEASE_COMPLETE_RX	ISDN RELEASE COMPLETE messages received.
ISDN_RELEASE_COMPLETE_TX	ISDN RELEASE COMPLETE messages sent from the reporting CA.
ISDN_RELEASE_RX	ISDN RELEASE messages received.
ISDN_RELEASE_TX	ISDN RELEASE messages sent from the reporting CA.
ISDN_RESTART_ACK_RX	ISDN RESTART ACK messages received.
ISDN_RESTART_ACK_TX	ISDN RESTART ACK messages sent from the reporting CA.
ISDN_RESTART_RX	ISDN RESTART messages received.
ISDN_RESTART_TX	ISDN RESTART messages sent from the reporting CA.
ISDN_RESUME_ACK_RX	ISDN Resume Acknowledge messages received, this only applies to ETSI PRI.
ISDN_RESUME_ACK_TX	ISDN Resume Acknowledge messages sent from the reporting CA, this only applies to ETSI PRI.
ISDN_RESUME_REJ_RX	ISDN Resume Reject messages received, this only applies to ETSI PRI.
ISDN_RESUME_REJ_TX	ISDN Resume Reject messages sent from the reporting CA, this only applies to ETSI PRI.
ISDN_RESUME_TX	ISDN Resume messages sent from the reporting CA, this only applies to ETSI PRI.
ISDN_SEGMENT_RX	ISDN Segment messages received, this only applies to ETSI PRI.
ISDN_SEGMENT_TX	ISDN Segment messages sent from the reporting CA, this only applies to ETSI PRI.

Table 6-2 ISDN Measurements (continued)

Measurement	Description (* = rapid count could mean a potential problem in the system)
ISDN_SETUP_ACK_RX	ISDN SETUP ACK messages received.
ISDN_SETUP_ACK_TX	ISDN SETUP ACK messages sent from the reporting CA.
ISDN_SETUP_RX	ISDN SETUP messages received.
ISDN_SETUP_TX	ISDN SETUP messages sent from the reporting CA.
ISDN_SRVC_ACK_RX	ISDN SERVICE ACK messages received.
ISDN_SRVC_ACK_TX	ISDN SERVICE ACK messages sent from the reporting CA.
ISDN_SRVC_RX	ISDN SERVICE messages received.
ISDN_SRVC_TX	ISDN SERVICE messages sent from the reporting CA.
ISDN_STATUS_ENQUIRY_RX	ISDN STATUS ENQUIRY messages received.
ISDN_STATUS_ENQUIRY_TX	ISDN STATUS ENQUIRY messages sent from the reporting CA.
ISDN_STATUS_RX	ISDN STATUS messages received.
ISDN_STATUS_TX	ISDN STATUS messages sent from the reporting CA.
ISDN_SUSPEND_ACK_RX	ISDN Suspend Acknowledge messages received, this only applies to ETSI PRI.
ISDN_SUSPEND_ACK_TX	ISDN Suspend Acknowledge messages sent from the reporting CA, this only applies to ETSI PRI.
ISDN_SUSPEND_REJ_RX	ISDN Suspend Reject messages received, this only applies to ETSI PRI.
ISDN_SUSPEND_REJ_TX	ISDN Suspend Reject messages sent from the reporting CA, this only applies to ETSI PRI.
ISDN_SUSPEND_RX	ISDN Suspend messages received, this only applies to ETSI PRI.
ISDN_SUSPEND_TX	ISDN Suspend messages sent from the reporting CA, this only applies to ETSI PRI.
ISDN_USER_INFO_RX	ISDN User Information messages received, this only applies to ETSI PRI.
ISDN_USER_INFO_TX	ISDN User Information messages sent from the reporting CA, this only applies to ETSI PRI.

Call Processing Measurements

Table 6-3 Call Processing Measurements

Measurement	Description (* = rapid count could mean a potential problem in the system)
CALLP_NCT_TEST_FAIL	Unsuccessful Network Continuity Tests completed, both call setup failures and resource failures. These are test calls abnormally released by the CA due to resource priorities.
CALLP_NLB_TEST_FAIL	Unsuccessful Network Loop Back Tests completed. This includes both call setup failures and resource failures. These are test calls abnormally released by the CA due to reasons such as resource priorities.
CALLP_NLB_TEST_SUCC	Successful Network Loop Back Tests completed.
CALLP_CALL_ABAND	Originating call attempts of all types abandoned.
CALLP_CALL_SUCC	Successful originating and terminating call attempts of all types.
CALLP_CAS_CALL_ABAND	CAS originating call attempts abandoned.
CALLP_CAS_CALL_SUCC	Successful CAS originating and terminating call attempts.
CALLP_CAS_CAS_CALL	Successfully completed calls from an CAS originator to an CAS terminator.
CALLP_CAS_H323_CALL	Successfully completed calls from a CAS originator to an H323 terminator.
CALLP_CAS_ISDN_CALL	Successfully completed calls from an CAS originator to an ISDN terminator.
CALLP_CAS_MGCP_CALL	Successfully completed calls from an CAS originator to an MGCP terminator.
CALLP_CAS_ORIG_ATTMP	Originating CAS call attempts.
CALLP_CAS_ORIG_FAIL	CAS originating call attempts that failed.
CALLP_CAS_SIP_CALL	Successfully completed calls from an CAS originator to an SIP terminator.
CALLP_CAS_SS7_CALL	Successfully completed calls from an CAS originator to an SS7 terminator.
CALLP_CAS_TERM_ATTMP	CAS terminating call attempts.
CALLP_CAS_TERM_FAIL	CAS terminating call attempts that failed.
CALLP_EMGNCY_ATTMP	Emergency call attempts.
CALLP_EMGNCY_CALL_ABAND	Emergency call origination attempts abandoned.
CALLP_EMGNCY_CALL_SUCC	Emergency call attempts that completed successfully.
CALLP_EMGNCY_FAIL	Emergency call attempts that failed.
CALLP_H323_CALL_ABAND	Terminating and originating H323 call attempts abandoned.
CALLP_H323_CALL_SUCC	Originating and terminating H323 call attempts that completed successfully.
CALLP_H323_CAS_CALL	Successfully completed calls from an H323 originator to a CAS terminator.
CALLP_H323_H323_CALL	Successfully completed calls from an H323 originator to an H323 terminator.
CALLP_H323_ISDN_CALL	Successfully completed calls from an H323 originator to an ISDN terminator.
CALLP_H323_MGCP_CALL	Successfully completed calls from an H323 originator to an MGCP terminator.
CALLP_H323_ORIG_ATTMP	Originating H323 call attempts.
CALLP_H323_ORIG_FAIL	Originating H323 call attempts that failed.
CALLP_H323_SIP_CALL	Successfully completed calls from an H323 originator to a SIP terminator.
CALLP_H323_SS7_CALL	Successfully completed calls from an H323 originator to an SS7 terminator.

Table 6-3 Call Processing Measurements (continued)

Measurement	Description (* = rapid count could mean a potential problem in the system)
CALLP_H323_TERM_ATTMP	Terminating H323 call attempts.
CALLP_H323_TERM_FAIL	Terminating H323 call attempts that failed.
CALLP_INTERLA_ABAND	Interlata call origination attempts abandoned.
CALLP_INTERLA_ATTMP	Interlata call attempts.
CALLP_INTERLA_FAIL	Interlata call attempts that failed.
CALLP_INTERLA_SUCC	Interlata call attempts that completed successfully.
CALLP_INTL_ABAND	International call origination attempts abandoned.
CALLP_INTL_ATTMP	International call attempts.
CALLP_INTL_FAIL	International call attempts that failed.
CALLP_INTL_SUCC	International call attempts that completed successfully.
CALLP_INTRALA_ABAND	Intralata call origination attempts abandoned.
CALLP_INTRALA_ATTMP	Intralata call attempts.
CALLP_INTRALA_FAIL	Intralata call attempts that failed.
CALLP_INTRALA_SUCC	Intralata call attempts that completed successfully.
CALLP_ISDN_CALL_ABAND	ISDN originating call attempts abandoned.
CALLP_ISDN_CALL_SUCC	Successful ISDN originating and terminating call attempts.
CALLP_ISDN_CAS_CALL	Successfully completed calls from an ISDN originator to an CAS terminator.
CALLP_ISDN_H323_CALL	Successfully completed calls from an ISDN originator to an H323 terminator.
CALLP_ISDN_ISDN_CALL	Successfully completed calls from an ISDN originator to an ISDN terminator.
CALLP_ISDN_MGCP_CALL	Successfully completed calls from an ISDN originator to an MGCP terminator.
CALLP_ISDN_ORIG_ATTMP	Originating ISDN call attempts.
CALLP_ISDN_ORIG_FAIL	ISDN originating call attempts that failed.
CALLP_ISDN_SIP_CALL	Successfully completed calls from an ISDN originator to an SIP terminator.
CALLP_ISDN_SS7_CALL	Successfully completed calls from an ISDN originator to an SS7 terminator.
CALLP_ISDN_TERM_ATTMP	ISDN terminating call attempts.
CALLP_ISDN_TERM_FAIL	ISDN terminating call attempts that failed.
CALLP_IVR_NATIVE_REQ	Requests for native IVR service.
CALLP_IVR_NETWORK_REQ	Requests for network based IVR service.
CALLP_IVR_RESOURCE_FAIL	IVR sessions that could not be established.
CALLP_LB_TEST_SUCC	Successful TDM Loop Back 108 Tests completed.
CALLP_LNP_RCV_MISROUTED_PORTED	The LNP Data Inconsistencies with release message (REL): misrouted calls to a ported number (ANSI ISUP REL cause 26) reported by another exchange after an LNP query in the reporting CA.
CALLP_LNP_RCV_MISROUTED_PORTED	Misrouted calls to a ported number (ANSI ISUP REL cause 26) reported by another exchange after an LNP query.

Table 6-3 Call Processing Measurements (continued)

Measurement	Description (* = rapid count could mean a potential problem in the system)
CALLP_LNP_SND_MISROUTED_PORTED	Misrouted calls to a ported number detected after an LNP query.
CALLP_LNP_SND_MISROUTED_PORTED	Misrouted calls to a ported number detected after an LNP query in the reporting CA.
CALLP_LNP_UNALLOC_NUM_NO_GAP	<p>The LNP Unallocated Number Calls: calls resulting in either:</p> <ul style="list-style-type: none"> • an unallocated number • a misrouted ported number <p>This shows when an LNP query (from the BTS or another switch) results in either of the above conditions from the donor switch's reporting CA.</p> <p>To find out when this query occurred use the Forward Call Indicator's (FCI) Ported Number Translation indicator parameter with no "Ported Number" generic address parameter (GAP).</p>
CALLP_LNP_UNALLOC_NUM_OWN_LRN	<p>LNP calls getting an Unallocated indication. This occurs when a donor (or another switch) detects the reporting CA's own local routing number (LRN) after an LNP query.</p> <p>To find out when this query occurred use the Forward Call Indicator's (FCI) Ported Number Translation indicator parameter with a "Ported Number" generic address parameter (GAP).</p> <p>Note This does not apply to DN's marked "LNP-Reserved."</p>
CALLP_LNP_UNALLOC_NUM_NO_GAP	<p>Calls that cause unallocated number indications in the donor switch reporting call agent. This follows an LNP query in this or another switch. View the FCI parameter's Ported Number Translation indicator with no "Ported Number" GAP.</p>
CALLP_LNP_UNALLOC_NUM_OWN_LRN	<p>LNP calls getting an unallocated indication; this means the LNP query to the donor (or another) switch returns the CA's own LRN. View the FCI parameter's Ported Number Translation indicator with no "Ported Number" GAP.</p> <p>Note This does not apply to "LNP-Reserved" DN's.</p>
CALLP_LOCAL_ABAND	Local call origination attempts abandoned.
CALLP_LOCAL_ATTMP	Local call attempts.
CALLP_LOCAL_FAIL	Local call attempts that failed.
CALLP_LOCAL_SUCC	Local call attempts that completed successfully.
CALLP_MGCP_CALL_ABAND	MGCP originating call attempts abandoned.
CALLP_MGCP_CALL_SUCC	Successful MGCP originating and terminating call attempts.
CALLP_MGCP_CAS_CALL	Successfully completed calls from an MGCP originator to an CAS terminator.
CALLP_MGCP_H323_CALL	Successfully completed calls from an MGCP originator to an H323 terminator.
CALLP_MGCP_ISDN_CALL	Successfully completed calls from an MGCP originator to an ISDN terminator.
CALLP_MGCP_MGCP_CALL	Successfully completed calls from an MGCP originator to an MGCP terminator.
CALLP_MGCP_ORIG_ATTMP	Originating MGCP call attempts.
CALLP_MGCP_ORIG_FAIL	MGCP originating call attempts that failed.
CALLP_MGCP_SIP_CALL	Successfully completed calls from an MGCP originator to an SIP terminator.

Table 6-3 Call Processing Measurements (continued)

Measurement	Description (* = rapid count could mean a potential problem in the system)
CALLP_MGCP_SS7_CALL	Successfully completed calls from an MGCP originator to an SS7 terminator.
CALLP_MGCP_TERM_ATTMP	MGCP terminating call attempts.
CALLP_MGCP_TERM_FAIL	MGCP terminating call attempts that failed.
CALLP_MODEM_MEDIA_SETUP_FAIL	Failed Modem calls. These calls fail because of resource or priority limits.
CALLP_MODEM_MEDIA_SETUP_SUCC	Successfully completed Modem calls.
CALLP_NAS_ADMIN_REBOOT	Admin Reboot - Reason Code 807 - that are received in the DLCX messages.
CALLP_NAS_ADMIN_RESET	Admin Reset - Reason Code 806 - that are received in the DLCX messages.
CALLP_NAS_AUTH_FAIL	Failed NAS Authentication Requests.
CALLP_NAS_AUTH_SUCC	Successful NAS Authentication Requests.
CALLP_NAS_CALLBACK	NAS Callback - Reason Code 816 - that are received in the DLCX messages.
CALLP_NAS_CLD_UNACC	NAS calls that failed on the reporting CA due to the called party number being blocked
CALLP_NAS_CLG_UNACC	NAS calls that failed on the reportingCA due to the calling party number being blocked
CALLP_NAS_HOST_REQUEST	Host Request - Reason Code 818 - that are received in the DLCX messages.
CALLP_NAS_IDLE_TIMEOUT	Idle Timeout - Reason Code 804 - that are received in the DLCX messages.
CALLP_NAS_ISP_PORT_LIMIT	NAS calls that failed on the reporting CA due to the port limit of a modem being exceeded
CALLP_NAS_LOST_CARRIER	Lost Carrier - Reason Code 802 - that are received in the DLCX messages.
CALLP_NAS_LOST_SERVICE	Lost Service - Reason Code 803 - that are received in the DLCX messages.
CALLP_NAS_NAS_ERROR	NAS Error- Reason Code 809 - that are received in the DLCX messages.
CALLP_NAS_NAS_REBOOT	NAS Reboot- Reason Code 811 - that are received in the DLCX messages.
CALLP_NAS_NAS_REQUEST	NAS Request - Reason Code 810 - that are received in the DLCX messages.
CALLP_NAS_NO_MODEMS	NAS calls that failed on the reporting CA due to the unavailability of a modem
CALLP_NAS_OP_FAIL	Operation failures that occurred on the reporting CA - typically indicative of a modem failure
CALLP_NAS_PORT_ERROR	Port Error- Reason Code 808 - that are received in the DLCX messages.
CALLP_NAS_PORT_PREEMPTED	Port Pre-empted - Reason Code 813 - that are received in the DLCX messages.
CALLP_NAS_PORT_SUSPENDED	Port Suspended - Reason Code 814 - that are received in the DLCX messages.
CALLP_NAS_PORT_UNNEEDED	Port Unneeded - Reason Code 812 - that are received in the DLCX messages.
CALLP_NAS_SERVICE_UNAVAIL	Service Unavailable - Reason Code 815 - that are received in the DLCX messages.
CALLP_NAS_SESSION_TIMEOUT	Session Timeout - Reason Code 805 - that are received in the DLCX messages.
CALLP_NAS_USER_ERROR	User Error - Reason Code 817 - that are received in the DLCX messages.
CALLP_NAS_USER_REQUEST	User Requests - Reason Code 801 - that are received in the DLCX messages.
CALLP_NCT_TEST_SUCC	Successful Network Continuity Tests completed.

Table 6-3 Call Processing Measurements (continued)

Measurement	Description (* = rapid count could mean a potential problem in the system)
CALLP_OHD_DIALTONE_TIMEO UT	Times the off hook delay trigger timed out.
CALLP_OLM _ ACCEPT	Calls accepted by OLM.
CALLP_OLM _ ACCEPT_MCL0	Calls accepted by OLM at MCL0.
CALLP_OLM _ ACCEPT_MCL1	Calls accepted by OLM at MCL1.
CALLP_OLM _ ACCEPT_MCL2	Calls accepted by OLM at MCL2.
CALLP_OLM _ ACCEPT_MCL3	Calls accepted by OLM at MCL3.
CALLP_OLM _ MCL1_COUNT	MCL1 occurrences.
CALLP_OLM _ MCL2_COUNT	MCL2 occurrences.
CALLP_OLM _ MCL3_COUNT	MCL3 occurrences.
CALLP_OLM _ MCL4_COUNT	MCL4 occurrences.
CALLP_OLM _ REJECT	Calls rejected by OLM.
CALLP_OLM _ REJECT_EMERGENCY	Emergency Calls rejected by OLM at MCL4.
CALLP_OLM _ REJECT_MCL1	Calls rejected by OLM at MCL1.
CALLP_OLM _ REJECT_MCL2	Calls rejected by OLM at MCL2.
CALLP_OLM _ REJECT_MCL3	Calls rejected by OLM at MCL3.
CALLP_OLM _ REJECT_MCL4	Calls rejected by OLM at MCL4.
CALLP_OLM _ OFFERED	Calls offered to OLM.
CALLP_OLM_ISUP_MSG_DUMPE D	ISUP messages dumped at MCL4 by layer3 (MIM) due to system overload.
CALLP_ORIG_ATTMP	Originating call attempts of all types.
CALLP_ORIG_FAIL	Originating call attempts of all types that failed.
CALLP_SIP_AS_302_TOTAL	Application Server calls that returned a 302 message.
CALLP_SIP_AS_REFERERRED_NEW DN	Application Server calls that returned a new DN.
CALLP_SIP_AS_REFERERRED_TOT AL	Application Server calls referred back.
CALLP_SIP_CALL_ABAND	SIP originating call attempts abandoned.
CALLP_SIP_CALL_SUCC	Successful SIP originating and terminating call attempts.
CALLP_SIP_CAS_CALL	Successfully completed calls from a SIP originator to an CAS terminator.
CALLP_SIP_H323_CALL	Successfully completed calls from a SIP originator to an H323 terminator.
CALLP_SIP_ISDN_CALL	Successfully completed calls from a SIP originator to an ISDN terminator.
CALLP_SIP_MGCP_CALL	Successfully completed calls from a SIP originator to an MGCP terminator.
CALLP_SIP_ORIG_ATTMP	Originating SIP call attempts.
CALLP_SIP_ORIG_CALL_ABDN	This counter is pegged when the caller abandons the call before the called party answers the call.

Table 6-3 Call Processing Measurements (continued)

Measurement	Description (* = rapid count could mean a potential problem in the system)
CALLP_SIP_ORIG_CALL_NOT_ANS	This counter is pegged when the incoming call is not answered by the called party.
CALLP_SIP_ORIG_END_USR_BUSY	This counter is pegged when the incoming call is not complete due to the called party being busy.
CALLP_SIP_ORIG_FAIL	The number of incoming SIP calls that are not established. This counter does not include the calls in these conditions: <ul style="list-style-type: none"> • When the call is abandoned by the caller before the called party answers. • The called party is busy. • The called party is not responding to the incoming call.
CALLP_SIP_ORIG_SUCC	Number of incoming established SIP calls.
CALLP_SIP_SIP_CALL	Successfully completed calls from a SIP originator to an SIP terminator.
CALLP_SIP_SS7_CALL	Successfully completed calls from a SIP originator to an SS7 terminator.
CALLP_SIP_TERM_ATTMP	SIP terminating call attempts.
CALLP_SIP_TERM_CALL_ABDN	This counter is pegged when the outgoing call is abandoned by the originator before the called party answers.
CALLP_SIP_TERM_CALL_NOT_ANS	This counter is pegged when the outgoing call is not answered by the called party.
CALLP_SIP_TERM_END_USR_BUSY	This counter is pegged when the outgoing call is terminated as the called party was busy. <p>Note The originating and terminating counters are pegged for both originating and terminating calls if both are using SIP.</p>
CALLP_SIP_TERM_FAIL	The number of outgoing SIP calls that are not established. This counter does not include the calls in these conditions: <ul style="list-style-type: none"> • When the call is abandoned by the caller before the called party answers. • The called party is busy. • The called party is not responding to the incoming call.
CALLP_SIP_TERM_SUCC	Number of outgoing established SIP calls.
CALLP_SS7_CALL_ABAND	SS7 originating call attempts abandoned.
CALLP_SS7_CALL_SUCC	Successful SS7 originating and terminating call attempts.
CALLP_SS7_CAS_CALL	Successfully completed calls from an SS7 originator to an CAS terminator.
CALLP_SS7_H323_CALL	Successfully completed calls from an SS7 originator to an H323 terminator.
CALLP_SS7_ISDN_CALL	Successfully completed calls from an SS7 originator to an ISDN terminator.
CALLP_SS7_MGCP_CALL	Successfully completed calls from an SS7 originator to an MGCP terminator.
CALLP_SS7_ORIG_ATTMP	Originating SS7 call attempts.
CALLP_SS7_ORIG_FAIL	SS7 originating call attempts that failed.
CALLP_SS7_SIP_CALL	Successfully completed calls from an SS7 originator to an SIP terminator.
CALLP_SS7_SS7_CALL	Successfully completed calls from an SS7 originator to an SS7 terminator.

Table 6-3 Call Processing Measurements (continued)

Measurement	Description (* = rapid count could mean a potential problem in the system)
CALLP_SS7_TERM_ATTMP	SS7 terminating call attempts.
CALLP_SS7_TERM_FAIL	SS7 terminating call attempts that failed.
CALLP_T38_FAX_MEDIA_SETUP_FAIL	Unsuccessful T.38 media connections between the endpoints for T.38 fax transmission.
CALLP_T38_FAX_MEDIA_SETUP_SUCC	Successful T.38 media connections between the endpoints for T.38 fax transmission.
CALLP_TDD_MEDIA_SETUP_FAIL	Failed calls of Call Type RELAY. The CA abnormally releases these calls because of resource or priority limits.
CALLP_TDD_MEDIA_SETUP_SUCC	Successfully completed calls of Call Type RELAY.
CALLP_TERM_ATTMP	Terminating call attempts of all types.
CALLP_TERM_FAIL	Terminating call attempts of all types that failed.
CALLP_TERM_WB_LIST_ALLOW	Terminating calls allowed by the white/black list.
CALLP_TERM_WB_LIST_BLOCK	Terminating calls blocked by the white/black list.
CALLP_TEST_ROUTE_SUCC	Successful TDM Loop Back 108 Tests with DN dialed out in outgoing message completed.
CALLP_TOLL_FREE_ABAND	Toll Free call origination attempts abandoned.
CALLP_TOLL_FREE_ATTMP	Toll Free call attempts.
CALLP_TOLL_FREE_FAIL	Toll Free call attempts that failed.
CALLP_TOLL_FREE_SUCC	Toll Free call attempts that completed successfully.
CALLP_TOTAL_SEASONAL_SUSPEND_ORIG_ATTMP	Origination attempts by subscribers marked as seasonal suspend.
CALLP_TOTAL_TDISC_ORIG_ATTMP	Origination attempts by subscribers marked as temporarily disconnected.

MGCP Adapter Measurements

Table 6-4 MGCP Adapter Measurements

Measurement	Description (* = rapid count could mean a potential problem in the system)
MGCP_AUCX_ACK_RX	AUCX ACK (Audit Connection Acknowledgement) messages received. Note This is enabled in a future release.
MGCP_AUCX_NACK_RX	AUCX NACK (Audit Connection NotAcknowledgement) messages received. Note This is enabled in a future release.
MGCP_AUCX_TX	AUCX (Audit Connection) messages sent. Note This is enabled in a future release.
MGCP_AUEP_ACK_RX	MGCP AUEP acknowledgement messages received.
MGCP_AUEP_NACK_RX	MGCP AUEP non-acknowledgement messages received.
MGCP_AUEP_TX	MGCP AUEP messages sent.
MGCP_CRCX_ACK_RX	MGCP CRCX acknowledgement messages received.
MGCP_CRCX_NACK_RX	MGCP CRCX non-acknowledgement messages received.
MGCP_CRCX_TX	MGCP CRCX messages sent.
MGCP_DECODE_ERROR	MGCP messages received that failed decoding.
MGCP_DLCX_ACK_RX	MGCP DLCX acknowledgement messages received.
MGCP_DLCX_NACK_RX	MGCP DLCX non-acknowledgement messages received.
MGCP_DLCX_RX	MGCP DLCX messages received from gateways.
MGCP_DLCX_TX	MGCP DLCX messages sent.
MGCP_ENCODE_ERROR	MGCP messages to be sent that failed encoding.
MGCP_MDCX_ACK_RX	MGCP MDCX acknowledgement messages received.
MGCP_MDCX_NACK_RX	MGCP MDCX non-acknowledgement messages received.
MGCP_MDCX_TX	MGCP MDCX messages sent.
MGCP_NTFY_RX	MGCP NTFY messages received from gateways.
MGCP_OC_CALL_REJECTED	MGCP calls rejected due to system overload.
MGCP_RQNT_ACK_RX	MGCP RQNT acknowledgement messages received.
MGCP_RQNT_NACK_RX	MGCP RQNT non-acknowledgement messages received.
MGCP_RQNT_TX	MGCP RQNT messages sent.
MGCP_RSIP_ACK_TX	MGCP RSIP acknowledgement messages sent.
MGCP_RSIP_RX	MGCP RSIP messages received from gateways.
MGCP_SEND_FAILED	MGCP messages sent from the reporting CA that failed while being sent to the target gateway.
MGCP_UNREACHABLE	MGCP messages sent from the reporting CA that failed due to the target gateway being unreachable.

DQoS Measurements

Table 6-5 DQoS Measurements

Measurement	Description (* = rapid count could mean a potential problem in the system)
DQOS_GATE_CLOSE_RX	DQOS Gate-Open messages received by the reporting BTS.
DQOS_GATE_DELETE_ACK_RX	DQOS Gate-Delete-Ack messages received by the reporting BTS.
DQOS_GATE_DELETE_TX	DQOS Gate-Delete messages sent from the reporting BTS.
DQOS_GATE_DELETE_ERR_RX	DQOS Gate-Delete-Err messages received by the reporting BTS.
DQOS_GATE_INFO_ACK_RX	DQOS Gate-Info-Ack messages received by the reporting BTS.
DQOS_GATE_INFO_ERR_RX	DQOS Gate-Info-Err messages received by the reporting BTS.
DQOS_GATE_INFO_TX	DQOS Gate-Info messages sent from the reporting BTS.
DQOS_GATE_OPEN_RX	DQOS Gate-Open messages received by the reporting BTS.
DQOS_GATE_SET_ACK_RX	DQOS Gate-Set-Ack messages received by the reporting BTS.
DQOS_GATE_SET_ERR_RX	DQOS Gate-Set-Err messages received by the reporting BTS.
DQOS_GATE_SET_TX	DQOS Gate-Set messages sent from the reporting BTS.

SIP Measurements

This table lists measurements for the Session Initiation Protocol (SIP). These are common to several reporting types: SIM, AIN-SVC, POTS-MISC, and SIA.

Table 6-6 Session Initiation Protocol (SIP) Measurements

Measurement	Description (* = rapid count could mean a potential problem in the system)
SIS_100_RX	100 class (TRYING) messages the reporting CA or FS received.
SIS_100_TX	100 class (TRYING) messages the reporting CA or FS sent.
SIS_18x_RX	18x class (INFORMATIONAL) messages the reporting CA or FS received.
SIS_18x_TX	18x class (INFORMATIONAL) messages the reporting CA or FS sent.
SIS_200_RX	200 class (SUCCESS) messages the reporting CA or FS received.
SIS_200_TX	200 class (SUCCESS) messages the reporting CA or FS sent.
SIS_3xx_RX	3xx class (REDIRECTION) messages the reporting CA or FS received.
SIS_3xx_TX	3xx class (REDIRECTION) messages the reporting CA or FS sent.
SIS_4xx_RX	4xx class (REQUEST FAILURES) messages the reporting CA or FS received.
SIS_4xx_TX	4xx class (REQUEST FAILURES) messages the reporting CA or FS sent.
SIS_5xx_RX	5xx class (SERVER FAILURES) messages the reporting CA or FS received.
SIS_5xx_TX	5xx class (SERVER FAILURES) messages the reporting CA or FS sent.
SIS_6xx_RX	6xx class (GLOBAL FAILURES) messages the reporting CA or FS received.
SIS_6xx_TX	6xx class (GLOBAL FAILURES) messages the reporting CA or FS sent.

Table 6-6 Session Initiation Protocol (SIP) Measurements (continued)

Measurement	Description (* = rapid count could mean a potential problem in the system)
SIS_7xx_RX	7xx class (RESERVED) messages the reporting CA or FS received.
SIS_7xx_TX	7xx class (RESERVED) messages the reporting CA or FS sent.
SIS_ACK_RX	SIP ACK messages the reporting CA or FS received.
SIS_ACK_TX	SIP ACK messages the reporting CA or FS sent.
SIS_BYE_RX	SIP BYE messages the reporting CA or FS received.
SIS_BYE_TX	SIP BYE messages the reporting CA or FS sent.
SIS_CANCEL_RX	SIP CANCEL messages the reporting CA or FS received.
SIS_CANCEL_TX	SIP CANCEL messages the reporting CA or FS sent.
SIS_INFO_RX	SIP INFO messages the reporting CA or FS received.
SIS_INFO_TX	SIP INFO messages the reporting CA or FS sent.
SIS_INVITE_REPLACES_RX	SIP INVITE REPLACES messages the reporting CA or FS received.
SIS_INVITE_REPLACES_TX	SIP INVITE REPLACES messages the reporting CA or FS sent..
SIS_INVITE_RX	SIP INVITE messages the reporting CA or FS received.
SIS_INVITE_TX	SIP INVITE messages the reporting CA or FS sent.
SIS_NOTIFY_RX	SIP NOTIFY messages the reporting CA or FS received.
SIS_NOTIFY_TX	SIP NOTIFY messages the reporting CA or FS sent.
SIS_OPTIONS_RX	SIP OPTIONS messages the reporting CA or FS received.
SIS_OPTIONS_TX	SIP OPTIONS messages the reporting CA or FS sent.
SIS_PRACK_RX	SIP PRACK messages the reporting CA or FS received.
SIS_PRACK_TX	SIP PRACK messages the reporting CA or FS sent.
SIS_PROV_RSP_RETRAN_RX	SIP provisioning response retransmission messages the reporting CA or FS received.
SIS_PROV_RSP_RETRAN_TX	SIP provisioning response retransmission messages the reporting CA or FS sent.
SIS_REFERER_RX	SIP REFER messages the reporting CA or FS received.
SIS_REFERER_TX	SIP REFER messages the reporting CA or FS sent..
SIS_REFERER_W_REPLACES_RX	SIP REFER with REPLACES messages the reporting CA or FS received.
SIS_REGISTER_RX	SIP REGISTER messages the reporting CA or FS received.
SIS_REGISTER_TX	SIP REGISTER messages the reporting CA or FS sent.
SIS_REL100_RX	REL100 class (TRYING) messages the reporting CA or FS received.
SIS_REL100_TX	REL100 class (TRYING) messages the reporting CA or FS sent..
SIS_REQ_RETRAN_RX	SIP request retransmission messages the reporting CA or FS received.
SIS_REQ_RETRAN_TX	SIP request retransmission messages the reporting CA or FS sent.
SIS_RSP_RETRAN_RX	SIP response retransmission messages the reporting CA or FS received.
SIS_RSP_RETRAN_TX	SIP response retransmission messages the reporting CA or FS sent.
SIS_SUBSCRIBE_RX	SIP SUBSCRIBE messages the reporting CA or FS received.

Table 6-6 Session Initiation Protocol (SIP) Measurements (continued)

Measurement	Description (* = rapid count could mean a potential problem in the system)
SIS_SUBSCRIBE_TX	SIP SUBSCRIBE messages the reporting CA or FS sent.
SIS_T1_TIMER_EXPIRED	SIP T1 Timer expirations that occurred on the reporting CA or FS received over the collection interval.
SIS_T2_TIMER_REACHED	SIP T2 Timer expirations that occurred on the reporting CA or FS received over the collection interval.
SIS_TOTAL_INCOM_MSG	SIP messages the reporting CA or FS attempted to receive.
SIS_TOTAL_OUTG_MSG_ATTMP	SIP messages the reporting CA or FS attempted to send.
SIS_TOTAL_SUCC_INCOM_MSG	SIP messages the reporting CA or FS successfully received.
SIS_TOTAL_SUCC_OUTG_MSG	SIP messages the reporting CA or FS successfully sent.
SIS_UNSUPPORTED_RX	Unsupported SIP messages the reporting CA or FS received.
SIS_UPDATE_RX	SIP UPDATE messages the reporting CA or FS received.
SIS_UPDATE_TX	SIP UPDATE messages the reporting CA or FS sent..

Service Interaction Manager Measurements

Table 6-7 Service Interaction Manager Measurements

Measurement	Description (* = rapid count could mean a potential problem in the system)
SIM_AUDIT_CCB_FREED	SIM relationships terminated with SSF due to the SIM memory audit.
SIM_AUDIT_SIP_CCB_FREED	SIM to SIP relationships released with the FS do to the SIM memory audit.
SIM_BCM_MSG	messages received by call processing from a FS in the reporting CA.
SIM_EDP_N	Event Detection Point messages received from call processing in the reporting CA that do not require a response from the target FS.
SIM_EDP_R	Event Detection Point messages received from call processing in the reporting CA that do require a response from the target FS.
SIM_FS_ASYNC_MSG_TX	ASYNC messages sent to FSs.
SIM_FS_MSG_RX	FCP messages received from FSs.
SIM_FS_MSG_TX	FCP messages sent to FSs.
SIM_FS_PING_MSG_TX	PING messages sent to FSs.
SIM_FS_PING_NO_RSP_FAULTY	Times no response was received from the target FS when sent a PING message.
SIM_FS_RESTART_MSG_TX	RESTART messages sent to FSs.
SIM_INSTRUCT	INSTRUCT messages sent to FSs.
SIM_INSTRUCT_RSP	INSTRUCT messages received from FSs.
SIM_OC_EMG_TRIG_FORCED	Emergency triggers forced when the FS is overloaded.
SIM_OC_TRIG_FILTERED	Triggers dropped when the FS is overloaded.
SIM_OC_TRIG_FORCED	Triggers forced when the FS is overloaded. This is usually for triggers in an existing call.
SIM_RELATIONS	TDP-Rs received from call processing by SIM in the reporting CA.
SIM_TDP_N	Trigger Detection Point messages received from call processing in the reporting CA that do not require a response from the target FS.
SIM_TDP_R	Trigger Detection Point messages received from call processing in the reporting CA that do require a response from the target FS.
SIM_TERMINATE_RX	TERMINATE messages received from FSs.
SIM_TERMINATE_TX	TERMINATE messages sent to FSs.

POTS Local FS Measurements

Table 6-8 Local POTS Local Measurements

Measurement	Description (* = rapid count could mean a potential problem in the system)
POTS_CFC_INTERROG_ATTMP	Call Forward Combination interrogation attempts on the reporting FS.
POTS_CFC_DEACT_ATTMP	Call Forward Combination deactivation attempts on the reporting FS.
POTS_CCW_ATTMP	Cancel Call Waiting attempts on the reporting FS.

Table 6-8 Local POTS Local Measurements (continued)

Measurement	Description (* = rapid count could mean a potential problem in the system)
POTS_CCW_LENGTH	Subscriber-seconds that Cancel Call WAITING was active on the reporting FS.
POTS_CCW_REJECT_BY_CCW	Cancel Call Waiting attempts rejected due to Call Waiting not already being active on the reporting FS.
POTS_CCW_REJECT_NO_RSRC	Cancel Call Waiting attempts rejected due to a lack of available resources on the reporting FS.
POTS_CFB_ACT_ATTMP	Call Forward Busy activation attempts on the reporting FS.
POTS_CFB_ACT_REFUSED	Call Forward Busy activation attempts refused on the reporting FS.
POTS_CFB_DEACT_ATTMP	Call Forward Busy deactivation attempts on the reporting FS.
POTS_CFB_FORWARD_FAIL	Call Forward Busy service instances that failed on the reporting FS.
POTS_CFB_FORWARD_SUCC	Call Forward Busy service instances that succeeded on the reporting FS.
POTS_CFB_INTERROG_ATTMP	Call Forward Busy interrogation attempts on the reporting FS.
POTS_CFC_ACT_ATTMP	Call Forward Combination activation attempts on the reporting FS.
POTS_CFC_ACT_FAIL	Unsuccessful Call Forward Combination activation attempts on the reporting FS.
POTS_CFC_ACT_SUCC	Successful Call Forward Combination activation attempts on the reporting FS.
POTS_CFC_DEACT_FAIL	Unsuccessful Call Forward Combination deactivation attempts on the reporting FS.
POTS_CFC_DEACT_SUCC	Successful Call Forward Combination deactivation attempts on the reporting FS.
POTS_CFC_DN_CHG_ACT_ATTMP	Call Forward Combination directory number change activation attempts on the reporting FS.
POTS_CFC_DN_CHG_ACT_FAIL	Unsuccessful Call Forward Combination directory number change activation attempts on the reporting FS.
POTS_CFC_DN_CHG_ACT_SUCC	Successful Call Forward Combination directory number change activation attempts on the reporting FS.
POTS_CFC_FORWARD_ATTMP	Call Forward Combination forwarding attempts on the reporting FS.
POTS_CFC_FORWARD_FAIL	Unsuccessful Call Forward Combination forwarding attempts on the reporting FS.
POTS_CFC_FORWARD_SUCC	Successful Call Forward Combination forwarding attempts on the reporting FS.
POTS_CFC_INTERROG_FAIL	Unsuccessful Call Forward Combination interrogation attempts on the reporting FS.
POTS_CFC_INTERROG_SUCC	Successful Call Forward Combination interrogation attempts on the reporting FS.
POTS_CFNA_ACT_ATTMP	Call Forward No Answer activation attempts on the reporting FS.
POTS_CFNA_ACT_REFUSED	Call Forward No Answer activation attempts refused on the reporting FS.
POTS_CFNA_DEACT_ATTMP	Call Forward No Answer deactivation attempts on the reporting FS.
POTS_CFNA_FORWARD_FAIL	Call Forward No Answer service instances that failed on the reporting FS.
POTS_CFNA_FORWARD_SUCC	Call Forward No Answer service instances that succeeded on the reporting FS.
POTS_CFNA_INTERROG_ATTMP	Call Forward No Answer interrogation attempts on the reporting FS.

Table 6-8 Local POTS Local Measurements (continued)

Measurement	Description (* = rapid count could mean a potential problem in the system)
POTS_CFU_ACT_ANSWERED	Call Forward Unconditional activation attempts answered by the called party on the reporting FS.
POTS_CFU_ACT_ATTMP	Call Forward Unconditional activation attempts on the reporting FS.
POTS_CFU_ACT_REFUSED	Call Forward Unconditional activation attempts refused on the reporting FS.
POTS_CFU_ACT_SECOND	Call Forward Unconditional second activation attempts on the reporting FS.
POTS_CFU_DEACT_ATTMP	Call Forward Unconditional deactivation attempts on the reporting FS.
POTS_CFU_FORWARD_FAIL	Call Forward Unconditional service instances that failed on the reporting FS.
POTS_CFU_FORWARD_SUCC	Call Forward Unconditional service instances that succeeded on the reporting FS.
POTS_CFU_INTERROG_ATTMP	Call Forward Unconditional interrogation attempts on the reporting FS.
POTS_CHD_ANSWER	Call Hold service instance attempts resulting in reconnection on the reporting FS.
POTS_CHD_ATTMP	Call Hold service instance attempts on the reporting FS.
POTS_CHD_NOT_ANSWER	Call Hold service instance attempts not reconnected on the reporting FS.
POTS_CHD_REJECT_INTERACT	Call Hold service instance attempts rejected due to feature interactions on the reporting FS.
POTS_CHD_REJECT_NO_RSRC	Call Hold service instance attempts rejected due to a lack of available resources on the reporting FS.
POTS_CIDS_ATTMP	Calling Identity Delivery attempts made on the reporting FS.
POTS_CIDSS_ATTMP	Calling Identity Delivery Suppression attempts made on the reporting FS.
POTS_CNAB_ATTMP	Calling Name Delivery Blocking attempts made on the reporting FS.
POTS_CNDB_ATTMP	Calling Number Delivery Blocking attempts made on the reporting FS.
POTS_CPRK_CLEAR	Call Park Attempts to clear during the collection interval
POTS_CPRK_FAIL_ATTMP	Call Park Attempts that failed during the collection interval
POTS_CPRK_FAIL_RET_ATTMP	Call Park Retrieval Attempts that failed during the collection interval
POTS_CPRK_FORWARD	Call Park Attempts to forward a call during the collection interval
POTS_CPRK_SUCC_ATTMP	Call Park Attempts successful during the collection interval
POTS_CPRK_SUCC_RET_ATTMP	Call Park Retrieval Attempts successful during the collection interval
POTS_CT_ANSWER	Call Transfer service instance attempts answered by the called party on the reporting FS.
POTS_CT_ATTMP	Call Transfer service instance attempts on the reporting FS.
POTS_CT_CONF	Call Transfer service instance attempts resulting in a successfully setup conference call on the reporting FS.
POTS_CT_FAIL	Call Transfer service instance attempts that failed on the reporting FS.
POTS_CT_TRANSFER	Call Transfer service instance attempts resulting in a successfully transferred call on the reporting FS.
POTS_CW_ANSWERED	Call Waiting service instance attempts answered by the called party on the reporting FS.

Table 6-8 Local POTS Local Measurements (continued)

Measurement	Description (* = rapid count could mean a potential problem in the system)
POTS_CW_ATTMP	Call Waiting service instance attempts on the reporting FS.
POTS_CW_NOT_ANSWERED	Call Waiting service instance attempts not answered by the called party on the reporting FS.
POTS_CW_REJECT_NO_RSRC	Call Waiting service instance attempts rejected due to a lack of available resources on the reporting FS.
POTS_CW_REJECTE_INTERACT	Call Waiting service instance attempts rejected due to feature interactions on the reporting FS.
POTS_CWD_ACT_FAIL	Call Waiting Deluxe unsuccessful service activation attempts on the reporting FS.
POTS_CWD_ACT_SUCC	Call Waiting Deluxe successful service activation attempts on the reporting FS.
POTS_CWD_ANSWER	Call Waiting Deluxe service instance attempts answered by the called party on the reporting FS.
POTS_CWD_ATTMP	Call Waiting Deluxe service instance attempts on the reporting FS.
POTS_CWD_DEACT_FAIL	Call Waiting Deluxe unsuccessful service deactivation attempts on the reporting FS.
POTS_CWD_DEACT_SUCC	Call Waiting Deluxe successful service deactivation attempts on the reporting FS.
POTS_CWD_INTERROG_FAIL	Call Waiting Deluxe unsuccessful service interrogation attempts on the reporting FS.
POTS_CWD_INTERROG_SUCC	Call Waiting Deluxe successful service interrogation attempts on the reporting FS.
POTS_DND_ACT_FAIL	Do Not Disturb deactivation attempts during the collection interval
POTS_DND_ACT_SUCC	Do Not Disturb activation attempts during the collection interval
POTS_DND_DEACT_FAIL	Do Not Disturb deactivation attempts during the collection interval
POTS_DND_DEACT_SUCC	Do Not Disturb activation attempts that failed due to a lack of resources during the collection interval
POTS_DND_REJECT	Do Not Disturb activation attempts successful during the collection interval
POTS_DRCW_ATTMP	Distinctive Ring Call Waiting service instance attempts on the reporting FS.
POTS_DRCW_REJECT_NO_RSRC	Distinctive Ring Call Waiting attempts rejected due to a lack of available resources on the reporting FS.
POTS_DRCW_SUCC	Distinctive Ring Call Waiting attempts successful on the reporting FS.
POTS_ECB_CALL_ATTEMPT	Calls originated from PSAP line to a subscriber.
POTS_EXT_CNAM_FAIL_APP	CNAM translation queries that resulted in a failed external query to a network database due to an application failure from the reporting FS.
POTS_EXT_CNAM_FAIL_NETW	CNAM translation queries that resulted in a failed external query to a network communication failure from the reporting FS.
POTS_EXT_CNAM_FAIL_NETW	CNAM translation queries that resulted in a failed external query to a network communication failure from the reporting FS.

Table 6-8 Local POTS Local Measurements (continued)

Measurement	Description (* = rapid count could mean a potential problem in the system)
POTS_EXT_CNAM_QUERY	CNAM translation queries that resulted in an external query to a network database attempted on the reporting FS.
POTS_EXT_CNAM_QUERY_SUCC	CNAM translation queries that resulted in a successful external query to a network database attempted on the reporting FS.
POTS_MDC_ATTMP	Mid Call Trigger attempts made by subscribers on the reporting FS.
POTS_MDC_REJECT_INTERACT	Mid Call Trigger attempts made by subscribers rejected due to feature interactions on the reporting FS.
POTS_MDC_REJECT_NO_RSRC	Mid Call Trigger attempts made by subscribers rejected due to a lack of available resources on the reporting FS.
POTS_MDC_REJECT_OTHERS	Mid Call Trigger attempts made by subscribers rejected due to unknown reasons on the reporting FS.
POTS_NSA_INVOKE_ABANDON	No Solicitation Announcement invocations detected on the reporting FS abandoned after the NSA announcement started but before the terminating endpoint began ringing
POTS_NSA_INVOKE_FAIL	No Solicitation Announcement unsuccessful invocations detected on the reporting FS.
POTS_NSA_INVOKE_SUCC	No Solicitation Announcement successful invocations detected on the reporting FS.
POTS_OCB_ACT_SUCC	Outward Call Barring successful activation attempts on the reporting FS.
POTS_OCB_DEACT_SUCC	Outward Call Barring successful deactivation attempts on the reporting FS.
POTS_OCB_INTERROG_SUCC	Outward Call Barring successful interrogation attempts on the reporting FS.
POTS_OCB_INTL_BLOCK	international calls blocked on the reporting FS via Outward Call Barring
POTS_OCB_INVALID_PASSWORD	Outward Call Barring attempts unsuccessful due to invalid password entry by the user on the reporting FS.
POTS_OCB_INVOCATION	Outward Call Barring invocation attempts on the reporting FS.
POTS_OCB_LOCAL_BLOCK	local calls blocked on the reporting FS via Outward Call Barring
POTS_OCB_NATL_BLOCK	national calls blocked on the reporting FS via Outward Call Barring
POTS_RACF_ATTMP	Remote Activation Call Forward attempts on the reporting FS.
POTS_RACF_CFU_ACT	Remote Activation Call Forward activation attempts successful on the reporting FS.
POTS_RACF_CFU_DEACT	Remote Activation Call Forward deactivation attempts successful on the reporting FS.
POTS_RACF_CFU_UNCHANGED	Remote Activation Call Forward service instances successful but resulted in no change to the forwarding-to number on the reporting FS.
POTS_RACF_PIN_ATTMP	Remote Activation Call Forward PIN input attempts on the reporting FS.
POTS_RACF_PIN_CHANGE	Remote Activation Call Forward PIN input attempts that resulted in a change to the previous PIN for that subscriber on the reporting FS.
POTS_RACF_PIN_REFUSE	Remote Activation Call Forward PIN input attempts refused on the reporting FS.

Table 6-8 Local POTS Local Measurements (continued)

Measurement	Description (* = rapid count could mean a potential problem in the system)
POTS_RACF_PIN_REJECT_NO_RSRC	Remote Activation Call Forward PIN input attempts refused due to a lack of resources on the reporting FS.
POTS_RACF_PIN_UNCHANGE	Remote Activation Call Forward PIN input attempts that resulted in no change to the previous PIN for that subscriber on the reporting FS.
POTS_RACF_REFUSE	Remote Activation Call Forward service instances refused by the reporting FS.
POTS_RACF_REJECT_NO_RSRC	Remote Activation Call Forward service instances refused due to a lack of available resources on the reporting FS.
POTS_RC_SUCC	Return Call attempts successful during the collection interval
POTS_REFERER_ATTMP	REFER attempts made on the reporting FS.
POTS_REFERER_FAIL	REFER failed attempts made on the reporting FS.
POTS_REFERER_SUCC	REFER successful attempts made on the reporting FS.
POTS_SC_1_DIGIT_ATTMP	Speed Call 1 digit attempts during the collection interval
POTS_SC_2_DIGIT_ATTMP	Speed Call 2 digit attempts during the collection interval
POTS_SC_SUCC_CCSC	CCSC successful attempts during the collection interval
POTS_SEASONAL_SUSPEND_CALLS_OUTG_BLOCKED	Calls blocked based on seasonal suspend status of the subscriber. Note This does not apply to Centrex, MLHG, or PBX-based subscribers.
POTS_TOTAL_CNAM_QUERY	CNAM translation queries attempted on the reporting FS.
POTS_TWC_ANSWERED	Three Way Call service instance attempts answered by the called party on the reporting FS.
POTS_TWC_ATTMP	Three Way Call service instance attempts on the reporting FS.
POTS_TWC_CONF	Three Way Call service instance attempts resulting in a successfully setup conference call on the reporting FS.
POTS_TWC_FAIL	Three Way Call service instance attempts that failed on the reporting FS.
POTS_TWCD_ATTMP	Three Way Calling Deluxe service instance attempts on the reporting FS. Incremented when a subscriber in a stable two-way call presses flash button followed by DN of a third party
POTS_TWCD_CONF	Three Way Calling Deluxe service instance conferencing attempts on the reporting FS. Incremented when a subscriber attempts to bridge all three parties (flash button followed by digit 3)

POTS Application Server Measurements

Table 6-9 POTS Application Server Measurements

Measurement	Description (* = rapid count could mean a potential problem in the system)
POTS_AS_ORIG_ABANDON	Times a origination to the Application Server was abandoned while trying to connect.
POTS_AS_ORIG_ATTMP	attempts to place a call to an Application Server on the originating side.
POTS_AS_ORIG_FAIL	Unsuccessfully placed calls to an Application Server on the originating side.
POTS_AS_ORIG_SUCC	Successfully placed calls to an Application Server on the originating side.
POTS_AS_TERM_ABANDON	Times a termination to the Application Server was abandoned while trying to connect.
POTS_AS_TERM_ATTMP	attempts to place a call to an Application Server on the terminating side.
POTS_AS_TERM_FAIL	unsuccessfully placed calls to an Application Server on the terminating side.
POTS_AS_TERM_SUCC	Successfully placed calls to an Application Server on the terminating side.
POTS_AS_VSC_ABANDON	Times a VSC initiated connection to the Application Server was abandoned while trying to connect.
POTS_AS_VSC_ATTMP	attempts to place a call to an Application Server using the VSC code
POTS_AS_VSC_FAIL	Failed call attempts on an Application Server. This includes abandon calls as well.
POTS_AS_VSC_SUCC	Successfully placed call attempts on an Application Server.
POTS_CFC_REDIRECT_SUCC	This increases when BTS uses redirection mechanism to perform CFC-No-Answer feature.
POTS_CFNA_REDIRECT_SUCC	This increases when BTS uses redirection mechanism to perform CFNA feature.
POTS_CFR_FORWARD_ATTMP	This increases when BTS receives SIP 302 and POTS-FS initiates the CFR processing.
POTS_CFR_FORWARD_FAIL	This increases when BTS receives SIP 302 and POTS-FS fails to forward the call to new destination.
POTS_CFR_FORWARD_SUCC	This increases when BTS receives SIP 302 and POTS-FS forwards the call to new destination successfully.
POTS_OC_DP_RECEIVED	DPs (Detection Points) reported by the FS during periods of congestion.
POTS_VM_REDIRECT_SUCC	This increases when BTS uses redirection mechanism to perform VW-No-Answer feature.

POTS Miscellaneous FS Measurements

Table 6-10 Miscellaneous POTS Measurements

Measurement	Description (* = rapid count could mean a potential problem in the system)
POTS_BLV_ATTMP	Busy Line Verification service instance attempts on the reporting FS.
POTS_CTX_SFG_OVERFLOW	Centrex SFG measurements that overflowed during the collection interval on the reporting FS.
POTS_HOTLINE_ATTMP	Hotline service instance attempts on the reporting FS.
POTS_HOTV_ACT_SUCC	Successful Hotline Variable activation attempts on the reporting FS.

Table 6-10 Miscellaneous POTS Measurements (continued)

Measurement	Description (* = rapid count could mean a potential problem in the system)
POTS_HOTV_ATTMP	Successful Hotline Variable instance attempts on the reporting FS.
POTS_HOTV_DEACT_SUCC	Successful Hotline Variable deactivation attempts on the reporting FS.
POTS_HOTV_INTERROG_SUCC	Successful Hotline Variable interrogation attempts on the reporting FS.
POTS_LCD_AUTH_ATTMP	Authorization attempts made for Limited Call Duration feature invocations on the reporting FS.
POTS_LCD_AUTH_FAIL	Unsuccessful authorization attempts made for Limited Call Duration feature invocations on the reporting FS.
POTS_LCD_AUTH_SUCC	Successful authorization attempts made for Limited Call Duration feature invocations on the reporting FS.
POTS_LCD_FORCED_DISC	forced call disconnections made for Limited Call Duration calls on the reporting FS.
POTS_LCD_REAUTH_FAIL	Unsuccessful re-authorization attempts made for Limited Call Duration feature invocations on the reporting FS.
POTS_MLS_ATTMP	Attempts on the reporting FS to change the language of choice by the user.
POTS_MLS_REJECT_NO_RSRC	Language change attempts refused due to a lack of available resources on the reporting FS. The most likely cause of this situation is a lack of resources on the FS to handle the IVR activity. This is normally a result of database access issues.
POTS_MLS_SUCC	Language change attempts there were successfully processed by the reporting FS. This is indicative of successful termination of the IVR when the user successfully changes their language choice, selects a language choice, or refuses to confirm a new choice.
POTS_OC_EDP_RECEIVED	EDP triggers received by a FS during periods of congestion.
POTS_OP_INTERRUPT_ATTMP	Operator Interrupt service instance attempts on the reporting FS.
POTS_PS_FAIL	Privacy Screening Invocations failures detected on the reporting FS. This is indicative of the external application server not answering the call or the trunk between the app server and the BTS is out of service.
POTS_PS_MANAGE_FAIL	Unsuccessful Managed Privacy Screening Activations/Deactivations detected on the reporting FS. This is indicative of the external application server not answering the call or the trunk between the app server and the BTS is out of service for PS Manage feature invocations.
POTS_PS_MANAGE_SUCC	Successful Managed Privacy Screening Activations/Deactivations detected on the reporting FS. This is indicative of the external application server having answered the call and sent a 200 OK to the BTS for PS Manage feature invocations.
POTS_PS_SUCC	Privacy Screening Invocations detected on the reporting FS. This is indicative of the external application server having answered the call and sent a 200 OK to the BTS.
POTS_VM_ACCESS	Voice Mail Redirect Accesses detected on the reporting FS.
POTS_VM_ACT_FAIL	Unsuccessful Voice Mail Redirect Activations detected on the reporting FS.
POTS_VM_ACT_SUCC	Successful Voice Mail Redirect Activations detected on the reporting FS.
POTS_VM_ATTMP	Voice Mail Redirect Invocations detected on the reporting FS.
POTS_VM_DEACT_FAIL	Unsuccessful Voice Mail Redirect Deactivations detected on the reporting FS.
POTS_VM_DEACT_SUCC	Successful Voice Mail Redirect Deactivations detected on the reporting FS.
POTS_WARMLINE_ATTMP	Warmline service instance attempts on the reporting FS.

POTS Class of Service FS Measurements

Table 6-11 POTS Class of Service Measurements

Measurement	Description (* = rapid count could mean a potential problem in the system)
POTS_COS_900_BLOCKED	Calls denied due to subscriber based 900 restrictions on the reporting FS.
POTS_COS_976_BLOCKED	Calls denied due to subscriber based 976 restrictions on the reporting FS.
POTS_COS_ACCT_CODE_FAIL	Not currently used.
POTS_COS_ACCT_CODE_SUCC	Successful account code validations on the reporting FS. Account codes do not get validated - any dialed account code entered by the user is considered valid - including an empty account code.
POTS_COS_ANI_ATTMP_SUCC	Automatic Number ID directory number lookups successfully attempted on the reporting FS. An ANI attempt is successful when the ANI DN is available on the reporting FS, and ANI status is allowed as per provisioning. In the case of casual calls, ALL ANI attempts are successful if the Casual Code is valid and allowed on reporting FS.
POTS_COS_ANI_BLOCKED_CALL	Calls blocked based on Automatic Number ID directory number lookups on the reporting FS. In the case of Casual calls, ANI does also get blocked if Casual Codes are invalid.
POTS_COS_AUTH_CODE_FAIL	Unsuccessful authentication code validations on the reporting FS.
POTS_COS_AUTH_CODE_SUCC	Successful authentication code validations on the reporting FS.
POTS_COS_CASUAL_RESTRICT	Calls denied due to subscriber based casual dialing restrictions on the reporting FS.
POTS_COS_DA_BLOCKED	calls denied due to subscriber based directory assistance restrictions on the reporting FS.
POTS_COS_INTL_BLOCKED_BW	International based calls blocked due to a match on a black list or an exclusion from a white list on the reporting FS.
POTS_COS_INTL_OP_BLOCKED	Calls denied due to subscriber based international operator restrictions on the reporting FS.
POTS_COS_INTL_RESTRICT	Not currently used.
POTS_COS_NANP_BLOCKED_BW	NANP based calls blocked due to a match on a black list or an exclusion from a white list on the reporting FS.
POTS_COS_NANP_OP_BLOCKED	Calls denied due to subscriber based NANP operator restrictions on the reporting FS.
POTS_COS_NANP_RESTRICT	Calls denied due to subscriber based NANP restrictions on the reporting FS.
POTS_COS_TOLLFREE_BLOCKED	Calls screened based on class of service restrictions on making toll free calls.
POTS_COS_TOT_ACCT_IVR_SESS ION	Class of Service Account Code IVR sessions established on the reporting FS.
POTS_COS_TOT_AUTH_IVR_SESS ION	Class of Service Authorization Code IVR sessions established on the reporting FS.
POTS_COS_TOT_IVR_FAIL	Class of Service IVR sessions that Failed to established due to an IVR related failure on the reporting FS.
POTS_TDISC_CALLS_OUTG_BLO CKED	Calls blocked because the subscriber is temporarily disconnected. This applies to POTS, Centrex, MLHG, and PBX based subscribers.

POTS Screen List Editing FS Measurements

Table 6-12 POTS Screen List Editing Measurements

Measurement	Description (* = rapid count could mean a potential problem in the system)
POTS_SCA_ATTMP	Selective Call Acceptance service instance attempts on the reporting FS.
POTS_SCA_REJECT_NO_RSRC	Selective Call Acceptance attempts made by subscribers rejected due to a lack of available resources on the reporting FS.
POTS_SCA_SUCC	Selective Call Acceptance service instance attempts resulting in successful acceptance of the call on the reporting FS.
POTS_SCF_ATTMP	Selective Call Forwarding service instance attempts on the reporting FS.
POTS_SCF_REJECT_NO_RSRC	Selective Call Forwarding attempts rejected due to a lack of available resources on the reporting FS.
POTS_SCF_SUCC	Selective Call Forwarding attempts successful on the reporting FS.
POTS_SCR_ATTMP	Selective Call Rejection service instance attempts on the reporting FS.
POTS_SCR_REJECT_NO_RSRC	Selective Call Rejection attempts made by subscribers rejected due to a lack of available resources on the reporting FS.
POTS_SCR_SUCC	Selective Call Rejection service instance attempts resulting in successful rejections of the call on the reporting FS.

POTS Customer Originated Trace FS Measurements

Table 6-13 POTS Customer Originated Trace Measurements

Measurement	Description (* = rapid count could mean a potential problem in the system)
POTS_COT_ABAND	Caller Originated Trace service activation abandonments that occurred on the reporting FS.
POTS_COT_ACCESS	Times the Caller Originated Trace star code was dialed by the subscriber (feature accesses and activations)
POTS_COT_ACT	Same as POTS_COT_ACCESS in this release. When 2-level COT (the digit "1" dialed) is available - this is both those and the current 1-level activations tracked in POTS_COT_ACCESS.
POTS_COT_DENY	Times the Caller Originated Trace data was unsuccessfully accessed on the reporting FS.
POTS_COT_DN_UNAVAIL	Caller Originated Trace service activation that failed due to the calling party directory number not be available on the reporting FS.
POTS_COT_TRACE_CONFIRM	Caller Originated Trace service instances successfully completed on the reporting FS.
POTS_COT_TRACE_OUTPUT	Caller Originated Trace service instances successfully completed and the data was stored persistently on the reporting FS.

POTS Automatic Callback, Recall, and Call Return Measurements

Table 6-14 POTS Automatic Callback, Recall, and Call Return Measurements

Measurement	Description (* = rapid count could mean a potential problem in the system)
POTS_AC_ACT_ATTMP	Automatic Callback service activation attempts on the reporting FS.
POTS_AC_DEACT_ATTMP	Automatic Callback service activation attempts deactivated by the requesting subscriber on the reporting FS.
POTS_AC_DEACT_BY_SYSTEM	Automatic Callback service activation attempts deactivated by the system on the reporting FS.
POTS_AC_DELAYED_PROC	Automatic Callback service activation attempts that resulted in delayed connection on the reporting FS.
POTS_AC_IMMEDIATE_PROC	Automatic Callback service activation attempts that resulted in immediate connection on the reporting FS.
POTS_AC_INTERLATA_ATTMP	Automatic Callback service activation attempts performed on an interlata basis on the reporting FS.
POTS_AC_OVERFLOW	Automatic Callback service activation attempts resulting in an overflow on the reporting FS.
POTS_ACART_ORIG_SCAN_REQ	Automatic Callback and Automatic Recall service requests queued for originators on the reporting FS.
POTS_ACART_QUEUED_REQ	Automatic Callback and Automatic Recall service requests queued on the reporting FS.
POTS_ACART_REJECT_NO_RSRC	Automatic Callback and Automatic Recall service requests rejected due to a lack of resources on the reporting FS.
POTS_ACART_TERM_SCAN_REQ	Automatic Callback and Automatic Recall service requests queued for terminators on the reporting FS.
POTS_ACR_ACT_ATTMP	Anonymous Call Rejection activation attempts during the collection interval
POTS_ACR_ACT_REJECT_NO_RSRC	Anonymous Call Rejection activation attempts that failed due to a lack of resources during the collection interval
POTS_ACR_DEACT_REJECT_NO_RSRC	Anonymous Call Rejection deactivation attempts during the collection interval
POTS_ACR_DEACT_ATTMP	Anonymous Call Rejection deactivation attempts during the collection interval
POTS_ACR_SUCC	Anonymous Call Rejection attempts successful during the collection interval
POTS_AR_2LEVEL_ACC_CODE_ATT MP	Automatic Callback service activation attempts on the reporting FS.
POTS_AR_2LEVEL_ACT_CODE_ATT MP	Times the activation code (*69) is dialed for the two level Automatic Recall activation procedure on the reporting FS.
POTS_AR_ACT_ATTMP	Automatic Recall service activation attempts on the reporting FS.
POTS_AR_DEACT_ATTMP	Automatic Recall service activation attempts deactivated by the requesting subscriber on the reporting FS.
POTS_AR_DEACT_BY_SYSTEM	Automatic Recall service activation attempts deactivated by the system on the reporting FS.

Table 6-14 POTS Automatic Callback, Recall, and Call Return Measurements (continued)

Measurement	Description (* = rapid count could mean a potential problem in the system)
POTS_AR_DELAYED_PROC	Automatic Recall service activation attempts that resulted in delayed connection on the reporting FS.
POTS_AR_IMMEDIATE_PROC	Automatic Recall service activation attempts that resulted in immediate connection on the reporting FS.
POTS_AR_INTERLATA_ATTMP	Automatic Recall service activation attempts performed on an interlata basis on the reporting FS.
POTS_AR_OVERFLOW	Automatic Recall service activation attempts resulting in an overflow on the reporting FS.

POTS Limited Call Duration (Prepaid/Postpaid) with RADIUS Interface to AAA Measurements

Table 6-15 POTS Limited Call Duration (Prepaid/Postpaid) with RADIUS Interface to AAA

Measurement	Description (* = rapid count could mean a potential problem in the system)
POTS_LCD_AUTH_ATTMP	authorization attempts made for Limited Call Duration feature invocations on the reporting FS. Note For three-leg calls, each call is authorized separately.
POTS_LCD_AUTH_FAIL	Unsuccessful authorization attempts made for Limited Call Duration feature invocations on the reporting FS.
POTS_LCD_AUTH_SUCC	Successful authorization attempts made for Limited Call Duration feature invocations on the reporting FS.
POTS_LCD_FORCED_DISC	forced call disconnections made for Limited Call Duration calls on the reporting FS.
POTS_LCD_REAUTH_FAIL	Unsuccessful reauthorization attempts made for Limited Call Duration feature invocations on the reporting FS.

POTS Call Forwarding Combination Measurements

Table 6-16 POTS Call Forwarding Combination Measurements

Measurement	Description (* = rapid count could mean a potential problem in the system)
POTS_CFC_ACT_ATTMP	CFC Activation Attempt
POTS_CFC_ACT_FAIL	CFC Activation Failure
POTS_CFC_ACT_SUCC	CFC Activation Successful
POTS_CFC_DEACT_ATTMP	CFC Deactivation Attempt
POTS_CFC_DEACT_FAIL	CFC Deactivation Failure
POTS_CFC_DEACT_SUCC:	CFC Deactivation Successful
POTS_CFC_DN_CHG_ACT_ATTMP	CFC DN Change Activation Attempt
POTS_CFC_DN_CHG_ACT_FAIL	CFC DN change Activation Failure
POTS_CFC_DN_CHG_ACT_SUCC	CFC DN change Activation Successful
POTS_CFC_FORWARD_FAIL	CFC Invocation Failure
POTS_CFC_FORWARD_SUCC	CFC Invocation Successful
POTS_CFC_INTERROG_ATTMP	CFC Interrogation Attempt
POTS_CFC_INTERROG_FAIL	CFC Interrogation Failure
POTS_CFC_INTERROG_SUCC	CFC Interrogation Success

AIN Services FS Measurements

Table 6-17 AIN Services Measurements

Measurement	Description (* = rapid count could mean a potential problem in the system)
AINSCV_LOC_LNP_FAIL_APP	Failures in querying the local LNP database.
AINSCV_LOC_LNP_QUERY	DN look ups in local LNP database.
AINSCV_LOC_LNP_QUERY_RN_FOUND	Successful queries to the local LNP database that returned an RN corresponding to the DN.
AINSCV_LOC_LNP_QUERY_SUCC	Successful queries to the local LNP database.
AINSVC_8XX_QUERY	8XX translation queries attempted on the reporting FS.
AINSVC_EXT_8XX_FAIL_APP	8XX translation queries that resulted in a failed external query to a network database due to an application failure from the reporting FS.
AINSVC_EXT_8XX_FAIL_NETW	8XX translation queries that resulted in a failed external query to a network database due to a network communication failure from the reporting FS.
AINSVC_EXT_8XX_QUERY	8XX translation queries that resulted in an external query to a network database attempted on the reporting FS.
AINSVC_EXT_8XX_QUERY_FAIL	8XX queries that failed due to an SCP timeout when attempted by the reporting FS.
AINSVC_EXT_8XX_QUERY_SUCC	8XX translation queries that resulted in a successful external query to a network database attempted on the reporting FS.
AINSVC_EXT_LNP_FAIL_APP	LNP translation queries that resulted in a failed external query to a network database due to an application failure from the reporting FS.
AINSVC_EXT_LNP_FAIL_NETW	LNP translation queries that resulted in a failed external query to a network database due to a network communication failure from the reporting FS.
AINSVC_EXT_LNP_QUERY	LNP translation queries that resulted in an external query to a network database attempted on the reporting FS.
AINSVC_EXT_LNP_QUERY_FAIL	LNP queries that failed due to an SCP timeout when attempted by the reporting FS.
AINSVC_EXT_LNP_QUERY_LRN	LNP queries that resulted in a successful response from the SCP with an LRN when attempted by the reporting FS.
AINSVC_EXT_LNP_QUERY_SUCC	LNP translation queries that resulted in a successful external query to a network database attempted on the reporting FS.
AINSVC_LNP_CALLS_WITH_CAUSE_26	Calls ending in an ISUP REL with cause code of 26 reported by the FS.
AINSVC_LNP_DATA_INCONSISTENT	Calls ending in an unallocated/vacant number indication when the CMS's own LRN has been detected after an LNP query in the donor switch, or in another switch as indicated by the Ported Number Translation indicator in the FCI parameter with no "Ported Number" GAP. This case does not apply to DNs marked as "LNP-Reserved".
AINSVC_LNP_QUERY_WITH_LRN	LNP query responses containing an LRN (not the dialed number) reported by the FS.
AINSVC_LNP_UNALLOC_NUM_CALL	Calls ending in an unallocated/vacant number indication in the donor switch, or another switch as indicated by the Ported Number Translation indicator in the FCI parameter with no "Ported Number" GAP.

Table 6-17 AIN Services Measurements (continued)

Measurement	Description (* = rapid count could mean a potential problem in the system)
AINSVC_LOC_8XX_ANI_BLOCK	8XX translation queries blocked due to ANI screening processed locally on the reporting FS.
AINSVC_LOC_8XX_DNIS_SUCC	8XX DNIS translation queries successfully processed locally on the reporting FS.
AINSVC_LOC_8XX_FAIL_APP	8XX translation queries that resulted in a failure due to an application error on the reporting FS.
AINSVC_LOC_8XX_II_BLOCK	8XX translation queries blocked due to II screening processed locally on the reporting FS.
AINSVC_LOC_8XX_QUERY	8XX translation queries attempted to be processed locally on the reporting FS.
AINSVC_LOC_8XX_QUERY_SUCC	8XX translation queries successfully processed locally on the reporting FS.
AINSVC_LOC_8XX_REROUTE	8XX translation queries successfully processed locally on the reporting FS that resulted in re-routing.
AINSVC_LOC_8XX_ROUTING_SUCC	8XX routing translation queries successfully processed locally on the reporting FS.
AINSVC_LOC_LNP_FAIL_APP	Failed attempts to look up a DN in the local LNP database by the reporting FS.
AINSVC_LOC_LNP_QUERY	DN look ups in the local LNP database by the reporting FS.
AINSVC_LOC_LNP_QUERY_NO_RN	Successful attempts to look up a DN in the local LNP database by the reporting FS that did not return a corresponding RN.
AINSVC_LOC_LNP_QUERY_RN_FOUND	Successful attempts to look up a DN in the local LNP database by the reporting FS that returned a corresponding RN.
AINSVC_LOC_LNP_QUERY_SUCC	Successful attempts to look up a DN in the local LNP database by the reporting FS.
AINSVC_TOTAL_LNP_QUERY	LNP translation queries attempted on the reporting FS.
AINSVC_TOTAL_QUERY	Queries attempted on the reporting FS.

SCCP Protocol Measurements

Table 6-18 *SCCP Measurements*

Measurement	Description (* = rapid count could mean a potential problem in the system)
SCCP_NSAP_OOS_GRANT_TX	Subsystem out-of-service grant messages sent on the reporting FS.
SCCP_NSAP_OOS_REQ_TX	Subsystem out-of-service request messages sent on the reporting FS.
SCCP_NSAP_PROHIBIT_TX	Subsystem prohibited messages sent on the reporting FS.
SCCP_NSAP_STAT_TEST_TX	Subsystem status test messages sent on the reporting FS.
SCCP_HOP_measurement_FAIL	Routing errors due to a hop measurement violation on the reporting FS.
SCCP_MSG_TX_BACKUP_SUBSYS	Messages sent to a backup subsystem on the reporting FS.
SCCP_NETWORK_CONGEST_FAIL	Routing errors due to network congestion on the reporting FS.
SCCP_NETWORK_FAIL	Routing errors due to a network failure from the point code being unavailable on the reporting FS.
SCCP_NO_TRANS_ADDR_FAIL	Routing errors due to no translation for address of such nature on the reporting FS.
SCCP_NO_TRANS_SPEC_ADDR_FAIL	Routing errors due to no translation for this specific address on the reporting FS.
SCCP_NSAP_ALLOW_MSG_RX	Subsystem allowed messages received on the reporting FS.
SCCP_NSAP_ALLOW_MSG_TX	Subsystem allowed messages sent on the reporting FS.
SCCP_NSAP_CONGEST_RX	Subsystem congested messages received on the reporting FS.
SCCP_NSAP_CONGEST_TX	Subsystem congested messages sent on the reporting FS.
SCCP_NSAP_OOS_GRANT_RX	Subsystem out-of-service grant messages received on the reporting FS.
SCCP_NSAP_OOS_REQ_RX	Subsystem out-of-service request messages received on the reporting FS.
SCCP_NSAP_PROHIBIT_RX	Subsystem prohibited messages received on the reporting FS.
SCCP_NSAP_STAT_TEST_RX	Subsystem status test messages received on the reporting FS.
SCCP_SUBSYS_CONGEST_FAIL	Routing errors due to subsystem congestion on the reporting FS.
SCCP_SUBSYS_FAIL	Routing errors due to a subsystem failure on the reporting FS.
SCCP_SUBSYS_OOS_REQ_DENY	Subsystem out-of-service requests denied on the reporting FS.
SCCP_SUBSYS_OOS_REQ_GRANT	Subsystem out-of-service requests granted on the reporting FS.
SCCP_SYNTAX_ERR	Syntax errors on the reporting FS.
SCCP_TOTAL_CLASS_0_RX	Class 0 messages received on the reporting FS.
SCCP_TOTAL_CLASS_0_TX	Class 0 messages sent on the reporting FS.
SCCP_TOTAL_CLASS_1_RX	Class 1 messages received on the reporting FS.
SCCP_TOTAL_CLASS_1_TX	Class 1 messages sent on the reporting FS.
SCCP_TOTAL_EXT_UDATA_RX	Extended unit data received on the reporting FS.
SCCP_TOTAL_EXT_UDATA_SVC_RX	Extended unit data service received on the reporting FS.
SCCP_TOTAL_EXT_UDATA_SVC_TX	Extended unit data service sent on the reporting FS.
SCCP_TOTAL_EXT_UDATA_TX	Extended unit data sent on the reporting FS.
SCCP_TOTAL_GLOBAL_ADDR_TRAN	Messages requiring global address translation on the reporting FS.

Table 6-18 SCCP Measurements (continued)

Measurement	Description (* = rapid count could mean a potential problem in the system)
SCCP_TOTAL_LOCAL_MSG	Messages intended for local subsystems on the reporting FS.
SCCP_TOTAL_LONG_UDATA_RX	Long unit data received on the reporting FS.
SCCP_TOTAL_LONG_UDATA_SVC_RX	Long unit data service received on the reporting FS.
SCCP_TOTAL_LONG_UDATA_SVC_TX	Long unit data service sent on the reporting FS.
SCCP_TOTAL_LONG_UDATA_TX	Long unit data sent on the reporting FS.
SCCP_TOTAL_MSG	Messages handled on the reporting FS.
SCCP_TOTAL_UDATA_RX	Unit data received on the reporting FS.
SCCP_TOTAL_UDATA_SVC_RX	Unit data service received on the reporting FS.
SCCP_TOTAL_UDATA_SVC_TX	Unit data service sent on the reporting FS.
SCCP_TOTAL_UDATA_TX	Unit data sent on the reporting FS.
SCCP_UNEQUIP_USER_FAIL	Routing errors due to an unequipped user on the reporting FS.
SCCP_UNKNOWN_FAIL	Routing errors due to an unknown reason on the reporting FS.
SCCP_USAP_TOTAL_CLASS_0_RX	Class 0 messages received on the reporting FS.
SCCP_USAP_TOTAL_CLASS_0_TX	Class 0 messages sent on the reporting FS.
SCCP_USAP_TOTAL_CLASS_1_RX	Class 1 messages received on the reporting FS.
SCCP_USAP_TOTAL_CLASS_1_TX	Class 1 messages sent on the reporting FS.

TCAP Protocol Measurements

Table 6-19 TCAP Measurements

Measurement	Description (* = rapid count could mean a potential problem in the system)
TCAP_INCORRECT_COMP_ENCODE_TX	Incorrect component encoding errors sent by the reporting FS.
TCAP_INVOKE_RSCR_LIMIT_PROB_TX	Resource limitation invoke problems sent by the reporting FS.
TCAP_TRANS_PORT_PERM_REL_TX	Transaction portion permission to release problems sent by the reporting FS.
TCAP_ABORT_IND_RX	Abort indication messages received on the reporting FS.
TCAP_ABORT_MSG_RX	Abort messages received on the reporting FS.
TCAP_ABORT_MSG_TX	Abort messages sent by the reporting FS.
TCAP_ACT_INVOCATIONS	Active invocations on the reporting FS.
TCAP_ACT_TRANSACTIONS	Active transactions on the reporting FS.
TCAP_BAD_STRUCT_COMP_PORT_RX	Badly-structured component portions received on the reporting FS.
TCAP_BAD_STRUCT_COMP_PORT_TX	Badly-structured component portions sent by the reporting FS.
TCAP_BAD_STRUCT_DIALOG_PORT_RX	Badly-structured dialog portions received on the reporting FS.
TCAP_BAD_STRUCT_DIALOG_PORT_TX	Badly-structured dialog portions sent by the reporting FS.
TCAP_BAD_STRUCT_TRANS_PORT_RX	Badly-structured transaction portions received on the reporting FS.
TCAP_BAD_STRUCT_TRANS_PORT_TX	Badly-structured transaction portions sent by the reporting FS.
TCAP_BEGIN_MSG_RX	Begin messages received on the reporting FS.
TCAP_BEGIN_MSG_TX	Begin messages sent by the reporting FS.
TCAP_BIND_CONFIRM_RX	TCAP bind confirm messages received on the reporting FS.
TCAP_CLOSE_IND_RX	Close indication messages received on the reporting FS.
TCAP_COMPONENT_CONFIRM_RX	Component confirm messages received on the reporting FS.
TCAP_COMPONENT_IND_RX	Component indication messages received on the reporting FS.
TCAP_COMPONENT_REQ_RX	Component request messages received on the reporting FS.
TCAP_CONT_MSG_RX	Continue messages received on the reporting FS.
TCAP_CONT_MSG_TX	Continue messages sent by the reporting FS.
TCAP_DATA_IND_RX	Data indication messages received on the reporting FS.
TCAP_DATA_REQ_RX	Data request messages received on the reporting FS.
TCAP_DELIMITER_IND_RX	Delimiter indication messages received on the reporting FS.
TCAP_DELIMITER_REQ_RX	Delimiter request messages received on the reporting FS.

Table 6-19 TCAP Measurements (continued)

Measurement	Description (* = rapid count could mean a potential problem in the system)
TCAP_DIALOG_CONFIRM_RX	Dialog confirm messages received on the reporting FS.
TCAP_DUP_INVOKE_ID_RX	Duplicate invoke ids received on the reporting FS.
TCAP_DUP_INVOKE_ID_TX	Duplicate invoke ids sent by the reporting FS.
TCAP_END_MSG_RX	End messages received on the reporting FS.
TCAP_END_MSG_TX	End messages sent by the reporting FS.
TCAP_INCONSIST_DIALOG_PORT_RX	Inconsistent dialog portions received on the reporting FS.
TCAP_INCONSIST_DIALOG_PORT_TX	Inconsistent dialog portions sent by the reporting FS.
TCAP_INCORRECT_COMP_ENCODE_RX	Incorrect component encoding errors received on the reporting FS.
TCAP_INCORRECT_COMP_PORT_RX	Incorrect component portions received on the reporting FS.
TCAP_INCORRECT_COMP_PORT_TX	Incorrect component portions sent by the reporting FS.
TCAP_INCORRECT_PARAM_RE_RX	Incorrect parameters on return errors received on the reporting FS.
TCAP_INCORRECT_PARAM_RE_TX	Incorrect parameters on return errors sent by the reporting FS.
TCAP_INCORRECT_PARAM_RR_RX	Incorrect parameters on return-results received on the reporting FS.
TCAP_INCORRECT_PARAM_RR_TX	Incorrect parameters on return-results sent by the reporting FS.
TCAP_INCORRECT_PARAM_RX	Incorrect parameters received on the reporting FS.
TCAP_INCORRECT_PARAM_TX	Incorrect parameters sent by the reporting FS.
TCAP_INCORRECT_TRANS_PORT_RX	Incorrect transaction portions received on the reporting FS.
TCAP_INCORRECT_TRANS_PORT_TX	Incorrect transaction portions sent by the reporting FS.
TCAP_INIT_REL_RX	Initiating releases received on the reporting FS.
TCAP_INIT_REL_TX	Initiating releases sent by the reporting FS.
TCAP_INVOKE_COMP_RX	Invoke components received on the reporting FS.
TCAP_INVOKE_COMP_TX	Invoke components sent by the reporting FS.
TCAP_INVOKE_RSCR_LIMIT_PROB_RX	Resource limitation invoke problems received on the reporting FS.
TCAP_MISSING_DIALOG_PORT_RX	Missing dialog portions received on the reporting FS.
TCAP_MISSING_DIALOG_PORT_TX	Missing dialog portions sent by the reporting FS.
TCAP_NO_PERMISS_CONVERS_RX	Conversation without permission messages received on the reporting FS.
TCAP_NO_PERMISS_CONVERS_TX	Conversation without permission messages sent by the reporting FS.
TCAP_NO_PERMISS_QUERY_RX	Query without permission messages received on the reporting FS.
TCAP_NO_PERMISS_QUERY_TX	Query without permission messages sent by the reporting FS.
TCAP_NOTICE_IND_RX	TCAP notice indication messages received on the reporting FS.

Table 6-19 TCAP Measurements (continued)

Measurement	Description (* = rapid count could mean a potential problem in the system)
TCAP_OPEN_CONFIRM_RX	Open confirm messages received on the reporting FS.
TCAP_OPEN_IND_RX	Open indication messages received on the reporting FS.
TCAP_OPERATION_CONFIRM_RX	Operation confirm messages received on the reporting FS.
TCAP_OPERATION_IND_RX	Operation indication messages received on the reporting FS.
TCAP_OPERATION_REQ_RX	Operation request messages received on the reporting FS.
TCAP_PERMISS_CONVERS_RX	Conversation with permission messages received on the reporting FS.
TCAP_PERMISS_CONVERS_TX	Conversation with permission messages sent by the reporting FS.
TCAP_PERMISS_QUERY_RX	Query with permission messages received on the reporting FS.
TCAP_PERMISS_QUERY_TX	Query with permission messages sent by the reporting FS.
TCAP_REJECT_COMP_RX	Reject components received on the reporting FS.
TCAP_REJECT_COMP_TX	Reject components sent by the reporting FS.
TCAP_RETURN_ERR_COMP_RX	Return-error components received on the reporting FS.
TCAP_RETURN_ERR_COMP_TX	Return-error components sent by the reporting FS.
TCAP_RETURN_RESULT_COMP_RX	Return-result components received on the reporting FS.
TCAP_RETURN_RESULT_COMP_TX	Return-result components sent by the reporting FS.
TCAP_RSCR_LIMIT_RX	Resource limitations received on the reporting FS.
TCAP_RSCR_LIMIT_TX	Resource limitations sent by the reporting FS.
TCAP_RSP_RX	Response messages received on the reporting FS.
TCAP_RSP_TX	Response messages sent by the reporting FS.
TCAP_STAT_CONFIRM_RX	TCAP statistics confirm messages received on the reporting FS.
TCAP_STAT_IND_RX	TCAP statistics indication messages received on the reporting FS.
TCAP_STATUS_IND_RX	Status indication messages received on the reporting FS.
TCAP_TOTAL_COMP_RX	Components received on the reporting FS.
TCAP_TOTAL_COMP_TX	Components sent by the reporting FS.
TCAP_TOTAL_DROPPED_MSG_RX	Received messages dropped on the reporting FS.
TCAP_TOTAL_MSG_RX	Messages received by the reporting FS.
TCAP_TOTAL_MSG_TX	Messages sent by the reporting FS.
TCAP_TOTAL_UNI_MSG_RX	Unidirectional messages received by the reporting FS.
TCAP_TOTAL_UNI_MSG_TX	Unidirectional messages sent by the reporting FS.
TCAP_TRANS_PORT_PERM_REL_RX	Transaction portion permission to release problems received on the reporting FS.
TCAP_TRANSACTION_IDS_INUSE	Transaction ids in use on the reporting FS.
TCAP_UDATA_IND_RX	Data indication messages received on the reporting FS.
TCAP_UNEXPECT_ERR_CODE_RX	Unexpected error codes on return-error received on the reporting FS.

Table 6-19 TCAP Measurements (continued)

Measurement	Description (* = rapid count could mean a potential problem in the system)
TCAP_UNEXPECT_ERR_CODE_TX	Unexpected error codes on return-error sent by the reporting FS.
TCAP_UNEXPECT_LINK_OPER_RX	Unexpected link operations received on the reporting FS.
TCAP_UNEXPECT_LINK_OPER_TX	Unexpected link operations sent by the reporting FS.
TCAP_UNEXPECT_LINK_RSP_RX	Unexpected link responses received on the reporting FS.
TCAP_UNEXPECT_LINK_RSP_TX	Unexpected link responses sent by the reporting FS.
TCAP_UNEXPECT_RE_RX	Unexpected return error received on the reporting FS.
TCAP_UNEXPECT_RE_TX	Unexpected return error sent by the reporting FS.
TCAP_UNEXPECT_RR_RX	Unexpected return-results received on the reporting FS.
TCAP_UNEXPECT_RR_TX	Unexpected return-results sent by the reporting FS.
TCAP_UNRECOG_COMP_RX	Unrecognized components received on the reporting FS.
TCAP_UNRECOG_COMP_TX	Unrecognized components sent by the reporting FS.
TCAP_UNRECOG_DIALOG_PORT_ID_RX	Unrecognized dialog portion ids received on the reporting FS.
TCAP_UNRECOG_DIALOG_PORT_ID_TX	Unrecognized dialog portion ids sent by the reporting FS.
TCAP_UNRECOG_ERR_CODE_RX	Unrecognized error codes on return-error received on the reporting FS.
TCAP_UNRECOG_ERR_CODE_TX	Unrecognized error codes on return-error sent by the reporting FS.
TCAP_UNRECOG_INVOKE_ID_RX	Unrecognized invoke ids on return-results received on the reporting FS.
TCAP_UNRECOG_INVOKE_ID_TX	Unrecognized invoke ids on return results sent by the reporting FS.
TCAP_UNRECOG_LINK_ID_RX	Unrecognized link ids received on the reporting FS.
TCAP_UNRECOG_LINK_ID_TX	Unrecognized link ids sent by the reporting FS.
TCAP_UNRECOG_MSG_TYPE_RX	Unrecognized messages types received on the reporting FS.
TCAP_UNRECOG_MSG_TYPE_TX	Unrecognized messages types sent by the reporting FS.
TCAP_UNRECOG_OPCODE_RX	Unrecognized opcodes received on the reporting FS.
TCAP_UNRECOG_OPCODE_TX	Unrecognized opcodes sent by the reporting FS.
TCAP_UNRECOG_RE_INVOKE_ID_RX	Unrecognized invoke ids on return-error received on the reporting FS.
TCAP_UNRECOG_RE_INVOKE_ID_TX	Unrecognized invoke ids on return-error sent by the reporting FS.
TCAP_UNRECOG_TRANS_ID_RX	Unrecognized transaction ids received on the reporting FS.
TCAP_UNRECOG_TRANS_ID_TX	Unrecognized transaction ids sent by the reporting FS.

SUA Measurements

Table 6-20 SUA Measurements

Measurement	Description (* = rapid count could mean a potential problem in the system)
SUA_ACTIVE_ACK_RX	ACTIVE Acknowledges received on the reporting signaling gateway process.
SUA_ACTIVE_TX	ACTIVES sent on the reporting signaling gateway process.
SUA_ASSOC_FAIL	Association failures on the reporting signaling gateway process.
SUA_BEAT_ACK_RX	BEAT Acknowledges received on the reporting signaling gateway process.
SUA_BEAT_ACK_TX	BEAT Acknowledges sent on the reporting signaling gateway process.
SUA_BEAT_RX	BEATs received on the reporting signaling gateway process.
SUA_BEAT_TX	BEATs sent on the reporting signaling gateway process.
SUA_CLDR_RX	CLDRs received on the reporting signaling gateway process.
SUA_CLDR_TX	CLDRs sent on the reporting signaling gateway process.
SUA_CLDT_RX	CLDTs received on the reporting signaling gateway process.
SUA_CLDT_TX	CLDTs sent on the reporting signaling gateway process.
SUA_DATA_BYTES_RX	Data bytes received on the reporting signaling gateway process.
SUA_DATA_BYTES_TX	Data bytes sent on the reporting signaling gateway process.
SUA_DAUD_TX	DAUDs sent on the reporting signaling gateway process.
SUA_DAVA_RX	DAVAs received on the reporting signaling gateway process.
SUA_DOWN_ACK_RX	DOWN Acknowledges received on the reporting signaling gateway process.
SUA_DOWN_TX	DOWNs sent on the reporting signaling gateway process.
SUA_DRST_RX	DRSTs received on the reporting signaling gateway process.
SUA_DUNA_RX	DUNAs received on the reporting signaling gateway process.
SUA_DUPU_RX	DUPUs received on the reporting signaling gateway process.
SUA_ERR_RX	Errors received on the reporting signaling gateway process.
SUA_ERR_TX	Errors sent on the reporting signaling gateway process.
SUA_INACTIVE_ACK_RX	INACTIVE Acknowledges received on the reporting signaling gateway process.
SUA_INACTIVE_TX	ACTIVES received on the reporting signaling gateway process.
SUA_INVALID_SCTP_SIGNALS	Invalid SCTP signals on the reporting signaling gateway process.
SUA_MSG_CLASS_ERR	Message class errors on the reporting signaling gateway process.
SUA_MSG_INVALID_LENGTH_RX	Messages of invalid length received on the reporting signaling gateway process.
SUA_MSG_TYPE_ERR	Message type errors on the reporting signaling gateway process.
SUA_NETWORK_APPEAR_ERR	Network appearance errors on the reporting signaling gateway process.
SUA_NO_MEMORY_FAIL	No memory for message errors on the reporting signaling gateway process.
SUA_NOTIFY_RX	NOTIFYs received on the reporting signaling gateway process.
SUA_NOTIFY_TX	NOTIFYs sent on the reporting signaling gateway process.
SUA_PARAM_FIELD_ERR	Parameter field errors on the reporting signaling gateway process.
SUA_PARAM_VALUE_ERR	Parameter value errors on the reporting signaling gateway process.

Table 6-20 SUA Measurements (continued)

Measurement	Description (* = rapid count could mean a potential problem in the system)
SUA_PROTOCOL_ERR	Protocol errors on the reporting signaling gateway process.
SUA_ROUTING_CONTEXT_ERR	Routing context errors on the reporting signaling gateway process.
SUA_SCON_RX	SCONs received on the reporting signaling gateway process.
SUA_SCON_TX	SCONs sent on the reporting signaling gateway process.
SUA_SCTP_TX_FAIL	SCTP send failures on message processing errors on the reporting signaling gateway process.
SUA_SINCE_LAST_RESET_ASSOC	SCTP errors since last reset of association on the reporting signaling gateway process.
SUA_STREAM_ID_ERR	Stream id errors on the reporting signaling gateway process.
SUA_UNEXPECT_MSG_ERR	Unexpected message errors on the reporting signaling gateway process.
SUA_UNEXPECT_PARAM_ERR	Unexpected parameter errors on the reporting signaling gateway process.
SUA_UP_ACK_RX	UP Acknowledges received on the reporting signaling gateway process.
SUA_UP_TX	UPs sent on the reporting signaling gateway process.
SUA_VERSION_ERR	Version errors on the reporting signaling gateway process.

M3UA Protocol Measurements

Table 6-21 M3UA Measurements

Measurement	Description (* = rapid count could mean a potential problem in the system)
M3UA_ACTIVE_ACK_RX	ACTIVE Acknowledges received on the reporting signaling gateway process.
M3UA_ACTIVE_TX	ACTIVEs sent on the reporting signaling gateway process.
M3UA_ASSOC_FAIL	Association failures on the reporting signaling gateway process.
M3UA_BEAT_ACK_RX	BEAT Acknowledges received on the reporting signaling gateway process.
M3UA_BEAT_ACK_TX	BEAT Acknowledges sent on the reporting signaling gateway process.
M3UA_BEAT_RX	BEATs received on the reporting signaling gateway process.
M3UA_BEAT_TX	BEATs sent on the reporting signaling gateway process.
M3UA_DATA_BYTES_RX	Data bytes received on the reporting signaling gateway process.
M3UA_DATA_BYTES_TX	Data bytes sent on the reporting signaling gateway process.
M3UA_DATA_TRANS_RX	Data transfers received on the reporting signaling gateway process.
M3UA_DATA_TRANS_TX	Data transfers sent on the reporting signaling gateway process.
M3UA_DAUD_TX	DAUDs sent on the reporting signaling gateway process.
M3UA_DAVA_RX	DAVAs received on the reporting signaling gateway process.
M3UA_DOWN_ACK_RX	DOWN Acknowledges received on the reporting signaling gateway process.
M3UA_DOWN_TX	DOWNs sent on the reporting signaling gateway process.
M3UA_DRST_RX	DRSTs received on the reporting signaling gateway process.
M3UA_DUNA_RX	DUNAs received on the reporting signaling gateway process.
M3UA_DUPU_RX	DUPUs received on the reporting signaling gateway process.
M3UA_ERR_RX	Errors received on the reporting signaling gateway process.
M3UA_ERR_TX	Errors sent on the reporting signaling gateway process.
M3UA_INACTIVE_ACK_RX	INACTIVE Acknowledges received on the reporting signaling gateway process.
M3UA_INACTIVE_TX	ACTIVEs received on the reporting signaling gateway process.
M3UA_INVALID_SCTP_SIGNALS	Invalid SCTP signals on the reporting signaling gateway process.
M3UA_MSG_CLASS_ERR	Message class errors on the reporting signaling gateway process.
M3UA_MSG_LENGTH_ERR	Messages of invalid length received on the reporting signaling gateway process.
M3UA_MSG_RX_OTHER_ERR	Messages received with other errors on the reporting CA or FS
M3UA_MSG_TYPE_ERR	Message type errors on the reporting signaling gateway process.
M3UA_NETWORK_APPEAR_ERR	Network appearance errors on the reporting signaling gateway process.
M3UA_NO_MEMORY_ERR	No memory for message errors on the reporting signaling gateway process.
M3UA_NOTIFY_RX	NOTIFYs received on the reporting signaling gateway process.
M3UA_NOTIFY_TX	NOTIFYs sent on the reporting signaling gateway process.
M3UA_PARAM_FIELD_ERR	Parameter field errors on the reporting signaling gateway process.
M3UA_PARAM_VALUE_ERR	Parameter value errors on the reporting signaling gateway process.
M3UA_PROTOCOL_ERR	Protocol errors on the reporting signaling gateway process.

Table 6-21 M3UA Measurements (continued)

Measurement	Description (* = rapid count could mean a potential problem in the system)
M3UA_ROUTING_CONTEXT_ERR	Routing context errors on the reporting signaling gateway process.
M3UA_SCON_RX	SCONs received on the reporting signaling gateway process.
M3UA_SCON_TX	SCONs sent on the reporting signaling gateway process.
M3UA_SCTP_TX_FAIL	SCTP send failures on message processing errors on the reporting signaling gateway process.
M3UA_SGP_ID	The id of the signaling gateway process that these measurements are associated with.
M3UA_SINCE_LAST_RESET_ASSOC	SCTP errors since last reset of association on the reporting signaling gateway process.
M3UA_STREAM_ID_ERR	Stream id errors on the reporting signaling gateway process.
M3UA_UNEXPECT_MSG_ERR	Unexpected message errors on the reporting signaling gateway process.
M3UA_UNEXPECT_PARAM_ERR	Unexpected parameter errors on the reporting signaling gateway process.
M3UA_UP_ACK_RX	UP Acknowledges received on the reporting signaling gateway process.
M3UA_UP_TX	UPs sent on the reporting signaling gateway process.
M3UA_VERSION_ERR	Version errors on the reporting signaling gateway process.

SCTP Measurements

Table 6-22 SCTP Measurements

Measurement	Description (* = rapid count could mean a potential problem in the system)
SCTP_ASSOC_COMM_LOST	Times the SCTP association communication was lost on the reporting sctp association.
SCTP_CHUNK_TOO_LARGE_ERR	Data chunks received too big on the reporting sctp association.
SCTP_CHUNK_ORDER_ERR	Ordered chunks in error on the reporting sctp association.
SCTP_CHUNK_TOO_SMALL_ERR	Data chunks received too small on the reporting sctp association.
SCTP_CONTROL_CHUNK_RX	Control chunks received on the reporting sctp association.
SCTP_CONTROL_CHUNK_TX	Control chunks sent on the reporting sctp association.
SCTP_COOKIE_IN_SHUTDOWN_ERR_RX	Times an SCTP peer reported that is received a COOKIE ECHO while in the SHUTDOWN_ACK_SENT state on the reporting sctp association.
SCTP_CWR_CHUNK_RX	CWR chunks received on the reporting sctp association.
SCTP_DATA_BYTE_RX	Data bytes received over SCTP on the reporting sctp association.
SCTP_DATA_BYTE_TX	Data bytes sent over SCTP on the reporting sctp association.
SCTP_DATA_CHUNK_DISCARD	Received duplicate data chunks discarded on the reporting sctp association.
SCTP_DATA_CHUNK_RETRAN	Data chunks retransmitted on the reporting sctp association.
SCTP_DATA_CHUNK_RX	Data chunks received on the reporting sctp association.
SCTP_DATA_CHUNK_RX_BUNDLE	Bundled data chunks received on the reporting sctp association.
SCTP_DATA_CHUNK_RX_ORDER	Ordered data chunks received on the reporting sctp association.
SCTP_DATA_CHUNK_RX_SEQ_ERR	Out-of-sequence data chunks received on the reporting sctp association.
SCTP_DATA_CHUNK_RX_UNORDER	Unordered data chunks received on the reporting sctp association.
SCTP_DATA_CHUNK_TX	Data chunks sent on the reporting sctp association.
SCTP_DATA_CHUNK_TX_BUNDLE	Bundled data chunks sent on the reporting sctp association.
SCTP_DATA_CHUNK_TX_ORDER	Ordered data chunks sent on the reporting sctp association.
SCTP_DATA_CHUNK_TX_UNORDER	Unordered data chunks sent on the reporting sctp association.
SCTP_DEST_ADDR_FAIL	Times a destination address failed on the reporting sctp association.
SCTP_ECNE_CHUNK_RX	ECNE chunks received on the reporting sctp association.
SCTP_EMPTY_DATAG_ERR	Datagrams received with no data chunks on the reporting sctp association.
SCTP_EXPIRED_COOKIE_ERR	Times a cookie echo was received after the cookie timer expired on the reporting sctp association.
SCTP_INVALID_BUNDLE_CHUNK	invalid bundle chunks received on the reporting sctp association.
SCTP_INVALID_CHECKSUM	SCTP datagrams received with an invalid checksum on the reporting sctp association.
SCTP_INVALID_COOKIE_SIG	Invalid cookie signals received on the reporting sctp association.
SCTP_INVALID_DATAG_LENGTH	Datagrams received with an invalid length on the reporting sctp association.

Table 6-22 SCTP Measurements (continued)

Measurement	Description (* = rapid count could mean a potential problem in the system)
SCTP_INVALID_PARAM_ERR_RX	Times an SCTP peer reported that it received an INIT or INIT ACK chunk containing one or more mandatory parameters set to an invalid value on the reporting sctp association.
SCTP_INVALID_STREAM	Datagrams with invalid stream ids received on the reporting sctp association.
SCTP_INVALID_STREAM_ERR_RX	Times an SCTP peer reported receiving a data chunk on a non-existing stream on the reporting sctp association.
SCTP_INVALID_VERIF_TAG	Datagrams with invalid verification tags received on the reporting sctp association.
SCTP_MISSING_PARAM_ERR	Times that an INIT or INIT ACK chunk was received with one or more mandatory parameters missing on the reporting sctp association.
SCTP_MISSING_PARAM_ERR_RX	Times an INIT or INIT ACK was missing one or more mandatory parameters received on the reporting sctp association.
SCTP_NO_SPACE_INCOM_ERR	Data chunks dropped due to lack of space in the local receive window on the reporting sctp association.
SCTP_NO_USER_DATA_ERR_RX	Times an SCTP peer reported that it received a data chunk with no user data in it on the reporting sctp association.
SCTP_OOTB	Out of the blue packets received on the reporting sctp association.
SCTP_OUT_OF_RSCR_ERR_RX	Times an SCTP peer reported it was out of resources on the reporting sctp association.
SCTP_PARTIAL_CHUNK_ERR	Partial chunks received in a datagram on the reporting sctp association.
SCTP_PEER_RESTART_ERR	Times the SCTP peer restarted on the reporting sctp association.
SCTP_SCTP_ASSOC_ID	The id of the SCTP association that the measurement measurement block is associated with.
SCTP_SCTP_DATAG_RX	Datagrams received on the reporting sctp association.
SCTP_SCTP_DATAG_TX	Datagrams sent on the reporting sctp association.
SCTP_STALE_COOKIE_ERR	Times other endpoint indicates that the cookie echo was received after the cookie time expired on the reporting sctp association.
SCTP_STALE_COOKIE_ERR_RX	Times an SCTP peer received a valid cookie that had expired on the reporting sctp association.
SCTP_ULP_QUEUE	Upper layer process datagrams queued to be transmitted on the reporting sctp association.
SCTP_ULP_READY	Received datagrams that are ready to be sent to upper layer processes on the reporting sctp association.
SCTP_ULP_RX	Received upper layer process datagrams on the reporting sctp association.
SCTP_ULP_TX	ULP datagrams sent on the reporting sctp association.
SCTP_UNKNOWN_CHUNK_TYPE	datagrams with an unknown chunk type received on the reporting sctp association.
SCTP_UNKNOWN_INIT_PARAM	INIT datagrams with an unknown parameter received on the reporting sctp association.

Table 6-22 SCTP Measurements (continued)

Measurement	Description (* = rapid count could mean a potential problem in the system)
SCTP_UNRECOG_CHUNK_ERR_RX	Times an SCTP peer reported that it received a chunk that it could not understand on the reporting sctp association.
SCTP_UNRECOG_PARAM_ERR_RX	Times an SCTP peer reported that it received an INIT ACK containing one or more parameters unrecognized on the reporting sctp association.
SCTP_UNRESOLV_ADDR_ERR_RX	Times an SCTP reported that it received a packet with an address it could not resolve on the reporting sctp association.
SCTP_V6_ADDR_PARAM_RX	Packets received with version 6 parameters on the reporting sctp association.

IUA Measurements

Table 6-23 IUA Measurements

Measurement	Description
IUA_ACTIVE_ACK_RX	ASP_ACTIVE_ACK messages received on the reporting SCTP association.
IUA_ACTIVE_TX	ASP_ACTIVE messages transmitted on the reporting SCTP association.
IUA_ASSOC_FAIL	SCTP association establishment failures on the reporting SCTP association.
IUA_BEAT_ACK_RX	HEARTBEAT ACK messages received on the reporting SCTP association.
IUA_BEAT_ACK_TX	HEARTBEAT ACK messages transmitted on the reporting SCTP association.
IUA_BEAT_RX	HEARTBEAT messages received on the reporting SCTP association.
IUA_BEAT_TX	HEARTBEAT messages transmitted on the reporting SCTP association.
IUA_DATA_BYTES_RX	Data bytes received on the reporting SCTP association.
IUA_DATA_BYTES_TX	Data bytes transmitted on the reporting SCTP association.
IUA_DATA_IND_RX	DATA_INDICATION messages received on the reporting SCTP association.
IUA_DATA_REQ_TX	DATA_REQUEST messages transmitted on the reporting SCTP association.
IUA_DOWN_ACK_RX	ASP_DOWN_ACK messages received on the reporting SCTP association.
IUA_DOWN_TX	ASP_DOWN messages transmitted on the reporting SCTP association.
IUA_ERR_RX	ERROR messages received on the reporting SCTP association.
IUA_ERR_TX	ERROR messages transmitted on the reporting SCTP association.
IUA_EST_CFM_RX	ESTABLISH_CONFIRM messages received on the reporting SCTP association.
IUA_EST_IND_RX	ESTABLISH_INDICATION messages received on the reporting SCTP association.
IUA_EST_REQ_TX	ESTABLISH_REQUEST messages transmitted on the reporting SCTP association.
IUA_INACTIVE_ACK_RX	ASP_INACTIVE_ACK messages received on the reporting SCTP association.
IUA_INACTIVE_TX	ASP_INACTIVE messages transmitted on the reporting SCTP association.
IUA_INTF_ID_ERR	Invalid interface id errors on the reporting SCTP association.
IUA_INVALID_SCTP_SIGNALS_SLR	Invalid SCTP signals received since last reset of association on the reporting SCTP association.
IUA_INVALID_SCTP_SIGNALS_TOTAL	Invalid SCTP signals received on the reporting SCTP association.
IUA_MSG_CLASS_ERR	Unsupported message class errors on the reporting SCTP association.
IUA_MSG_LENGTH_ERR	Message length errors on the reporting SCTP association.

Table 6-23 IUA Measurements (continued)

Measurement	Description
IUA_MSG_OTHER_ERR	Other message errors on the reporting SCTP association.
IUA_MSG_TYPE_ERR	Unsupported message type errors on the reporting SCTP association.
IUA_NO_MEMORY_ERR	No memory for message errors on the reporting SCTP association.
IUA_NOTIFY_RX	NOTIFY messages received on the reporting SCTP association.
IUA_PARAM_FIELD_ERR	Parameter field errors on the reporting SCTP association.
IUA_PARAM_VALUE_ERR	Parameter value errors on the reporting SCTP association.
IUA_PROTOCOL_ERR	Protocol errors on the reporting SCTP association.
IUA_REL_CFM_RX	RELEASE_CONFIRM messages received on the reporting SCTP association.
IUA_REL_IND_RX	RELEASE_INDICATION messages received on the reporting SCTP association.
IUA_REL_REQ_TX	RELEASE_REQUEST messages transmitted on the reporting SCTP association.
IUA_SCTP_ASSOC_ID	The id of the sctp association with which the measurement measurement block is associated. This is not an incremental measurement.
IUA_SCTP_TX_FAIL	SCTP send failures on message processing errors on the reporting SCTP association.
IUA_STREAM_ID_ERR	Invalid stream id errors on the reporting SCTP association.
IUA_TEI_SAPI_ERR	Invalid TEI or SAPI errors on the reporting SCTP association.
IUA_UNEXPECT_MSG_ERR	Unexpected message errors on the reporting SCTP association.
IUA_UNEXPECT_PARAM_ERR	Unexpected parameter errors on the reporting SCTP association.
IUA_UP_ACK_RX	ASP_UP_ACK messages received on the reporting SCTP association.
IUA_UP_TX	ASP_UP messages transmitted on the reporting SCTP association.
IUA_VERSION_ERR	Invalid version errors on the reporting SCTP association.

ISUP Measurements

Table 6-24 ISUP Protocol Measurements

ISUP_ABNORMAL_REL_RX	Release messages received with a cause other than NORMAL on the reporting trunk group.
ISUP_ABNORMAL_REL_TX	Release messages sent with a cause other than NORMAL on the reporting trunk group.
ISUP_ACM_RX	Address Complete messages received on the reporting trunk group.
ISUP_ACM_TX	Address Complete messages sent on the reporting trunk group.
ISUP_ANM_RX	Answer messages received on the reporting trunk group.
ISUP_ANM_TX	Answer messages sent on the reporting trunk group.
ISUP_ARR_RX	Automatic Re-Route messages received on the reporting trunk group.
ISUP_ARR_TX	Automatic Re-Route messages sent on the reporting trunk group.
ISUP_BLA_RX	Blocking Acknowledge messages received on the reporting trunk group.
ISUP_BLA_TX	Blocking Acknowledge messages sent on the reporting trunk group.
ISUP_BLO_RX	Blocking messages received on the reporting trunk group.
ISUP_BLO_TX	Blocking messages sent on the reporting trunk group.
ISUP_CCL_RX	Calling Party Clear messages received on the reporting trunk group.
ISUP_CCL_TX	Calling Party Clear messages sent on the reporting trunk group.
ISUP_CCR_RX	Continuity Check Request messages received on the reporting trunk group.
ISUP_CCR_TX	Continuity Check Request messages sent on the reporting trunk group.
ISUP_CFN_RX	Confusion messages received on the reporting trunk group.
ISUP_CFN_TX	Confusion messages sent on the reporting trunk group.
ISUP_CGB_RX	Circuit Group Blocking messages received on the reporting trunk group.
ISUP_CGB_TX	Circuit Group Blocking messages sent on the reporting trunk group.
ISUP_CGBA_RX	Circuit Group Blocking Acknowledgement messages received on the reporting trunk group.
ISUP_CGBA_TX	Circuit Group Blocking Acknowledgement messages sent on the reporting trunk group.
ISUP_CGU_RX	Circuit Group Unblocking messages received on the reporting trunk group.
ISUP_CGU_TX	Circuit Group Unblocking messages sent on the reporting trunk group.
ISUP_CGUA_RX	Circuit Group Unblocking Acknowledgement messages received on the reporting trunk group.
ISUP_CGUA_TX	Circuit Group Unblocking Acknowledgement messages sent on the reporting trunk group.
ISUP_CON_RX	Connect messages received on the reporting trunk group.
ISUP_CON_TX	Connect messages sent on the reporting trunk group.
ISUP_CONG_CALL_REJECTED	The congestion-rejected calls on a per trunk group basis. This is implemented for SGA.
ISUP_COT_RX	Continuity messages received on the reporting trunk group.

Table 6-24 ISUP Protocol Measurements (continued)

ISUP_COT_TX	Continuity messages sent on the reporting trunk group.
ISUP_CPG_RX	Call Progress messages received on the reporting trunk group.
ISUP_CPG_TX	Call Progress messages sent on the reporting trunk group.
ISUP_CQM_RX	Circuit Query messages received on the reporting trunk group.
ISUP_CQM_TX	Circuit Query messages sent on the reporting trunk group.
ISUP_CQR_RX	Circuit Query Response messages received on the reporting trunk group.
ISUP_CQR_TX	Circuit Query Response messages sent on the reporting trunk group.
ISUP_CRA_RX	Circuit Reservation Acknowledgement messages received on the reporting trunk group.
ISUP_CRA_TX	Circuit Reservation Acknowledgement messages sent on the reporting trunk group.
ISUP_CRG_RX	Charge Information messages received on the reporting trunk group.
ISUP_CRG_TX	Charge Information messages sent on the reporting trunk group.
ISUP_CRM_RX	Circuit Reservation messages received on the reporting trunk group.
ISUP_CRM_TX	Circuit Reservation messages sent on the reporting trunk group.
ISUP_CVR_RX	Circuit Validation Response messages received on the reporting trunk group.
ISUP_CVR_TX	Circuit Validation Response messages sent on the reporting trunk group.
ISUP_CVT_RX	Circuit Validation Test messages received on the reporting trunk group.
ISUP_CVT_TX	Circuit Validation Test messages sent on the reporting trunk group.
ISUP_EXM_RX	Exit messages received on the reporting trunk group.
ISUP_EXM_TX	Exit messages sent on the reporting trunk group.
ISUP_FAA_RX	Facility Accepted messages received on the reporting trunk group.
ISUP_FAA_TX	Facility Accepted messages sent on the reporting trunk group.
ISUP_FAC_RX	Facility messages received on the reporting trunk group.
ISUP_FAC_TX	Facility messages sent on the reporting trunk group.
ISUP_FAR_RX	Facility Request messages received on the reporting trunk group.
ISUP_FAR_TX	Facility Request messages sent on the reporting trunk group.
ISUP_FOT_RX	Forward Transfer messages received on the reporting trunk group.
ISUP_FOT_TX	Forward Transfer messages sent on the reporting trunk group.
ISUP_FRJ_RX	Facility Reject messages received on the reporting trunk group.
ISUP_FRJ_TX	Facility Reject messages sent on the reporting trunk group.
ISUP_FWT_RX	Forward Transfer messages received on the reporting trunk group.
ISUP_FWT_TX	Forward Transfer messages sent on the reporting trunk group.
ISUP_GRA_RX	Circuit Group Reset Acknowledge messages received on the reporting trunk group.
ISUP_GRA_TX	Circuit Group Reset Acknowledge messages sent on the reporting trunk group.
ISUP_GRS_RX	Circuit Group Reset messages received on the reporting trunk group.
ISUP_GRS_TX	Circuit Group Reset messages sent on the reporting trunk group.

Table 6-24 ISUP Protocol Measurements (continued)

ISUP_IAM_RX	Initial Address messages received on the reporting trunk group.
ISUP_IAM_TX	Initial Address messages sent on the reporting trunk group.
ISUP_IDR_RX	ID Request messages received on the reporting trunk group.
ISUP_IDR_TX	ID Request messages sent on the reporting trunk group.
ISUP_INF_RX	Information messages received on the reporting trunk group.
ISUP_INF_TX	Information messages sent on the reporting trunk group.
ISUP_INR_RX	Information Request messages received on the reporting trunk group.
ISUP_INR_TX	Information Request messages sent on the reporting trunk group.
ISUP_IRS_RX	ID Response messages received on the reporting trunk group.
ISUP_IRS_TX	ID Response messages sent on the reporting trunk group.
ISUP_ITX_RX	Charge Unit messages received on the reporting trunk group.
ISUP_ITX_TX	Charge Unit messages sent on the reporting trunk group.
ISUP_LPA_RX	Loop Prevention Acknowledgement messages received on the reporting trunk group.
ISUP_LPA_TX	Loop Prevention Acknowledgement messages sent on the reporting trunk group.
ISUP_LPM_RX	Loop Prevention messages received on the reporting trunk group.
ISUP_LPM_TX	Loop Prevention messages sent on the reporting trunk group.
ISUP_MSG_RX	Messages received on the reporting trunk group.
ISUP_MSG_TX	Messages sent on the reporting trunk group.
ISUP_NRM_RX	NRM messages received on the reporting trunk group.
ISUP_NRM_TX	Network Resource Management messages sent on the reporting trunk group.
ISUP_OC_IAM_REJECTED	Congestion-rejected calls per trunk group.
ISUP_OLM_RX	Overload messages received on the reporting trunk group.
ISUP_OLM_TX	Overload messages sent on the reporting trunk group.
ISUP_OPR_RX	Operator messages received on the reporting trunk group.
ISUP_OPR_TX	Operator messages sent on the reporting trunk group.
ISUP_PAM_RX	Pass Along messages received on the reporting trunk group.
ISUP_PAM_TX	Pass Along messages sent on the reporting trunk group.
ISUP_PRI_RX	Pre-Release Information messages received on the reporting trunk group.
ISUP_PRI_TX	Pre-Release Information messages sent on the reporting trunk group.
ISUP_REL_RX	Release messages received on the reporting trunk group.
ISUP_REL_TX	Release messages sent on the reporting trunk group.
ISUP_RES_RX	Resume messages received on the reporting trunk group.
ISUP_RES_TX	Resume messages sent on the reporting trunk group.
ISUP_RLC_RX	Release Complete messages received on the reporting trunk group.
ISUP_RLC_TX	Release Complete messages sent on the reporting trunk group.
ISUP_RSC_RX	Reset Circuit messages received on the reporting trunk group.

Table 6-24 ISUP Protocol Measurements (continued)

ISUP_RSC_TX	Reset Circuit messages sent on the reporting trunk group.
ISUP_SAM_RX	Subsequent Address messages received on the reporting trunk group.
ISUP_SAM_TX	Subsequent Address messages sent on the reporting trunk group.
ISUP_SGM_RX	Segmentation messages received on the reporting trunk group.
ISUP_SGM_TX	Segmentation messages sent on the reporting trunk group.
ISUP_SUS_RX	Suspend messages received on the reporting trunk group.
ISUP_SUS_TX	Suspend messages sent on the reporting trunk group.
ISUP_TXA_RX	Charging Acknowledgement messages received on the reporting trunk group.
ISUP_TXA_TX	Charging Acknowledgement messages sent on the reporting trunk group.
ISUP_UBA_RX	Unblocking Acknowledge messages received on the reporting trunk group.
ISUP_UBA_TX	Unblocking Acknowledge messages sent on the reporting trunk group.
ISUP_UBL_RX	Unblocking messages received on the reporting trunk group.
ISUP_UBL_TX	Unblocking messages sent on the reporting trunk group.
ISUP_UNEXPECT_MSG_RX	Unexpected messages received on the reporting trunk group.
ISUP_UNRECOG_MSG_RX	Unrecognized messages received on the reporting trunk group.
ISUP_UPA_RX	User Part Acknowledgement messages received on the reporting trunk group.
ISUP_UPA_TX	User Part Acknowledgement messages sent on the reporting trunk group.
ISUP_UPT_RX	User Part Test messages received on the reporting trunk group.
ISUP_UPT_TX	User Part Test messages sent on the reporting trunk group.
ISUP_USR_RX	User To User messages received on the reporting trunk group.
ISUP_USR_TX	User To User messages sent on the reporting trunk group.

The following table illustrates the message measurements applicable to a given ISUP variant, the total message, abnormal release, unexpected and unrecognized message measurements that apply to all variants:

Table 6-25 Message Measurements Applicable to ISUP Variants

Message	ANSI	China	Mexico	Thailand	Hong-Kong	Chile	Australia	Israel	ETSIv2	Hungary	France	Poland
ACM	X	X	X	X	X	X	X	X	X	X	X	X
ANM	X	X	X	X	X	X	X	X	X	X	X	X
ARR				X								
BLA	X	X	X	X	X	X	X	X	X	X	X	X
BLO	X	X	X	X	X	X	X	X	X	X	X	X
CCL		X	X				X	X	X			
CCR	X	X	X	X		X	X	X	X	X	X	X
CFN	X		X	X	X					X	X	X
CGB	X	X	X	X	X	X	X	X	X	X	X	X
CGBA	X	X	X	X	X	X	X	X	X	X	X	X
CGU	X	X	X	X	X	X	X	X	X	X	X	X

Table 6-25 Message Measurements Applicable to ISUP Variants (continued)

CGUA	X	X	X	X	X	X	X	X	X	X	X	X
CON		X	X	X	X	X	X	X	X	X	X	X
COT	X	X	X	X	X	X	X	X	X	X	X	X
CPG	X	X	X	X	X	X	X	X	X	X	X	X
CQM	X		X	X								
CQR	X		X	X								
CRA	X											
CRM	X											
CRG						X						
CVR	X											
CVT	X											
EXM	X											
FAA									X	X	X	X
FAC	X				X					X	X	X
FAR						X						
FOT	X											
FRJ						X						
FWT						X						
GRA	X	X	X	X	X	X	X	X	X	X	X	X
GRS	X	X	X	X	X	X	X	X	X	X	X	X
IAM	X	X	X	X	X	X	X	X	X	X	X	X
IDR						X				X	X	X
INF	X		X	X	X	X				X	X	X
INR			X	X	X	X				X	X	X
IRS						X				X	X	X
ITX											X	X
LPA	X											
LPM						X						
NRM					X	X						
OLM										X	X	X
OPR		X					X	X	X			
PAM	X				X	X						
PRI						X						
REL	X	X	X	X	X	X	X	X	X	X	X	X
RES	X	X	X	X	X	X	X	X	X	X	X	X
RLC	X	X	X	X	X	X	X	X	X	X	X	X
RSC	X	X	X	X	X	X	X	X	X	X	X	X
SAM		X	X	X	X	X	X	X	X	X	X	X
SGM		X			X	X	X	X	X	X	X	X
SUS	X	X	X	X	X	X	X	X	X	X	X	X
TXA											X	X
UBA	X	X		X	X	X	X	X	X	X	X	X

Table 6-25 *Message Measurements Applicable to ISUP Variants (continued)*

UBL	X	X	X	X		X	X	X	X	X	X	X
UCIC	X		X	X		X						
UPA										X	X	X
UPT										X	X	X
USR	X					X				X	X	X

ISUP (ANSI) Measurements

Table 6-26 ISUP (ANSI) Measurements

Measurement	Description (* = rapid count could mean a potential problem in the system)
SGA_ABNORMAL_REL_RX	RELS received with a cause other than NORMAL on the reporting trunk group.
SGA_ACM_RX	ACM messages received on the reporting trunk group.
SGA_ACM_TX	ACM messages sent on the reporting trunk group.
SGA_ANM_RX	ANM messages received on the reporting trunk group.
SGA_ANM_TX	ANM messages sent on the reporting trunk group.
SGA_BLA_RX	BLA messages received on the reporting trunk group.
SGA_BLA_TX	BLA messages sent on the reporting trunk group.
SGA_BLO_RX	BLO messages received on the reporting trunk group.
SGA_BLO_TX	BLO messages sent on the reporting trunk group.
SGA_CCR_RX	CCR messages received on the reporting trunk group.
SGA_CCR_TX	CCR messages sent on the reporting trunk group.
SGA_CFN_RX	CFN messages received on the reporting trunk group.
SGA_CFN_TX	CFN messages sent on the reporting trunk group.
SGA_CGB_RX	CGB messages received on the reporting trunk group.
SGA_CGB_TX	CGB messages sent on the reporting trunk group.
SGA_CGBA_RX	CGBA messages received on the reporting trunk group.
SGA_CGBA_TX	CGBA messages sent on the reporting trunk group.
SGA_CGU_RX	CGU messages received on the reporting trunk group.
SGA_CGU_TX	CGU messages sent on the reporting trunk group.
SGA_CGUA_RX	CGUA messages received on the reporting trunk group.
SGA_CGUA_TX	CGUA messages sent on the reporting trunk group.
SGA_COT_RX	COT messages received on the reporting trunk group.
SGA_COT_TX	COT messages sent on the reporting trunk group.
SGA_CPG_RX	CPG messages received on the reporting trunk group.
SGA_CPG_TX	CPG messages sent on the reporting trunk group.
SGA_CQM_RX	CQM messages received on the reporting trunk group.
SGA_CQM_TX	CQM messages sent on the reporting trunk group.
SGA_CQR_RX	CQR messages received on the reporting trunk group.
SGA_CQR_TX	CQR messages sent on the reporting trunk group.
SGA_CRA_RX	CRA messages received on the reporting trunk group.
SGA_CRA_TX	CRA messages sent on the reporting trunk group.
SGA_CRM_RX	CRM messages received on the reporting trunk group.
SGA_CRM_TX	CRM messages sent on the reporting trunk group.
SGA_CVR_RX	CVR messages received on the reporting trunk group.

Table 6-26 ISUP (ANSI) Measurements (continued)

Measurement	Description (* = rapid count could mean a potential problem in the system)
SGA_CVR_TX	CVR messages sent on the reporting trunk group.
SGA_CVT_RX	CVT messages received on the reporting trunk group.
SGA_CVT_TX	CVT messages sent on the reporting trunk group.
SGA_EXM_RX	EXM messages received on the reporting trunk group.
SGA_EXM_TX	EXM messages sent on the reporting trunk group.
SGA_FAC_RX	FAC messages received on the reporting trunk group.
SGA_FAC_TX	FAC messages sent on the reporting trunk group.
SGA_FOT_RX	FOT messages received on the reporting trunk group.
SGA_FOT_TX	FOT messages sent on the reporting trunk group.
SGA_GRA_RX	GRA messages received on the reporting trunk group.
SGA_GRA_TX	GRA messages sent on the reporting trunk group.
SGA_GRS_RX	GRS messages received on the reporting trunk group.
SGA_GRS_TX	GRS messages sent on the reporting trunk group.
SGA_IAM_RX	IAM messages received on the reporting trunk group.
SGA_IAM_TX	IAM messages sent on the reporting trunk group.
SGA_INF_RX	INF messages received on the reporting trunk group.
SGA_INF_TX	INF messages sent on the reporting trunk group.
SGA_INR_RX	INR messages received on the reporting trunk group.
SGA_INR_TX	INR messages sent on the reporting trunk group.
SGA_LPA_RX	LPA messages received on the reporting trunk group.
SGA_LPA_TX	LPA messages sent on the reporting trunk group.
SGA_MSG_RX	messages received on the reporting trunk group.
SGA_MSG_TX	messages sent on the reporting trunk group.
SGA_PAM_RX	PAM messages received on the reporting trunk group.
SGA_PAM_TX	PAM messages sent on the reporting trunk group.
SGA_REL_RX	REL messages received on the reporting trunk group.
SGA_REL_TX	REL messages sent on the reporting trunk group.
SGA_RES_RX	RES messages received on the reporting trunk group.
SGA_RES_TX	RES messages sent on the reporting trunk group.
SGA_RLC_RX	RLC messages received on the reporting trunk group.
SGA_RLC_TX	RLC messages sent on the reporting trunk group.
SGA_RSC_RX	RSC messages received on the reporting trunk group.
SGA_RSC_TX	RSC messages sent on the reporting trunk group.
SGA_SUS_RX	SUS messages received on the reporting trunk group.
SGA_SUS_TX	SUS messages sent on the reporting trunk group.

Table 6-26 ISUP (ANSI) Measurements (continued)

Measurement	Description (* = rapid count could mean a potential problem in the system)
SGA_UBA_RX	UBA messages received on the reporting trunk group.
SGA_UBA_TX	UBA messages sent on the reporting trunk group.
SGA_UBL_RX	UBL messages received on the reporting trunk group.
SGA_UBL_TX	UBL messages sent on the reporting trunk group.
SGA_UCIC_RX	UCIC messages received on the reporting trunk group.
SGA_UCIC_TX	UCIC messages sent on the reporting trunk group.
SGA_UNEXPECT_MSG_RX	Unexpected messages received on the reporting trunk group.
SGA_UNRECOG_MSG_RX	Unrecognized messages received on the reporting trunk group.
SGA_USR_RX	USR messages received on the reporting trunk group.
SGA_USR_TX	USR messages sent on the reporting trunk group.

ISUP (France) Measurements

Table 6-27 ISUP (France) Measurements

Measurement	Description (* = rapid count could mean a potential problem in the system)
SGA_ITX_RX	Charge Unit (ITX) message received on the reporting trunk group.
SGA_ITX_TX	ITX messages sent on the reporting trunk group.
SGA_TXA_RX	Charging Acknowledgement (TXA) messages received on the reporting trunk group.
SGA_TXA_TX	TXA messages sent on the reporting trunk group.

ISUP (Poland) Measurements

Table 6-28 ISUP (Poland) Measurements

Measurement	Description (* = rapid count could mean a potential problem in the system)
SGA_CRG_RX	Charging Information messages received on the reporting trunk group.
SGA_CRG_TX	Charging Information messages transmitted on the reporting trunk group.

ISUP (ITU-China) Measurements

Table 6-29 ISUP (ITU-China) Measurements

Measurement	Description (* = rapid count could mean a potential problem in the system)
SGA_ABNORMAL_REL_RX	RELs received with a cause other than NORMAL on the reporting trunk group.
SGA_ABNORMAL_REL_TX	RELs sent with a cause other than NORMAL on the reporting trunk group.
SGA_ACM_RX	ACM messages received on the reporting trunk group.
SGA_ACM_TX	ACM messages sent on the reporting trunk group.
SGA_ANM_RX	ANM messages received on the reporting trunk group.
SGA_ANM_TX	ANM messages sent on the reporting trunk group.
SGA_BLA_RX	BLA messages received on the reporting trunk group.
SGA_BLA_TX	BLA messages sent on the reporting trunk group.
SGA_BLO_RX	BLO messages received on the reporting trunk group.
SGA_BLO_TX	BLO messages sent on the reporting trunk group.
SGA_CCL_RX	CCL messages received on the reporting trunk group.
SGA_CCL_TX	CCL messages sent on the reporting trunk group.
SGA_CCR_RX	CCR messages received on the reporting trunk group.
SGA_CCR_TX	CCR messages sent on the reporting trunk group.
SGA_CGB_RX	CGB messages received on the reporting trunk group.
SGA_CGB_TX	CGB messages sent on the reporting trunk group.

Table 6-29 ISUP (ITU-China) Measurements (continued)

Measurement	Description (* = rapid count could mean a potential problem in the system)
SGA_CGBA_RX	CGBA messages received on the reporting trunk group.
SGA_CGBA_TX	CGBA messages sent on the reporting trunk group.
SGA_CGU_RX	CGU messages received on the reporting trunk group.
SGA_CGU_TX	CGU messages sent on the reporting trunk group.
SGA_CGUA_RX	CGUA messages received on the reporting trunk group.
SGA_CGUA_TX	CGUA messages sent on the reporting trunk group.
SGA_CON_RX	CON messages received on the reporting trunk group.
SGA_CON_TX	CON messages sent on the reporting trunk group.
SGA_COT_RX	COT messages received on the reporting trunk group.
SGA_COT_TX	COT messages sent on the reporting trunk group.
SGA_CPG_RX	CPG messages received on the reporting trunk group.
SGA_CPG_TX	CPG messages sent on the reporting trunk group.
SGA_GRA_RX	GRA messages received on the reporting trunk group.
SGA_GRA_TX	GRA messages sent on the reporting trunk group.
SGA_GRS_RX	GRS messages received on the reporting trunk group.
SGA_GRS_TX	GRS messages sent on the reporting trunk group.
SGA_IAM_RX	IAM messages received on the reporting trunk group.
SGA_IAM_TX	IAM messages sent on the reporting trunk group.
SGA_MSG_RX	Messages received on the reporting trunk group.
SGA_MSG_TX	Messages sent on the reporting trunk group.
SGA_OPR_RX	OPR messages received on the reporting trunk group.
SGA_OPR_TX	OPR messages sent on the reporting trunk group.
SGA_REL_RX	REL messages received on the reporting trunk group.
SGA_REL_TX	REL messages sent on the reporting trunk group.
SGA_RES_RX	RES messages received on the reporting trunk group.
SGA_RES_TX	RES messages sent on the reporting trunk group.
SGA_RLC_RX	RLC messages received on the reporting trunk group.
SGA_RLC_TX	RLC messages sent on the reporting trunk group.
SGA_RSC_RX	RSC messages received on the reporting trunk group.
SGA_RSC_TX	RSC messages sent on the reporting trunk group.
SGA_SAM_RX	SAM messages received on the reporting trunk group.
SGA_SAM_TX	SAM messages sent on the reporting trunk group.
SGA_SGM_RX	SGM messages received on the reporting trunk group.
SGA_SGM_TX	SGM messages sent on the reporting trunk group.
SGA_SUS_RX	SUS messages received on the reporting trunk group.

Table 6-29 ISUP (ITU-China) Measurements (continued)

Measurement	Description (* = rapid count could mean a potential problem in the system)
SGA_SUS_TX	SUS messages sent on the reporting trunk group.
SGA_UBA_RX	UBA messages received on the reporting trunk group.
SGA_UBA_TX	UBA messages sent on the reporting trunk group.
SGA_UBL_RX	UBL messages received on the reporting trunk group.
SGA_UBL_TX	UBL messages sent on the reporting trunk group.
SGA_UNEXPECT_MSG_RX	Unexpected messages received on the reporting trunk group.
SGA_UNRECOG_MSG_RX	Unrecognized messages received on the reporting trunk group.

ISUP (ITU-Mexico) Measurements

Table 6-30 ISUP (ITU-Mexico) Measurements

Measurement	Description (* = rapid count could mean a potential problem in the system)
SGA_ABNORMAL_REL_RX	RELS received with a cause other than NORMAL on the reporting trunk group.
SGA_ABNORMAL_REL_TX	RELS sent with a cause other than NORMAL on the reporting trunk group.
SGA_ACM_RX	ACM messages received on the reporting trunk group.
SGA_ACM_TX	ACM messages sent on the reporting trunk group.
SGA_ANM_RX	ANM messages received on the reporting trunk group.
SGA_ANM_TX	ANM messages sent on the reporting trunk group.
SGA_BLA_RX	BLA messages received on the reporting trunk group.
SGA_BLA_TX	BLA messages sent on the reporting trunk group.
SGA_BLO_RX	BLO messages received on the reporting trunk group.
SGA_BLO_TX	BLO messages sent on the reporting trunk group.
SGA_CCL_RX	CCL messages sent on the reporting trunk group.
SGA_CCL_TX	CCL messages sent on the reporting trunk group.
SGA_CCR_RX	CCR messages received on the reporting trunk group.
SGA_CCR_TX	CCR messages sent on the reporting trunk group.
SGA_CFN_RX	CFN messages received on the reporting trunk group.
SGA_CFN_TX	CFN messages sent on the reporting trunk group.
SGA_CGB_RX	CGB messages received on the reporting trunk group.
SGA_CGB_TX	CGB messages sent on the reporting trunk group.
SGA_CGBA_RX	CGBA messages received on the reporting trunk group.
SGA_CGBA_TX	CGBA messages sent on the reporting trunk group.
SGA_CGU_RX	CGU messages received on the reporting trunk group.
SGA_CGU_TX	CGU messages sent on the reporting trunk group.
SGA_CGUA_RX	CGUA messages received on the reporting trunk group.
SGA_CGUA_TX	CGUA messages sent on the reporting trunk group.
SGA_CON_RX	CON messages received on the reporting trunk group.
SGA_CON_TX	CON messages sent on the reporting trunk group.
SGA_COT_RX	COT messages received on the reporting trunk group.
SGA_COT_TX	COT messages sent on the reporting trunk group.
SGA_CPG_RX	CPG messages received on the reporting trunk group.
SGA_CPG_TX	CPG messages sent on the reporting trunk group.
SGA_CQM_RX	CQM messages received on the reporting trunk group.
SGA_CQM_TX	CQM messages sent on the reporting trunk group.
SGA_CQR_RX	CQR messages received on the reporting trunk group.
SGA_CQR_TX	CQR messages sent on the reporting trunk group.

Table 6-30 ISUP (ITU-Mexico) Measurements (continued)

Measurement	Description (* = rapid count could mean a potential problem in the system)
SGA_GRA_RX	GRA messages received on the reporting trunk group.
SGA_GRA_TX	GRA messages sent on the reporting trunk group.
SGA_GRS_RX	GRS messages received on the reporting trunk group.
SGA_GRS_TX	GRS messages sent on the reporting trunk group.
SGA_IAM_RX	IAM messages received on the reporting trunk group.
SGA_IAM_TX	IAM messages sent on the reporting trunk group.
SGA_INF_RX	INF messages received on the reporting trunk group.
SGA_INF_TX	INF messages sent on the reporting trunk group.
SGA_INR_RX	INR messages received on the reporting trunk group.
SGA_INR_TX	INR messages sent on the reporting trunk group.
SGA_MSG_RX	Messages received on the reporting trunk group.
SGA_MSG_TX	Messages sent on the reporting trunk group.
SGA_REL_RX	REL messages received on the reporting trunk group.
SGA_REL_TX	REL messages sent on the reporting trunk group.
SGA_RES_RX	RES messages received on the reporting trunk group.
SGA_RES_TX	RES messages sent on the reporting trunk group.
SGA_RLC_RX	RLC messages received on the reporting trunk group.
SGA_RLC_TX	RLC messages sent on the reporting trunk group.
SGA_RSC_RX	RSC messages received on the reporting trunk group.
SGA_RSC_TX	RSC messages sent on the reporting trunk group.
SGA_SAM_RX	SAM messages received on the reporting trunk group.
SGA_SAM_TX	SAM messages sent on the reporting trunk group.
SGA_SUS_RX	SUS messages received on the reporting trunk group.
SGA_SUS_TX	SUS messages sent on the reporting trunk group.
SGA_UBA_RX	UBA messages received on the reporting trunk group.
SGA_UBA_TX	UBA messages sent on the reporting trunk group.
SGA_UBL_RX	UBL messages received on the reporting trunk group.
SGA_UBL_TX	UBL messages sent on the reporting trunk group.
SGA_UCIC_RX	UCIC messages received on the reporting trunk group.
SGA_UCIC_TX	UCIC messages sent on the reporting trunk group.
SGA_UNEXPECT_MSG_RX	Unexpected messages received on the reporting trunk group.
SGA_UNRECOG_MSG_RX	Unrecognized messages received on the reporting trunk group.

ISUP (ITU-HongKong) Measurements

Table 6-31 ISUP (ITU-HongKong) Measurements

Measurement	Description (* = rapid count could mean a potential problem in the system)
SGA_ABNORMAL_REL_RX	RELS received with a cause other than NORMAL on the reporting trunk group.
SGA_ABNORMAL_REL_TX	RELS sent with a cause other than NORMAL on the reporting trunk group.
SGA_ACM_RX	ACM messages received on the reporting trunk group.
SGA_ACM_TX	ACM messages sent on the reporting trunk group.
SGA_ANM_RX	ANM messages received on the reporting trunk group.
SGA_ANM_TX	ANM messages sent on the reporting trunk group.
SGA_BLA_RX	BLA messages received on the reporting trunk group.
SGA_BLA_TX	BLA messages sent on the reporting trunk group.
SGA_BLO_RX	BLO messages received on the reporting trunk group.
SGA_BLO_TX	BLO messages sent on the reporting trunk group.
SGA_CFN_RX	CFN messages received on the reporting trunk group.
SGA_CFN_TX	CFN messages sent on the reporting trunk group.
SGA_CGB_RX	CGB messages received on the reporting trunk group.
SGA_CGB_TX	CGB messages sent on the reporting trunk group.
SGA_CGBA_RX	CGBA messages received on the reporting trunk group.
SGA_CGBA_TX	CGBA messages sent on the reporting trunk group.
SGA_CGU_RX	CGU messages received on the reporting trunk group.
SGA_CGU_TX	CGU messages sent on the reporting trunk group.
SGA_CGUA_RX	CGUA messages received on the reporting trunk group.
SGA_CGUA_TX	CGUA messages sent on the reporting trunk group.
SGA_CON_RX	CON messages received on the reporting trunk group.
SGA_CON_TX	CON messages sent on the reporting trunk group.
SGA_COT_RX	COT messages received on the reporting trunk group.
SGA_COT_TX	COT messages sent on the reporting trunk group.
SGA_CPG_RX	CPG messages received on the reporting trunk group.
SGA_CPG_TX	CPG messages sent on the reporting trunk group.
SGA_FAC_RX	FAC messages received on the reporting trunk group.
SGA_FAC_TX	FAC messages sent on the reporting trunk group.
SGA_GRA_RX	GRA messages received on the reporting trunk group.
SGA_GRA_TX	GRA messages sent on the reporting trunk group.
SGA_GRS_RX	GRS messages received on the reporting trunk group.
SGA_GRS_TX	GRS messages sent on the reporting trunk group.
SGA_IAM_RX	IAM messages received on the reporting trunk group.
SGA_IAM_TX	IAM messages sent on the reporting trunk group.

Table 6-31 ISUP (ITU-HongKong) Measurements

Measurement	Description (* = rapid count could mean a potential problem in the system)
SGA_INF_RX	INF messages received on the reporting trunk group.
SGA_INF_TX	INF messages sent on the reporting trunk group.
SGA_INR_RX	INR messages received on the reporting trunk group.
SGA_INR_TX	INR messages sent on the reporting trunk group.
SGA_MSG_RX	Messages received on the reporting trunk group.
SGA_MSG_TX	Messages sent on the reporting trunk group.
SGA_NRM_RX	NRM messages received on the reporting trunk group.
SGA_NRM_TX	NRM messages sent on the reporting trunk group.
SGA_PAM_RX	PAM messages received on the reporting trunk group.
SGA_PAM_TX	PAM messages sent on the reporting trunk group.
SGA_REL_RX	REL messages received on the reporting trunk group.
SGA_REL_TX	REL messages sent on the reporting trunk group.
SGA_RES_RX	RES messages received on the reporting trunk group.
SGA_RES_TX	RES messages sent on the reporting trunk group.
SGA_RLC_RX	RLC messages received on the reporting trunk group.
SGA_RLC_TX	RLC messages sent on the reporting trunk group.
SGA_RSC_RX	RSC messages received on the reporting trunk group.
SGA_RSC_TX	RSC messages sent on the reporting trunk group.
SGA_SAM_RX	SAM messages received on the reporting trunk group.
SGA_SAM_TX	SAM messages sent on the reporting trunk group.
SGA_SGM_RX	SGM messages received on the reporting trunk group.
SGA_SGM_TX	SGM messages sent on the reporting trunk group.
SGA_SUS_RX	SUS messages received on the reporting trunk group.
SGA_SUS_TX	SUS messages sent on the reporting trunk group.
SGA_UBA_RX	UBA messages received on the reporting trunk group.
SGA_UBA_TX	UBA messages sent on the reporting trunk group.
SGA_UNEXPECT_MSG_RX	Unexpected messages received on the reporting trunk group.
SGA_UNRECOG_MSG_RX	Unrecognized messages received on the reporting trunk group.

Audit Measurements

Table 6-32 Audit Measurements

Measurement	Description (* = rapid count could mean a potential problem in the system)
AUDIT_FS_TOTAL_CA_SWITCHOVER	Audits to check all active CCBs in response to a CA platform switchover occurring. This is only applicable when the standby CA becomes active.
AUDIT_FS_TOTAL_SIP_NOACK_TMO	CCB audits initiated due to a SIP Invite that was not acknowledged that is detected by the reporting FS.
AUDIT_FS_TOTAL_SIP_RESP_TMO	CCB audits initiated due to a SIP Request that has timed out that is detected by the reporting FS.
AUDIT_SS7_LONG_DUR_EXCEEDED	SS7 calls that exceeded the long duration threshold on the reporting trunk group.
AUDIT_SS7_TRUNK_STATE_SYNCED	SS7 trunks that had their local and remote states synchronized on the reporting trunk group.
QOS_GATE_AUDIT_FREED	Dangling Gate IDX memory entries detected and freed by audit by the reporting BTS.

SIP Interface Adapter Measurements

Table 6-33 SIP Interface Adapter Measurements

Measurement	Description (* = rapid count could mean a potential problem in the system)
SIA_AUDIT_BCM_CALL_RELEASED	Calls released when the SIP side is inactive.
SIA_AUDIT_CALL_RELEASED	SIP side calls released due to the SIA memory audit when the BCM side of the call is already released.
SIA_AUDIT_CCB_FREED	Call Control Blocks freed due to the SIA audit.
SIA_AUDIT_REGCONTACT_FREED	SIP Registration Contacts freed as a result of the SIA Memory Audit.
SIA_CALL_FAIL_BY_EXPIRED_REG	Call failures due to a registration expiration.
SIA_INCOM_CALL_ABDN	Incoming calls abandoned at the reporting CA.
SIA_INCOM_CALL_NOT_ANS	Incoming calls not answered by Called party at reporting CA.
SIA_INCOM_END_USR_BUSY	Incoming calls not completed because the end user is busy.
SIA_INCOM_FAIL	Failed incoming SIP calls.
SIA_INCOM_INIT	Incoming SIP call initializations.
SIA_INCOM_SUCC	Successful incoming SIP calls.
SIA_INVITE_NO_CALL_TO_REPLACE	“INVITE” SIP messages with “Replaces” header. Calls are rejected because the “replaces” call ID is not found.
SIA_KPML_SUBSCRIBE_RX	KPML SIP SUBSCRIBE messages received.
SIA_KPML_NOTIFY_RX	KPML SIP NOTIFY messages received.
SIA_KPML_NOTIFY_TX	KPML SIP NOTIFY messages sent to SIP phones.
SIA_KPML_SUBSCRIBE_TX	KPML SIP SUBSCRIBE messages sent out by the CA.

Table 6-33 SIP Interface Adapter Measurements (continued)

Measurement	Description (* = rapid count could mean a potential problem in the system)
SIA_MWI_NOTIFY_RX	SIP Notify MWIs received from SIP subscribers.
SIA_MWI_NOTIFY_TX	SIP Notify MWIs sent to SIP phones.
SIA_MWI_NOTIFY_TX_FAIL	SIP Notify MWIs that failed to be sent to SIP phones.
SIA_OC_INVITE_REJECT	Incoming INVITE messages rejected due to an overload.
SIA_OC_REFERER_REJECT	Incoming REFER messages rejected due to an overload.
SIA_OC_REGISTER_REJECT	Incoming REGISTER messages rejected due to an overload.
SIA_OC_RX_OPTIONS_REJECT	Incoming OPTIONS requests rejected due to an overload.
SIA_OC_SUBSCRIBE_REJECT	Incoming SUBSCRIBE messages rejected due to an overload.
SIA_OC_UN SOL_NOTIFY_SUPP	Incoming unsolicited notification requests suppressed without sending to the endpoints due to an overload.
SIA_OUTG_CALL_ABDN	Outgoing calls abandoned at the reporting CA.
SIA_OUTG_CALL_NOT_ANS	Outgoing calls not answered by Called party at reporting CA.
SIA_OUTG_END_USR_BUSY	Outgoing calls not completed because the end user is busy.
SIA_OUTG_FAIL	Failed outgoing SIP calls.
SIA_OUTG_INIT	Outgoing SIP call initializations.
SIA_OUTG_SUCC	Successful outgoing SIP calls.
SIA_REFERER_TO_TRUNK_ATTENDED_RX	Calls that receive “Refer” which replaces the call ID (attended transfer) with “Refer-to” to domains that are BTS trunks. The SIA_REFERER_TO_TRUNK_RX measurement is incremented as well as this measurement.
SIA_REFERER_TO_TRUNK_RX	Tracks “Refer” with “Refer-to” via domains defined as BTS trunks
SIA_REFERER_TO_UNKNOWN_DOMAIN_RX	Tracks “Refer” with “Refer-to” via domains neither a BTS service domain nor a trunk.
SIA_REFRESHES_TX	SIP message refreshes that occurred.
SIA_SECURE_FQDN_VIOLATION_REQ	Times that a SIP request fails the validation for a secure SIP endpoint.
SIA_SECURE_FQDN_VIOLATION_RESP	Times that a SIP response fails the validation for a secure SIP endpoint.
SIA_TOTAL_FAIL	Unsuccessfully completed SIP calls on the reporting CA (DEPRECATED - always will contain a value of ZERO).
SIA_TOTAL_INCOM_MSG_FAIL	Incoming SIP message attempts not successfully received (DEPRECATED - always will contain a value of ZERO).
SIA_TOTAL_OUTG_MSG_FAIL	Outgoing SIP message attempts not successfully transmitted (DEPRECATED - always will contain a value of ZERO).
SIA_TOTAL_SESS_TIMER_FAIL	Call failures due to session timer expiry that occurred.
SIA_TOTAL_SUCC	Successfully completed SIP calls on the reporting CA (DEPRECATED - always will contain a value of ZERO).

Call Detail Block Measurements

Table 6-34 Call Detail Block Measurements

Measurement	Description (* = rapid count could mean a potential problem in the system)
BILLING_TOTAL_500	CDBs of type 500 created by the reporting EMS.
BILLING_TOTAL_700	CDBs of type 700 created by the reporting EMS.
BILLING_TOTAL_900	CDBs of type 900 created by the reporting EMS.
BILLING_TOTAL_976	CDBs of type 976 created by the reporting EMS.
BILLING_TOTAL_AIRLINES	CDBs of type Airlines created by the reporting EMS.
BILLING_TOTAL_AMBULANCE	CDBs of type ambulance created by the reporting EMS.
BILLING_TOTAL_ATTENDANT	CDBs of type attendant created by the reporting EMS.
BILLING_TOTAL_BLV	CDBs of type busy line verification created by the reporting EMS.
BILLING_TOTAL_BUSINESS	CDBs of type business created by the reporting EMS.
BILLING_TOTAL_CARRIER_OP	CDBs of type carrier operator created by the reporting EMS.
BILLING_TOTAL_CNA	CDBs of type Calling Number Announcement created by the reporting EMS.
BILLING_TOTAL_CUT_THRU	CDBs of type cut thru created by the reporting EMS.
BILLING_TOTAL_DA	CDBs of type directory assistance created by the reporting EMS.
BILLING_TOTAL_DA_INTER	CDBs of type Directory Assistance Interlata created by the reporting EMS.
BILLING_TOTAL_DA_INTL	CDBs of type Directory Assistance International created by the reporting EMS.
BILLING_TOTAL_DA_TOLL	CDBs of type directory assistance toll created by the reporting EMS.
BILLING_TOTAL_EMG	CDBs of type emergency created by the reporting EMS.
BILLING_TOTAL_EXTENSION	CDBs of type extension created by the reporting EMS.
BILLING_TOTAL_FIRE	CDBs of type fire created by the reporting EMS.
BILLING_TOTAL_INFO	CDBs of type information (i.e. 976 calls) created by the reporting EMS.
BILLING_TOTAL_INTERLATA	CDBs of type interlata created by the reporting EMS.
BILLING_TOTAL_INTL	CDBs of type international created by the reporting EMS.
BILLING_TOTAL_INTL_OPR	CDBs of type International Operator created by the reporting EMS.
BILLING_TOTAL_INTL_WZ1	CDBs of type International World Zone 1 created by the reporting EMS.
BILLING_TOTAL_INVALID	CDBs of type invalid created by the reporting EMS.
BILLING_TOTAL_LOCAL	CDBs of type local created by the reporting EMS.
BILLING_TOTAL_LRN	CDBs of type LRN created by the reporting EMS.
BILLING_TOTAL_MOBILE	CDBs of type Mobile created by the reporting EMS.
BILLING_TOTAL_NAS	CDBs of type NAS created by the reporting EMS.
BILLING_TOTAL_NAT_OPR	CDBs of type National Operator created by the reporting EMS.
BILLING_TOTAL_NATIONAL	CDBs of type national (NANP) created by the reporting EMS.
BILLING_TOTAL_NON_EMG	CDBs of type non-emergency created by the reporting EMS.
BILLING_TOTAL_NONE	CDBs of type none created by the reporting EMS.
BILLING_TOTAL_NULL	CDBs of type "null" (non-routed calls) created by the reporting EMS.

Table 6-34 Call Detail Block Measurements (continued)

Measurement	Description (* = rapid count could mean a potential problem in the system)
BILLING_TOTAL_OP	CDBs of type cut operator created by the reporting EMS
BILLING_TOTAL_OP_ASSIST	CDBs of type operator assisted created by the reporting EMS
BILLING_TOTAL_PCS	CDBs of type pcs created by the reporting EMS.
BILLING_TOTAL_POLICE	CDBs of type police created by the reporting EMS
BILLING_TOTAL_PREMIUM	CDBs of type premium (i.e. 900 calls) created by the reporting EMS
BILLING_TOTAL_RAILWAYS	CDBs of type Railways created by the reporting EMS.
BILLING_TOTAL_RELAY	CDBs of type relay created by the reporting EMS.
BILLING_TOTAL_REPAIR	CDBs of type repair created by the reporting EMS.
BILLING_TOTAL_SPEED_DIAL	CDBs of type speed dial created by the reporting EMS
BILLING_TOTAL_SVC_CODE	CDBs of type Service Code created by the reporting EMS.
BILLING_TOTAL_TANDEM	CDBs of type tandem created by the reporting EMS.
BILLING_TOTAL_TEST	CDBs of type test call created by the reporting EMS - this includes all subtypes of test calls performed by the CA.
BILLING_TOTAL_TEST	Calls of the network loopback test type (based on the CALL-TYPE field in the destination table).
BILLING_TOTAL_TIME	CDBs of type time created by the reporting EMS.
BILLING_TOTAL_TOLL	CDBs of type toll created by the reporting EMS.
BILLING_TOTAL_TOLL_FREE	CDBs of type toll free created by the reporting EMS.
BILLING_TOTAL_TRAFFIC	CDBs of type traffic created by the reporting EMS.
BILLING_TOTAL_TW	CDBs of type time and weather created by the reporting EMS
BILLING_TOTAL_UAN	CDBs of type Universal Access Number created by the reporting EMS.
BILLING_TOTAL_VACANT	CDBs of type vacant created by the reporting EMS.
BILLING_TOTAL_WEATHER	CDBs of type weather created by the reporting EMS.
CALLP_NCT_TEST_FAIL	CDBs of test calls of the “network continuity” type that are abnormally released by the BTS (due to reasons such as resource priority should be given to regular calls).
CALLP_NCT_TEST_SUCC	CDBs of type test calls of type “network continuity” created by the reporting EMS.
CALLP_NLB_TEST_FAIL	CDBs of test calls of the “network loopback” type that are abnormally released by the BTS (due to reasons such as resource priority should be given to regular calls).
CALLP_NLB_TEST_SUCC	CDBs of test calls of the “network loopback” type created by the reporting EMS.
CALLP-LB-TEST-SUCC	CDBs of test calls of the “TDM loop back 108 test” type created by the reporting EMS.
CALLP-TEST-ROUTE-SUCC	CDBs of test calls of the “TDM loop back 108 test” type and the DN dialed out in an outgoing message.

Event Messaging Measurements

Table 6-35 Event Messaging Measurements

Measurement	Description (*= rapid count could mean a potential problem in the system)
BILLING_EM_ACKED	Event messages acknowledged by the Record Keeping System.
BILLING_EM_LOGGED	Event messages written to disk but not sent to any RKS.
BILLING_EM_RETRANS	Event messages transmitted to an alternate RKS due to a lack of response from a previously tried RKS, excluding retries. The measurement is incremented when an event message is first sent to an alternate RKS. Any retries that occur at the RADIUS stack level (as provisioned in the “radius-profile” table) will not be included in this count.

Dynamic QoS Measurements

Table 6-36 Dynamic QoS Measurements

Measurement	Description (*= rapid count could mean a potential problem in the system)
DQOS_CONFIG_INFO_ATT MP	Configuration Info message attempts from the reporting CMS to the specified CMTS.
DQOS_CONFIG_INFO_SU CC	Configuration Acknowledgement messages received by the reporting CMS from the specified CMTS.
DQOS_CONFIG_UPDATE	Configuration Update messages received by the reporting CMS from the specified CMTS.
DQOS_GATE_OPEN_RX	DQOS Gate-Open messages received by the reporting BTS.
DQOS_GATE_CLOSE_RX	DQOS Gate-Closed messages received by the reporting BTS.
DQOS_GATE_DELETE_TX	DQOS Gate-Delete messages sent from the reporting BTS.
DQOS_GATE_DELETE_AC K_RX	DQOS Gate-Delete-Ack messages received by the reporting BTS.
DQOS_GATE_DELETE_ER R_RX	DQOS Gate-Delete-Err messages received by the reporting BTS.
DQOS_GATE_SET_TX	DQOS Gate-Set messages sent from the reporting BTS.
DQOS_GATE_SET_ACK_R X	DQOS Gate-Set-Ack messages received by the reporting BTS.
DQOS_GATE_SET_ERR_R X	DQOS Gate-Set-Err messages received by the reporting BTS.
DQOS_GATE_INFO_TX	DQOS Gate-Info messages sent from the reporting BTS.
DQOS_GATE_INFO_ACK_ RX	DQOS Gate-Info-Ack messages received by the reporting BTS.
DQOS_GATE_INFO_ERR_ RX	DQOS Gate-Info-Err messages received by the reporting BTS.

PCMM Measurements

Table 6-37 PCMM Measurements

Measurement	Description (*= rapid count could mean a potential problem in the system)
PCMM_GATE_INFO_TX	PCMM Gate-Info messages sent from the reporting BTS.
PCMM_GATE_INFO_ACK_RX	PCMM Gate-Info-Ack messages received by the reporting BTS.
PCMM_GATE_INFO_ERR_RX	PCMM Gate-Info-Err messages received by the reporting BTS.
PCMM_GATE_OPEN_RX	PCMM Gate-Open messages received by the reporting BTS.
PCMM_GATE_CLOSED_RX	PCMM Gate-Closed messages received by the reporting BTS.
PCMM_GATE_DELETE_TX	PCMM Gate-Delete messages sent from the reporting BTS.
PCMM_GATE_DELETE_ACK_RX	PCMM Gate-Delete-Ack messages received by the reporting BTS.
PCMM_GATE_DELETE_ERR_RX	PCMM Gate-Delete-Err messages received by the reporting BTS.
PCMM_GATE_SET_TX	PCMM Gate-Set messages sent from the reporting BTS.
PCMM_GATE_REPORT_DELETE_RX	PCMM Gate-Report-Delete messages received by the reporting BTS.

SNMP Protocol Measurements

Table 6-38 SNMP Protocol Measurements

Measurement	Description (*= rapid count could mean a potential problem in the system)
SNMP_TRAP_TX	SNMP TRAPs generated by the reporting EMS.
SNMP_SET_RX	SNMP SETs received by the reporting EMS.
SNMP_SET_TX	SNMP SETs transmitted by the reporting EMS.
SNMP_GET_RX	SNMP GETs received by the reporting EMS.
SNMP_GET_TX	SNMP GETs transmitted by the reporting EMS.
SNMP_GET_NEXT_RX	SNMP GET NEXTs received by the reporting EMS.
SNMP_GET_NEXT_TX	SNMP GET NEXTs transmitted by the reporting EMS.

Trunk Group Usage Measurements

Table 6-39 Trunk Group Usage Measurements

Measurement	Description (*= rapid count could mean a potential problem in the system)
TRKGRP_401S_SENT	
TRKGRP_AVERAGE_USAGE	The percent of the trunk group used, between 0-100. This is not incremented for SIP or H323 trunk groups. $\text{TRKGRP_AVERAGE_USAGE} = 100 * (\text{TRKGRP_TOTAL_USAGE} * (100/60)) / (\text{TRKGRP_TOTAL_TRK} * \text{STATISTICS_INTERVAL_MINUTES})$
TRKGRP_EXCHANGE	The CLLI code from the POP table of the reporting trunk group.
TRKGRP_GLARE_COUNT	Attempts by the local and remote switch to use the same CIC on a 2-way trunk group. When glare is enmeasuremented and pegged here, the TRKGRP_OUTGOING_ATTMP measurement is NOT pegged. This is not incremented for SIP or H323 trunk groups.
TRKGRP_ID	The ID number of the reporting trunk group.
TRKGRP_INBOUND_FAIL	Number of failed inbound calls on a SIP trunk. However, calls that fail for Abandon, User busy, or No answer scenarios are not pegged.
TRKGRP_INBOUND_SUCC	Number of established inbound calls on a SIP trunk.
TRKGRP_INCOM_ATTMP	Times the system recognizes an incoming seizure for any trunk within the reporting trunk group: <ul style="list-style-type: none"> • In the case of a SIP trunk, this is incremented for every Invite received on a trunk. • In the case of an H.323 trunk, this is incremented for each Incoming Setup received on a trunk when not associated with a H.323 subscriber.
TRKGRP_INCOM_BUSY_TRK	Summation (CCS based) of trunk circuits within the reporting trunk group marked as busy with terminating calls taken every 100 seconds during the interval. This is not incremented for SIP or H323 trunk groups.
TRKGRP_INCOM_CALL_ABDN	Number of incoming abandoned SIP trunk calls at the reporting call agent. For SIP trunks only.
TRKGRP_INCOM_CALL_NOT_ANS	Number of incoming SIP trunk calls not answered by a called party. For SIP trunks only.
TRKGRP_INCOM_END_USR_BUSY	Number of incoming SIP trunk calls not completed because the called party was busy. For SIP trunks only.
TRKGRP_INCOM_USAGE	Summation (CCS based) of trunk circuits within the reporting trunk group marked as busy or in the maintenance state with terminating calls taken every 100 seconds during the interval. This is mapped to the same value as the TRKGRP_INCOM_BUSY_TRK in this release. This will be re-implemented to account for the MAINT state in a later release.
TRKGRP_LBLK_TRK_USAGE	The CCS value for trunks that are Local Blocked in the reporting trunk group for this reporting period. This is not incremented for SIP or H323 trunk groups.
TRKGRP_NAME	The remote switch CLLI code and trunk group type of the reporting trunk group.
TRKGRP_OOS_TRK_USAGE	The CCS value for OOS trunks in the trunk group for this period. This is not incremented for SIP or H323 trunk groups.

Table 6-39 Trunk Group Usage Measurements (continued)

Measurement	Description (*= rapid count could mean a potential problem in the system)
TRKGRP_OUTBOUND_FAIL	<p>Times the system tries to access any trunk for an outbound call unsuccessfully within the reporting trunk group:</p> <ul style="list-style-type: none"> In the case of a SIP trunk, this is incremented for each outgoing initial Invite request failure over a SIP trunk. For each failure response received over a trunk for any other failure causing failure of the outbound call setup. If an Invite is cancelled, the measurement for failure is not incremented as this includes just an outbound call. This counter does not include the following types of SIP calls: Abandon, User busy, No answer. In the case of an H.323 trunk, this is incremented for each Outgoing Setup sent on a trunk that failed when not associated with a H.323 subscriber.
TRKGRP_OUTBOUND_SUCC	Number of established outbound calls on a SIP trunk.
TRKGRP_OUTG_ATTMP	<p>Times the system tries to access any trunk for an outbound call within the reporting trunk group:</p> <ul style="list-style-type: none"> In the case of a SIP trunk, this is incremented for each received SetupReq request for a SIP trunk. In the case of an H.323 trunk, this is incremented for each Outgoing Setup sent on a trunk when not associated with a H.323 subscriber.
TRKGRP_OUTG_BUSY_TRK	Summation (CCS based) of trunk circuits within the reporting trunk group marked as busy with originating calls taken every 100 seconds during the interval. This is not incremented for SIP or H323 trunk groups.
TRKGRP_OUTG_CALL_ABDN	<p>Number of outgoing abandoned SIP trunk calls at the reporting call agent.</p> <p>For SIP trunks only.</p>
TRKGRP_OUTG_CALL_NOT_ANS	<p>Number of outgoing SIP trunk calls not answered by a called party.</p> <p>For SIP trunks only.</p>
TRKGRP_OUTG_END_USR_BUSY	<p>Number of SIP trunk calls not completed because the called party was busy.</p> <p>For SIP trunks only.</p>
TRKGRP_OUTG_USAGE	<p>Summation (CCS based) of trunk circuits within the reporting trunk group marked as busy or in the maintenance state with originating calls taken every 100 seconds during the interval.</p> <p>This is mapped to the same value as the TRKGRP_OUTG_BUSY_TRK in this release. This will be re-implemented to account for the MAINT state in a later release.</p>
TRKGRP_RBLK_TRK_USAGE	The CCS value for trunks that are Remote Blocked in the reporting trunk group for this reporting period. This is not incremented for SIP or H323 trunk groups.
TRKGRP_REGISTERS_RECVD	
TRKGRP_SIP_3xx_RX	Number of 3xx class (REDIRECTION) messages the reporting call agent received on a SIP trunk group.
TRKGRP_SIP_3xx_TX	Number of 3xx class (REDIRECTION) messages the reporting call agent transmitted on a SIP trunk group.
TRKGRP_SIP_4xx_RX	Number of 4xx class (REQUEST FAILURES) messages the reporting call agent received on a SIP trunk group.

Table 6-39 Trunk Group Usage Measurements (continued)

Measurement	Description (*= rapid count could mean a potential problem in the system)
TRKGRP_SIP_4xx_TX	Number of 4xx class (REQUEST FAILURES) messages the reporting call agent transmitted on a SIP trunk group.
TRKGRP_SIP_5xx_RX	Number of 5xx class (SERVER FAILURES) messages the reporting call agent received on a SIP trunk group.
TRKGRP_SIP_5xx_TX	Number of 5xx class (SERVER FAILURES) messages the reporting call agent transmitted on a SIP trunk group.
TRKGRP_SIP_6xx_RX	Number of 6xx class (GLOBAL FAILURES) messages the reporting call agent received on a SIP trunk group.
TRKGRP_SIP_6xx_TX	Number of 6xx class (GLOBAL FAILURES) messages the reporting call agent transmitted on a SIP trunk group.
TRKGRP_TOTAL_INS_TRK	The CCS value for trunks with a status of INS in the reporting trunk group. This is not incremented for SIP or H323 trunk groups.
TRKGRP_TOTAL_OOS_TRK	A total of the following types of OOS trunks in a trunk group: <ul style="list-style-type: none"> • TRKGRP_UEQP_TRK_USAGE • TRKGRP_LBLK_TRK_USAGE—this includes trunks in the administrative states of MAINT and OOS This is not incremented for SIP or H323 trunk groups.
TRKGRP_TOTAL_OVERFLOW	Outbound trunk call attempt failures due to all trunks within the reporting trunk group being in a busy state. This is not incremented for SIP or H.323 trunk groups.
TRKGRP_TOTAL_TRK	Trunks within the reporting trunk group.
TRKGRP_TOTAL_USAGE	Summation (CCS based) of the incoming usage and the outgoing usage measurements for the reporting trunk group. This is not incremented for SIP or H323 trunk groups.
TRKGRP_TYPE	The signaling type of the reporting trunk group.
TRKGRP_UEQP_TRK_USAGE	The CCS value for trunks that are UEQP, in the reporting trunk group for this reporting period. This is not incremented for SIP or H323 trunk groups.

Announcement Measurements

Table 6-40 *Announcement Measurements*

Measurement	Description (* = rapid count could mean a potential problem in the system)
ANM_SEASONAL_SUSPEND	calls that cause the CA to play the seasonal suspend announcement.
ANM_CKT_UNAVAIL	calls resulting in the playing of the circuit unavailable announcement
ANM_CALL_REJECTED	calls resulting in the playing of the call rejected announcement
ANM_ADDR_INCOMPLETE	calls resulting in the playing of the address incomplete announcement
ANM_FAC_REJECTED	calls resulting in the playing of the facility rejected announcement
ANM_PRE_0_1_ABSENT	calls resulting in the playing of the prefix of 0 or 1 absent announcement
ANM_PRE_0_1_PRESENT	calls resulting in the playing of the prefix 0 or 1 present announcement
ANM_HNPA_ABSENT	calls resulting in the playing of the HNPA area code announcement
ANM_NO_ROUTE_DEST	calls resulting in the playing of the no route to destination announcement
ANM_UNALLOCATED_NUM	calls resulting in the playing of the unallocated directory number announcement
ANM_NUM_CHANGED	calls resulting in the playing of the directory number changed announcement
ANM_DEST_OUTOFORDER	calls resulting in the playing of the destination out of order announcement
ANM_TEMP_DISCONNECT	calls resulting in the playing of the temporarily disconnected announcement
ANM_FEAT_NOT_SUBS	calls resulting in the playing of the feature not subscribed to announcement
ANM_AUTHCODE_INVALID	calls resulting in the playing of the authorization code invalid announcement
ANM_NO_RTE_TRANSITNW	calls resulting in the playing of the no route to specified network announcement
ANM_CAUSE_UNKNOWN	calls resulting in the playing of the cause unknown announcement
ANM_EMG_CKT_UNAVAIL	calls resulting in the playing of the “No Emergency Circuit Available” announcement.

H.323 Protocol Measurements

Table 6-41 *H.323 Protocol Measurements*

Measurement	Description (* = rapid count could mean a potential problem in the system)
H323_SETUP_RX	H323 SETUPs received
H323_SETUP_TX	H323 SETUPs transmitted
H323_SETUP_FAIL	H323 SETUPs that failed. The failure is due to one of the following scenarios: unable to send due to full socket queue, unable to compose message due to invalid socket, or lack of available memory.
H323_CONNECT_RX	H323 CONNECTs received
H323_CONNECT_TX	H323 CONNECTs transmitted
H323_CONNECT_FAIL	H323 CONNECT CONFIRMS that failed. The failure is due to one of the following scenarios: unable to send due to full socket queue, unable to compose message due to invalid socket, or lack of available memory.
H323_ALERT_RX	H323 ALERTs received

Table 6-41 H.323 Protocol Measurements (continued)

Measurement	Description (*= rapid count could mean a potential problem in the system)
H323_ALERT_TX	H323 ALERTs transmitted
H323_ALERT_FAIL	H323 ALERTs that failed. The failure is due to one of the following scenarios: unable to send due to full socket queue, unable to compose message due to invalid socket, or lack of available memory.
H323_IN_PROGRESS_RX	H323 IN PROGRESSs received
H323_IN_PROGRESS_TX	H323 IN PROGRESSs transmitted
H323_IN_PROGRESS_FAIL	H323 IN PROGRESSs that failed. The failure is due to one of the following scenarios: unable to send due to full socket queue, unable to compose message due to invalid socket, or lack of available memory.
H323_CALL_PROCEEDING_RX	H323 CALL PROCEEDINGs received
H323_CALL_PROCEEDING_TX	H323 CALL PROCEEDINGs transmitted
H323_CALL_PROCEEDING_FAIL	H323 CALL PROCEEDINGs that failed. The failure is due to one of the following scenarios: unable to send due to full socket queue, unable to compose message due to invalid socket, or lack of available memory.
H323_RELEASE_COMPLETE_RX	H323 RELEASEs received
H323_RELEASE_COMPLETE_TX	H323 RELEASEs transmitted
H323_RELEASE_COMPLETE_FAIL	H323 RELEASEs that failed. The failure is due to one of the following scenarios: unable to send due to full socket queue, unable to compose message due to invalid socket, or lack of available memory.
H323_REJECT_RX	H323 REJECTs received
H323_REJECT_TX	H323 REJECTs transmitted
H323_REJECT_FAIL	H323 REJECTs that failed. The failure is due to one of the following scenarios: unable to send due to full socket queue, unable to compose message due to invalid socket, or lack of available memory.
H323_INFORMATION_RX	H323 INFOs received
H323_INFORMATION_TX	H323 INFOs transmitted
H323_INFORMATION_FAIL	H323 INFOs that failed. The failure is due to one of the following scenarios: unable to send due to full socket queue, unable to compose message due to invalid socket, or lack of available memory.
H323_USER_INFO_RX	H323 USER INFOs received
H323_USER_INFO_TX	H323 USER INFOs transmitted
H323_USER_INFO_FAIL	H323 USER INFOs that failed. The failure is due to one of the following scenarios: unable to send due to full socket queue, unable to compose message due to invalid socket, or lack of available memory.
H323_FACILITY_RX	H323 FACILITYs received
H323_FACILITY_TX	H323 FACILITYs transmitted
H323_FACILITY_FAIL	H323 FACILITYs that failed. The failure is due to one of the following scenarios: unable to send due to full socket queue, unable to compose message due to invalid socket, or lack of available memory.
H323_NOTIFY_RX	H323 NOTIFYs received

Table 6-41 H.323 Protocol Measurements (continued)

Measurement	Description (*= rapid count could mean a potential problem in the system)
H323_NOTIFY_TX	H323 NOTIFYs transmitted
H323_NOTIFY_FAIL	H323 NOTIFYs that failed. The failure is due to one of the following scenarios: unable to send due to full socket queue, unable to compose message due to invalid socket, or lack of available memory.
H323_PASSTHROU_RX	H323 PASS THROUGHs received
H323_PASSTHROU_TX	H323 PASS THROUGHs transmitted
H323_PASSTHROU_FAIL	H323 PASS THROUGHs that failed. The failure is due to one of the following scenarios: unable to send due to full socket queue, unable to compose message due to invalid socket, or lack of available memory.
H323_GRQ_TX	H323 GRQs transmitted
H323_GRQ_RX	H323 GRQs received
H323_GCF_TX	H323 GCFs transmitted
H323_GCF_RX	H323 GCFs received
H323_GRJ_TX	H323 GRJs received
H323_GRJ_RX	H323 GRJs transmitted
H323_RRQ_TX	H323 RRQs transmitted
H323_RRQ_RX	H323 RRQs received
H323_RCF_TX	H323 RCFs transmitted
H323_RCF_RX	H323 RCFs received
H323_RRJ_TX	H323 RRJs transmitted
H323_RRJ_RX	H323 RRJs received
H323_RIP_TX	H323 RIPs transmitted
H323_RIP_RX	H323 RIPs received
H323_RAI_TX	H323 RAIs transmitted
H323_RAI_RX	H323 RAIs received
H323_RAC_TX	H323 RACs transmitted
H323_RAC_RX	H323 RACs received
H323_ARQ_TX	H323 ARQs transmitted
H323_ARQ_RX	H323 ARQs received
H323_ACF_TX	H323 ACFs transmitted
H323_ACF_RX	H323 ACFs received
H323_ARJ_TX	H323 ARJs transmitted
H323_ARJ_RX	H323 ARJs received
H323_URQ_RX	H323 URQs received
H323_URQ_TX	H323 URQs transmitted
H323_UCF_RX	H323 UCFs received

Table 6-41 H.323 Protocol Measurements (continued)

Measurement	Description (*=rapid count could mean a potential problem in the system)
H323_UCF_TX	H323 UCFs transmitted
H323_URJ_RX	H323 URJs received
H323_URJ_TX	H323 URJs transmitted
H323_BRQ_RX	H323 BRQs received
H323_BRQ_TX	H323 BRQs transmitted
H323_BCF_RX	H323 BCFs received
H323_BCF_TX	H323 BCFs transmitted
H323_BRJ_RX	H323 BRJs received
H323_BRJ_TX	H323 BRJs transmitted
H323_DRQ_RX	H323 DRQs received
H323_DRQ_TX	H323 DRQs transmitted
H323_DCF_RX	H323 DCFs received
H323_DCF_TX	H323 DCFs transmitted
H323_DRJ_RX	H323 DRJs received
H323_DRJ_TX	H323 DRJs transmitted
H323_OC_SETUP_REJECTED	incoming H323 SETUP messages received and rejected due to overload condition.

Call Tools Measurements

Table 6-42 Call Tools Measurements

Measurement	Description (*= rapid count could mean a potential problem in the system)
TOOLS_TRUNK_TRANS_ATTMP	Times the TVT process on the reporting CA received a request to perform a trunk based translation.
TOOLS_TRUNK_TRANS_SUCC	Times the TVT process on the reporting CA received a request to perform a trunk based translation and completed it successfully.
TOOLS_LINE_TRANS_ATTMP	Times the TVT process on the reporting CA received a request to perform a line based translation.
TOOLS_LINE_TRANS_SUCC	Times the TVT process on the reporting CA received a request to perform a line based translation and completed it successfully.

AIN Tools Measurements

Table 6-43 AIN Tools Measurements

Measurement	Description (*= rapid count could mean a potential problem in the system)
TOOLS_LNP_QUERY_ATTMP	Times the reporting FS received a request to perform an LNP query from the QVT tool.
TOOLS_LNP_QUERY_SUCC	Times the reporting FS received a request to perform an LNP query from the QVT tool and completed it successfully.
TOOLS_TOLLFREE_QUERY_ATTMP	Times the reporting FS received a request to perform a Toll Free query from the QVT tool.
TOOLS_TOLLFREE_QUERY_SUCC	Times the reporting FS received a request to perform a Toll Free query from the QVT tool and completed it successfully.

PCT Tools Measurements

Table 6-44 PCT Tools Measurements

Measurement	Description (*= rapid count could mean a potential problem in the system)
TOOLS_LIDB_QUERY_ATTMP	Times the reporting FS received a request to perform an LIDB query from the QVT tool.
TOOLS_LIDB_QUERY_SUCC	Times the reporting FS received a request to perform an LIDB query from the QVT tool and completed it successfully.

CPU Usage Measurements

Table 6-45 CPU Usage Measurements

Measurement	Description (*= rapid count could mean a potential problem in the system)
CPU_USAGE_CPU_ID	The id of CPU.
CPU_USAGE_IDLE	The percent of CPU in idle in the last sample interval (100 sec CCS based).
CPU_USAGE_USER	The percent of CPU in idle in the last sample interval (100 sec CCS based).
CPU_USAGE_SYSTEM	The percent of CPU used by system in the last sample interval (100 sec CCS based).
CPU_USAGE_IOWAIT	The percent of CPU used by iowait in the last sample interval (100 sec CCS based).

Memory Usage Measurements

Table 6-46 Memory Usage Measurements

Measurement	Description (*= rapid count could mean a potential problem in the system)
TOTAL_MEMORY	MBs in overall memory.
FREE_MEMORY	MBs in free memory.
TOTAL_SWAP	MBs in total swap.
FREE_SWAP	MBs in free swap.

Network I/O Usage Measurements

Table 6-47 Network I/O Usage Measurements

Measurement	Description (*= rapid count could mean a potential problem in the system)
NETWORK_DEVICE_NAME	The ID name of network device.
IN_PACKETS_PER_SECOND	input packets/sec (100 sec CCS based).
IN_BYTES_PER_SECOND	input bytes/sec (100 sec CCS based).
OUT_PACKETS_PER_SECOND	output packets/sec (100 sec CCS based).
OUT_BYTES_PER_SECOND	output bytes/sec (100 sec CCS based)

Disk Usage Measurements

Table 6-48 Disk Usage Measurements

Measurement	Description (*= rapid count could mean a potential problem in the system)
DISK_USAGE_PARTITION_NAME	The ID name of disk partition. Retrieved from /etc/mnttab.

Table 6-48 *Disk Usage Measurements*

Measurement	Description (*= rapid count could mean a potential problem in the system)
DISK_USAGE_TOTAL_AVAILABLE	blocks on file system.
DISK_USAGE_TOTAL_USED	used blocks.

System Load Usage Measurements

Table 6-49 System Load Usage Measurements

Measurement	Description (*= rapid count could mean a potential problem in the system)
SYSTEM_LOAD_AVERAGE_1MIN	Decaying averages over the last 1 minute of the sum of user + system times +runqueue wait times. The decaying averages are updated once per second. In other words, it is effectively the average number of running plus runnable (waiting on a cpu run queue) threads over the sample period. (100 sec CCS based)
SYSTEM_LOAD_AVERAGE_5MIN	Decaying averages over the last 5 minutes of the sum of user + system times +runqueue wait times. The decaying averages are updated once per second. In other words, it is effectively the average number of running plus runnable (waiting on a cpu run queue) threads over the sample period. (100 sec CCS based)
SYSTEM_LOAD_AVERAGE_15MIN	Decaying averages over the last 15 minutes of the sum of user + system times +runqueue wait times. The decaying averages are updated once per second. In other words, it is effectively the average number of running plus runnable (waiting on a cpu run queue) threads over the sample period. (100 sec CCS based)

Disk I/O Usage Measurements

Table 6-50 Disk I/O Usage Measurements

Measurement	Description (*= rapid count could mean a potential problem in the system)
DISK_IO_DEVICE_NAME	The ID name of disk.
DISK_IO_BYTES_READ	The average value of read bytes during the last several sample intervals, in bytes/sec (100 sec CCS based).
DISK_IO_BYTES_WRITTEN	The average value of write bytes during the last several sample intervals, in bytes/sec (100 sec CCS based).
DISK_IO_READ_OPERATION	The average value of read operation during the last several sample intervals, per second (100 sec CCS based).
DISK_IO_WRITE_OPERATION	The average value of write operation during the last several sample intervals, per second (100 sec CCS based).

ENUM Measurements

Measurement	Description (*= rapid count could mean a potential problem in the system)
ENUM_QUERY_LAUNCHED	The number of ENUM queries launched by the reporting call agent.
ENUM_QUERY_SUCCESSFUL	The number of ENUM queries for which the reporting call agent received a successful response.
ENUM_QUERY_TIMEOUT	The number of ENUM queries for which the reporting call agent timed out.

Measurement	Description (*= rapid count could mean a potential problem in the system)
ENUM_QUERY_NO_VALID_URI	The number of ENUM queries for which the reporting call agent received only malformed URIs.
ENUM_QUERY_NO_URI	The number of ENUM queries for which the reporting call agent did not receive any URIs.
ENUM_QUERY_NO_SERVER	The number of ENUM queries for which the reporting call agent did not find any server.

Diameter Message Counters

The BTS 10200 keeps counters for both base Diameter messages and Sh Diameter messages. You can reset (clear) measurement counters for both types.

Table 6-51 lists the measurement counters related to Diameter messages:

Table 6-51 Diameter Message Measurement Counters

Measurement	Description (*= rapid count could mean a potential problem in the system)
DI_TX_DEVICE_WATCHDOG_REQ	Diameter Device-Watchdog-Request transmitted
DI_RX_DEVICE_WATCHDOG_REQ	Diameter Device-Watchdog-Request received
DI_RX_DEVICE_WATCHDOG_ANS	Diameter Device-Watchdog-Answer received
DI_TX_DEVICE_WATCHDOG_ANS	Diameter Device-Watchdog-Answer transmitted
DI_RX_CAPABILITY_EXCHANGE_REQ	Diameter Capability-Exchange-Request received
DI_TX_CAPABILITY_EXCHANGE_REQ	Diameter Capability-Exchange-Request transmitted
DI_RX_CAPABILITY_EXCHANGE_ANS	Diameter Capability-Exchange-Answer received
DI_TX_CAPABILITY_EXCHANGE_ANS	Diameter Capability-Exchange-Answer transmitted
DI_RX_DISCONNECT_PEER_REQ	Diameter Disconnect Peer Request received
DI_RX_DISCONNECT_PEER_ANS	Diameter Disconnect Peer Answer transmitted
DI_RX_SESSION_TERMINATION_REQ	Diameter Session-Termination-Request received
DI_RX_SESSION_TERMINATION_ANS	Diameter Session-Termination-Answer received
DI_RX_ABORT_SESSION_REQ	Diameter Session-Termination-Answer transmitted
DI_TX_ABORT_SESSION_REQ	Diameter Abort-Session-Request received
DI_RX_ABORT_SESSION_ANS	Diameter Abort-Session-Answer received
DI_TX_ABORT_SESSION_ANS	Diameter Abort-Session-Answer transmitted
DI_USER_DATA_REQ	Diameter User-Data-Request
DI_USER_DATA_ANS	Diameter User-Data-Answer
DI_PROFILE_UPDATE_REQ	Diameter Profile-Update-Request
DI_PROFILE_UPDATE_ANS	Diameter Profile-Update-Answer
DI_SUBSCRIBER_NOTIFICATION_REQ	Diameter Subscriber-Notification-Request

Table 6-51 Diameter Message Measurement Counters

Measurement	Description (*= rapid count could mean a potential problem in the system)
DI_SUBSCRIBER_NOTIFICATION_ANS	Diameter Subscriber-Notification-Answer
DI_PROFILE_NOTIFICATION_REQ	Diameter Profile-Notification-Request
DI_PROFILE_NOTIFICATION_ANS	Diameter Profile-Notification-Answer
DI_SH_ERROR_MSG	Diameter Sh Interface error message

Single Number Reach Counters

Table 6-52 lists Single Number Reach counters. These counters are kept on a BTS 10200 system-wide basis rather than for each subscriber.

Use the **report measurement-pots-local-summary** command to generate a report of the counters.

Because Single Number Reach (follow-me) uses CFU and VM service logic, the invocation of follow-me shows in CFU and VM counters.

Table 6-52 Single Number Reach Feature Counters

Counter Label	Counter Context
POTS_SNR_FIND_ME_ATTMP	Number of find me attempts (in FS Table).
POTS_SNR_FIND_ME_ANSWERED	Number of find me calls answered (in FS Table).
POTS_SNR_FIND_ME_FAIL	Number of find me calls failed due to the system failure (in FS Table).
POTS_SNR_FIND_ME_FORK_INVOKE	Number of forked calls invoked (in FS Table).
POTS_SNR_IVR_REDIRECT_VM	Number of find me calls redirected to voice mail (in FS Table).
POTS_SNR_IVR_ACCESS	Number of times Single Number Reach IVR system accessed.
POTS_SNR_IVR_INVALID_UID_ATTMP	Number of IVR invalid User ID attempts (in FS Table).
POTS_SNR_IVR_INVALID_PIN_ATTMP	Number of IVR invalid PIN attempts (in FS Table).



CHAPTER 7

Using the BTS SNMP Agent

Revised: August 10, 2011, OL-25015-01

Introduction

This chapter explains how to use the Simple Network Management Protocol (SNMP) agent.

The BTS uses a SNMP agent to communicate with a service provider's network management system (NMS). Working together, the SNMP agent and NMS monitor and control BTS components on the managed network. The NMS does most of the processing and provides the majority of memory resources. The SNMP agent collects statistical data (traffic measurements) for the following BTS components:

- AINSVC
- Element Manager
- MGCP Adapter
- SNMP
- Announcement
- H323
- POTS-Feature Server
- SUA
- Audit
- INAP
- SCCP
- TCAP
- Billing
- ISDN
- SCTP
- TSA
- Call Processing
- ISUP SGA
- SIA
- Trunk
- DQOS
- M3UA
- SIM

Using the SNMP agent a user can do the following:

- View and change the status of individual BTS components
- View and change the status of a group of BTS components
- View SNMP trap (alarm) reports

Managing User Access to the SNMP Agent

The SNMP agent has access levels. Tasks you can perform depend both on your user group (community) and CLI security privileges.

Table 7-1 *Managing SNMP Agent Access*


Task	Sample Command
Viewing all read user groups	<pre>show snmpconfig type=readcommunity</pre> <p>The default is “public”. A user needs read level access to:</p> <ul style="list-style-type: none"> • Collect statistics on BTS components • View status on individual BTS components • View status on a group of BTS components
Viewing all write user groups	<pre>show snmpconfig type=writecommunity</pre> <p>The default is “public”. A user needs write level access to:</p> <ul style="list-style-type: none"> • Change settings on individual BTS components • Change settings on a group of BTS components
Adding read user groups	<pre>add snmpconfig type=readcommunity; value=.....; key1=command_level; value1=8;</pre> <p>Values are ASCII strings up to 64 characters.</p>
Adding write user groups	<pre>add snmpconfig type=writecommunity; value=.....; key1=command_level; value1=8;</pre> <p>Values are ASCII strings up to 64 characters.</p>
Deleting read user groups	<pre>delete snmpconfig type=readcommunity; value=.....</pre> <p>Values are ASCII strings up to 64 characters.</p>
Deleting write user groups	<pre>delete snmpconfig type=writecommunity; value=.....</pre> <p>Values are ASCII strings up to 64 characters.</p>

Viewing SNMP Trap Reports

The SNMP agent sends traps to the NMS; each trap maps to an EMS alarm. Alarms not mapped to a specific trap map to a generic trap. Traps show you the following, depending on information availability:

- Severity level
- Alarm ID associated with the trap
- Alarm category
- Set/Cleared flag
- Component (instance) ID
- Component type
- Details of the trap
- Time that trap was generated

Table 7-2 **Receiving Trap Reports**

Task	Operation
Receiving traps reports from the SNMP agent	<p>Add an entry to SNMPTRAPDEST including the following:</p> <ul style="list-style-type: none"> • NMS IP address or hostname • Port number to receive traps • Community string (not used) • Owner string (not used) • Filter Types—This specifies which subsystem events to receive: <ul style="list-style-type: none"> - BILLING - CALLP - CONFIG - DATABASE - MAINTENANCE - OSS - SECURITY - SIGNALING - STATISTICS - SYSTEM - AUDIT • Filter Levels—This specifies which levels of events to receive: <ul style="list-style-type: none"> - DEBUG - INFO - WARNING - MINOR - MAJOR - CRITICAL <p> Caution Filters with DEBUG and/or INFO traps tax BTS resources.</p>

Viewing and Managing BTS Components

Table 7-3 Viewing and Managing BTS Components

Task	Operation
Viewing individual BTS components	<p>GET/GETNEXT</p> <ul style="list-style-type: none"> • Primary and secondary EMS • Primary and secondary BDMS • Primary and secondary CA • Primary and secondary POTS/Centrex/Tandem FS • Primary and secondary AIN FS <p>GET/GETNEXT on MIB State columns</p> <ul style="list-style-type: none"> • MGW • TG • Subscriber Termination • Trunk Termination • SGP • DPC • SCTP Association <p>Note GET/GETNEXT on the ControlState results in one of the following: insufficient-data, not all necessary fields are set or ready-to-commit.</p>

Table 7-3 Viewing and Managing BTS Components (continued)

Task	Operation
Changing settings on BTS components	<ol style="list-style-type: none"> 1. SET necessary fields (Mode column, TargetState column, etc). 2. SET on the ControlState column, using 1 (commit) to change the state. <p>SET</p> <ul style="list-style-type: none"> • Primary EMS • Primary BDMS • Primary CA • Primary POTS/Centrex/Tandem FS • Primary AIN FS <p>SETs on MIB columns</p> <ul style="list-style-type: none"> • MGW • TG • Subscriber Termination • Trunk Termination • SCTP Association
Viewing groups of BTS components	<p>GET/GETNEXT on the following branch: .iso.org.dod.internet.private.enterprises.ipcell.opticall.statusControlBulk</p> <ul style="list-style-type: none"> • MGW • TG • Subscriber Termination • Trunk Termination <p>The Status Value column displays components as follows:</p> <ul style="list-style-type: none"> • ; = separates each instance of a BTS component • = separates status fields • enumerated states are the same as the component's OAMPTable • . = separates CIC and TGN_ID

Querying the SNMP Agent

Table 7-4 Querying the SNMP Agent

Task	Operation
Querying the SNMP agent directly	<ol style="list-style-type: none"> 1. Open the /etc/snmp/conf/snmpd.conf file. 2. In read-community enter a single user group for read access. 3. In managers enter the IP address or hostname of NMS to query, enter multiple addresses separated by spaces. <p>Note To keep communication with the Master Agent leave the localhost entry.</p> <ol style="list-style-type: none"> 4. Restart the SNMP agent, enter: <pre>/etc/init.d/S98mibiisa stop</pre> <pre>/etc/init.d/S98mibiisa start</pre> 5. Query the SNMP agent using the read-community and port 13230.
Querying the SNMP agent via the Master Agent	<ol style="list-style-type: none"> 1. Open the /etc/snmp/conf/snmpd.conf file. 2. In read-community enter a single user group for read access. 3. In managers ensure the localhost is an entry. 4. Change the SNMP configuration type and value: <pre>add snmpconfig type=SETTING; value=COUPLE_SUN_AGENT</pre> 5. Restart the Master Agent. 6. Log in as root. <pre>kill `ps -ef grep -i sad grep -v grep awk '{print \$2}'`</pre> 7. Query the SNMP agent using the read-community and standard port 161.
Querying the MIBs version	<ol style="list-style-type: none"> 1. Open the /opt/BTSsnmp/etc file. 2. View the main MIB, called “optical.mib”. The SNMP Agent supports SNMPv2c operations defined in optical.mib. optical.mib uses variables from other MIBs: <ul style="list-style-type: none"> - IPCELL-TC - SNMPv2-TC - SNMPv2-SMI

Enabling NMS to Query/Poll Solaris SNMP Agent

The EMS runs two SNMP agents as follows:

- SAD (SNMP agent adapter)
- Solaris SNMP agent

The active EMS node runs the SAD process, which converts the BTS 10200 specific events/alarms into SNMP traps and sends them to the configured SNMP Trap listeners or the NMSes. The SAD process handles the SNMPWALK/GET/GETNEXT/SET on the OIDs that are defined in the `optical.mib` file. The SAD process also runs on the standby EMS, but does not perform any function.



Note The SAD process does not run on the CA nodes.



Note The CA runs only the standard Solaris SNMP agent.

The standard Solaris SNMP agent runs on both the active and standby EMS and CA nodes. Therefore, all the four nodes generate the solaris-level traps. The name of the standard Solaris SNMP agent is `mibiisa`, which runs on port number 13230. The Solaris SNMP agent can be used to collect the sun box related statistics and/or traps. Note that the `mibiisa` supports only those OIDs (object identifiers) that are defined in the SUN MIB.



Note The active/standby EMS and active/standby CA nodes generate the solaris-level traps, whereas only the active EMS generates BTS-specific traps and sends them to NMS. The NMS can query/poll all the four nodes to receive the generated traps.

To enable the NMS to directly query the Solaris SNMP agent for a range of OIDs specified by SUN MIBs, and receive Solaris box-level traps, do the following:

1. Open the `/etc/snmp/conf/snmpd.conf` file.
2. Define the read-community as “public”.
3. In the “Managers” field, enter the IP address or hostname of the NMS from where the user needs to send the SNMP query. Enter multiple addresses separated by spaces, but leave the “localhost” entry as is.
4. In the Trap field, configure the IP address or hostname of the NMS where the traps have to be sent.
5. Restart the SNMP agent, enter:

```
/etc/init.d/S98mibiisa stop
/etc/init.d/S98mibiisa start
```

6. Query the SNMP agent (using SNMPGET/SNMPWALK) from the Manager using the read-community and port 13230. For example, to get the system up time, enter the following command:

```
snmpwalk -c public -p 13230 prica07 system
```

The output appears as given below:

```
system.sysDescr.0 = Sun SNMP Agent
system.sysObjectID.0 = OID: enterprises.42.2.1.1
system.sysUpTime.0 = Timeticks: (279199168) 32 days, 7:33:11.68
system.sysContact.0 = System administrator
system.sysName.0 = prica07
system.sysLocation.0 = System administrators office
system.sysServices.0 = 72
```




APPENDIX **A**

Feature Tones

Revised: August 10, 2011, OL-25015-01

Introduction

This appendix explains special tones the BTS supports for subscriber and operator features. The BTS supports these tones by sending MGCP messages to the gateways.

Tones per Feature

Table A-1 Feature Tones

Feature	Tone	Condition(s) That Initiate Tone ¹
AC	ALERTING PATTERN 3	
ACR	No tone	
ACRA ACRD	CONFIRMATION TONE	Anonymous call rejection (ACR) was successfully activated or deactivated by subscriber actions.
	REORDER TONE	ACR was not successfully activated or deactivated by subscriber actions.
AR	ALERTING PATTERN 3	
BLV/OI	REORDER TONE	Normal access is not available. There is a local office problem. The line is momentarily unavailable. No-test access is not available.
	BUSY VERIFICATION	CFU is activated on the terminating line. Terminating line is a data-only line or a denied line.
	PERMANENT SIGNAL TONE	Line up to receiver off-hook tone. Terminating line receiving a permanent signal announcement. Terminating line is high and wet (battery and ground shorted) or high and dry (off hook for an extended period).

Table A-1 Feature Tones (continued)

Feature	Tone	Condition(s) That Initiate Tone ¹
CW CIDCW	CW TONE	If called party has MDN feature: primary DN matched. If called party is in Centrex system with DACWI: there is no extension for the number dialed. If called party has DRCW feature: calling party is not on the DRCW screening list. ²
	CW TYPE 2	If called party has MDN feature: second DN matched. If called party is in Centrex system with DACWI: extension exists for the number dialed.
	CW TYPE 3	If called party has MDN feature: third DN matched.
	CW TYPE 4	If called party has DRCW feature: calling party is on the DRCW screening list. ²
	STUTTER TONE	For Centrex subscriber with CHD feature and currently on an active call: A third party calls in, and the called party hears a call-waiting tone. The called party presses Flash button or switchhook to place the current remote station on hold, and hears the stutter tone. The called party has the following options: <ul style="list-style-type: none"> • Press Flash button or switchhook again to return to the original call. • Dial a designated vertical service code (VSC)—typically *52—to be connected to the new calling party; the first calling party is kept on hold.
	TONES OFF	No tones are played for CW or CIDCW. (Tones are turned off under certain special circumstances.)
	ALERTING PATTERN 1	Alerting pattern (ringing) is provided to the calling party and called party, as applicable, for all reconnect, re-ring, callback and recall scenarios.
CCW	CONFIRMATION TONE	The subscriber in two-way call cancels call waiting.
	DIAL TONE	POTS or Centrex subscriber picks up phone to cancel call waiting.
	STUTTER TONE	The subscriber places the other party on hold (CHD) and then activates CCW while call is still on hold.
	ALERTING PATTERN 1	The subscriber goes on hook with the other party still on hold; the BTS provides alerting pattern (ringing).
CDP	DIAL TONE	The subscriber is granted access to an outside (public) line, typically after dialing 9.
	ALERTING PATTERN 3	Member of a Centrex group receives an incoming call from the group attendant.
CFU	REMINDER RING TONE	Alerting pattern (ringing) is provided on the called station to indicate that a call has been received and automatically forwarded.

Table A-1 Feature Tones (continued)

Feature	Tone	Condition(s) That Initiate Tone ¹
CFU-ACT	STUTTER TONE	The subscriber has successfully activated CFU from the handset.
	DIAL TONE	The subscriber has dialed the CFU-ACT star code, and the BTS is ready to receive digits for the forward-to DN. 1-second timer elapses following the confirmation tone.
	CONFIRMATION TONE	Centrex subscriber successfully activates extension forwarding. If the subscriber has multiple call forwarding (MCF), the subscriber has successfully activated a chain call forwarding scenario POTS subscriber receives ROUTE SELECTED DIALING PLAN.
	REORDER TONE	The CFU-ACT attempt was not successful due to <ul style="list-style-type: none"> Attempt to activate CFU when it was already activated Attempt to forward calls to a DN that could not be reached Attempt to forward call from a DN to itself.
CFU-DEACT	CONFIRMATION TONE	The subscriber successfully deactivates CFU.
	DIAL TONE	1-second timer elapses following the confirmation tone.
	REORDER TONE	The subscriber attempts to deactivate CFU when it was already deactivated
CFB-ACT and CFNA-ACT	DIAL TONE	The subscriber has dialed the CFB-ACT or CFNA-ACT star code, and the BTS is ready to receive digits for the forward-to DN.
	CONFIRMATION TONE	The subscriber successfully activates CFB or CFNA.
	DIAL TONE	1-second timer elapses following the confirmation tone.
CFB-DEACT and CFNA-DEACT	CONFIRMATION TONE	The subscriber has dialed the CFB-DEACT or CFNA-DEACT star code, and CFB or CFNA has been deactivated.
	DIAL TONE	Issued after a 1-second timer elapses following the confirmation tone.
CHD	STUTTER TONE	For Centrex subscriber (controlling party) currently on an active call: The controlling party places the other party on hold by pressing the Flash button or switchhook, and hears the stutter tone. Controlling party has the following options: <ul style="list-style-type: none"> Press Flash button or switchhook again to return to the original call. Dial a designated vertical service code (VSC)—typically *52—hear the stutter tone again, then dial a third party. The first calling party is kept on hold.
	ALERTING PATTERN 1	Alerting pattern (ringing) is provided to the calling party and called party, as applicable, for all reconnect, re-ring, callback and recall scenarios.
CNAM CND	No tone	

Table A-1 Feature Tones (continued)

Feature	Tone	Condition(s) That Initiate Tone ¹
CNDB CNAB CIDB CIDS	DIAL TONE	The subscriber has dialed the star code for the identity blocking feature, and the BTS is ready to receive digits for the DN to be called.
COS: Account Codes	CONFIRMATION TONE	The BTS prompts the subscriber to enter the account code.
COS: Authorization Codes	CONFIRMATION TONE	The BTS prompts the subscriber to enter the authorization code.
CPRK	REORDER TONE	The subscriber has dialed the call park (CPRK) access code, but is not subscribed to the CPRK feature. The subscriber has CPRK and has dialed the CPRK access code, but the CPRK attempt was not successful. Note In this case (CPRK attempt was not successful), the reorder tone is played for two seconds, and then the subscriber is reconnected to the original call.
	STUTTER TONE	The subscriber presses Flash button or switchhook to park the call.
CPRK_RET	REORDER TONE	The subscriber has CPRK and has dialed the CPRK access code, but is unable to retrieve the call.
	STUTTER TONE	The subscriber enters the CPRK_RET access code, and the BTS is waiting for the subscriber to dial the extension against which the parked call should be retrieved.
CT/TWC	ALERTING PATTERN 1	The subscriber hangs up with one party on hold.
DACWI	ALERTING PATTERN 3	Distinctive ring pattern.
DPN	STUTTER TONE	The subscriber has dialed DPN access code, and DPN access has been granted.
	REORDER TONE	Reorder tone is returned to the subscriber who initiated a DPN request when any of the following occurs: <ul style="list-style-type: none"> • The DPN feature has not been assigned to the requesting line. • The dialed extension is not assigned in the business group dialing plan. • The line associated with the dialed extension is not being rung. (Note that “being rung” should not include being given call-waiting treatment.) • The call has been answered, picked up, or abandoned. • The requesting line is not allowed to pick up the particular call because of being assigned the fully restricted terminating or the denied termination feature.

Table A-1 Feature Tones (continued)

Feature	Tone	Condition(s) That Initiate Tone ¹
DPU	STUTTER TONE	The subscriber has dialed DPU access code, and DPU access has been granted.
	REORDER TONE	Reorder tone is returned to the subscriber who initiated a DPU request when any of the following occurs: <ul style="list-style-type: none"> The dialed extension is not assigned in the business group dialing plan. The line associated with the dialed extension is not assigned the DPU feature. The line associated with the dialed extension is neither being rung nor involved in a stable two-way call. (Note that “being rung” should not include being given call-waiting treatment. Note also that DPU should not allow a subscriber to barge-in on the controller of a multiway connection, that is, a call-waiting configuration, a call-hold configuration, or a conference call.) The call is abandoned by the caller before the DPU request is recognized or has been picked up by a line without DPU assigned. The requesting line is not allowed to pick up the particular call because of being assigned the fully restricted terminating or the denied termination feature.
	CONFIRMATION TONE	Barge-in connection is being processed and connection will occur within one second. Note Confirmation tone is repeated twice.
DRCW	ALERTING PATTERN 1	DN of incoming call is <i>not</i> on the DRCW screening list.
	ALERTING PATTERN 6	DN of incoming call is on the DRCW screening list.
	CW TONE	DN of incoming call is <i>not</i> on the DRCW screening list.
	CW TYPE 4	DN of incoming call is on the DRCW screening list.
Emergency—911	ALERTING PATTERN 1	After a normal two-party call, the subscriber presses the Flash button or hookswitch, dials 911, and then hangs up before the 911 operator answers.
MDN	ALERTING PATTERN 1	Station is on hook and there is an incoming call to primary DN.
	ALERTING PATTERN 4	Station is on hook and there is an incoming call to secondary DN.
	ALERTING PATTERN 5	Station is on hook and there is an incoming call to the third DN.
	CW TONE	Station is off hook and there is an incoming call to primary DN.
	CW TYPE 2	Station is off hook and there is an incoming call to secondary DN.
	CW TYPE 3	Station is off hook and there is an incoming call to the third DN.
MWI ³	MWI TONE	The subscriber has MWI service and has a message waiting.
MIDCALL	STUTTER TONE	After pressing Flash button or hookswitch and the BTS acknowledges it is as a valid midcall action.
	ALERTING PATTERN 1	The subscriber goes on hook with the other party still on hold; the BTS provides alerting pattern (ringing).

Table A-1 Feature Tones (continued)

Feature	Tone	Condition(s) That Initiate Tone ¹
SC1D-ACT SC2D-ACT	STUTTER TONE	Stutter tone is used once after the subscriber enters the *74 (SC1D activation) or *75 (SC2D activation) to begin the process of collecting the information required to provision one of the speed call slots. After a speed call slot has been successfully provisioned, the subscriber will again receive the stutter tone to signify that the speed call slot was successfully provisioned.
VMWI ³	STUTTER TONE	The subscriber has VMWI and has a message waiting, but the serving MGW does not have a visual indicator.

1. When more than one condition is listed for a single tone, any one of the conditions can cause the tone to be played.
2. For more information on the screening list, refer to the *Cisco BTS 10200 Softswitch System Description*.
3. MWI = message waiting indicator; VMWI = visual message waiting indicator.

Tone Frequencies and Cadences

Tones are requested by the BTS and delivered to the subscriber or operator by the MGW. Some MGWs can be provisioned to play tone cadences different than the ones described in this table.

Table A-2 Subscriber and Operator Tone Descriptions

Tone	Frequency (Hz)	Cadence Played by MGW
Alerting pattern (ringing) 1	440 + 480	2 sec on, 4 sec off, repeating
Alerting pattern (ringing) 2	440 + 480	0.8 sec on, 0.4 sec off, 0.8 sec on, 4.0 sec off, repeating
Alerting pattern (ringing) 3	440 + 480	0.4 sec on, 0.2 sec off, 0.4 sec on, 0.2 sec off, 0.8 sec on, 4 seconds off, repeating
Alerting pattern (ringing) 4	440 + 480	0.3 sec on, 0.2 sec off, 1 sec on, 0.2 sec off, 0.3 sec on, 4 sec off, repeating
Alerting pattern (ringing) 5	440 + 480	0.5 sec on once
Alerting pattern (ringing) 6	440 + 480	1 sec on, 3sec off, repeating
Busy verification (used for operator BLV ¹)	440	2 sec burst, followed by 0.5 sec burst every 10 sec
CW tone	440	0.3 sec on once
CW Type 1	440	0.3 sec on once
CW Type 2	440	0.1 sec on, 0.1 sec off, 2 times
CW Type 3	440	0.1 sec on, 0.1 sec off, 3 times
CW Type 4	440	0.1 sec on, 0.1 sec off, 0.3 sec on, 0.1 sec off, 0.1 sec on
Confirmation tone	350 + 440	0.1 sec on, 0.1 sec off, 3 times
Dial tone	350 + 440	steady on
Line busy tone	480 + 620	0.5 sec on, 0.5 sec off, repeating
Message waiting indicator tone	350 + 440	10 bursts (0.1 sec on, 0.1 sec off), then steady on
Off-hook warning tone (receiver off-hook tone)	1400 + 2060 + 2450 + 2600	0.1 sec on, 0.1 sec off, repeating

Table A-2 Subscriber and Operator Tone Descriptions (continued)

Tone	Frequency (Hz)	Cadence Played by MGW
Permanent signal (used for operator BLV ¹)	480	Steady on
Reminder ring tone (ring splash)	440 + 480	0.5 sec ring
Reorder tone	480 + 620	0.25 sec on, 0.25 sec off, repeating
Ringback tone (audible ringing)	440 + 480	2 sec on, 4 sec off (repeated)
Stutter (recall) dial tone	350 + 440	3 bursts (0.1 sec on, 0.1 sec off), then steady on

1. BLV = busy line verification

Table A-3 lists the maintenance tones used for continuity testing. See the Telcordia document GR-317-CORE for additional details.

Table A-3 Maintenance Tone Descriptions

Tone	Frequency (Hz)	Description
2010-Hz continuity tone	2010	Used for single-tone test under either of the following conditions: <ul style="list-style-type: none"> The circuit is a 4-wire circuit at both the transceiver end and the distant end The circuit is a 2-wire circuit at the transceiver end
1780-Hz continuity tone	1780	Used for dual-tone test with a 4-wire circuit at the transceiver end and a 2-wire circuit at the distant end

All tones are based on information in the following:

- Telcordia document *GR-506-CORE, Signaling for Analog Interfaces*
- Telcordia document *TR-NWT-506, Issue 3, Signaling*
- Telcordia document *GR-590-CORE, Call Pickup Features (FSD 01-02-2800)*
- Telcordia document *GR-317-CORE, Switching System Generic Requirements for Call Control Using the Integrated Services Digital Network User Part (ISDNUP)*
- Telcordia document *GR-219-CORE, Distinctive Ringing/Call Waiting (FSD 01-01-1110)*.
- IETF document *RFC 2705, Media Gateway Control Protocol (MGCP) Version 1.0*



APPENDIX **B**

FIM/XML

Revised: August 10, 2011, OL-25015-01

This appendix describes the FIM/XML feature of the Cisco BTS 10200 Softswitch and explains how to use it. This document includes the following topics:

- [Understanding the Configurable FIM/XML Feature](#)
- [Tool Requirements](#)
- [Writing an External FIM/XML File](#)
- [Defining Features](#)
- [Installing the FIM/XML File Using the Offline FIM/XML Tool](#)
- [FIM/XML File and Shared iFC File](#)
- [Provisioning iFC](#)
- [Feature Restrictions and Limitations](#)

Understanding the Configurable FIM/XML Feature

The Cisco BTS 10200 supports a Feature Interaction Module/Extensible Markup Language (FIM/XML) file that defines the interactions between the internal features (for example, Call Waiting, Call Forwarding) and external features (features that reside on application servers that interact with Cisco BTS 10200 and SIP triggers like, TV Caller ID, Network Address Book).

However, the current FIM/XML format can be time consuming as the service provider or operator needs to configure and define large number of parameters. The configurable FIM/XML feature introduces a new external configurable FIM/XML file which is more efficient because it defines the interactions between the IMS Service Control Interface (ISC) and Feature Control Protocol (FCP) features. The Cisco BTS 10200 Feature Server manages the ISC and FCP feature interactions based on the rules in this FIM/XML file.

The Cisco BTS 10200 Softswitch Plain Old Telephone Service (POTS) Feature Server uses the configurable FIM/XML file to manage the ISC and FCP features using the parameters defined in the configurable FIM/XML file. You can produce the new FIM/XML file using the old FIM/XML file and schema data.

External FIM/XML file allows you to do the following:

- Add a new external feature name
- Specify the list of features inhibited by an external feature

- Specify the precedence order for the external features
- Define the list of features that inhibit the external feature
- Define error response operations

Advantages of the FIM/XML Tool

The FIM/XML tool enables the service provider or operator to specify the SIP trigger-based features. The SIP trigger-based feature examples are, Off-Hook Delay Trigger (OHD), Termination Attempt Triggers TAT-1 and TAT-2.

The tool helps to define the interactions and precedence with the other features of Cisco BTS 10200. The service provider can generate his or her own XML file (FIM/XML) according to the schema data provided in the Cisco BTS 10200. Once the generated FIM/XML file is installed on the Cisco BTS 10200, the new external application server-driven features and their interactions with other Cisco BTS 10200 features comes into effect.

The advantages of the FIM/XML tool are:

- The tool prevents the operator from the possibility of disrupting the external/current features when editing the complex FIM/XML file. The FIM/XML tool now provides an easy and efficient way of editing the complex file seamlessly.
- Provides a semantic check on the operator-generated FIM/XML file.

In order to specify a common SIP trigger profile, an additional XML file needs to be generated. This XML file calls the Shared Initial Filter Criteria (iFC) XML file read by Cisco BTS 10200 to determine the SIP trigger profiles. SIP trigger profiles are used to determine the address of the application server and populate the different route-headers when SIP triggers launch. For additional information on the shared iFC file, refer to the [“FIM/XML File and Shared iFC File” section on page B-9](#).

Tool Requirements

Each Cisco BTS 10200 release includes an original FIM/XML file. The offline FIM/XML tool allows the service provider or operator to define a new external feature or modify existing interactions involving the ISC features.

The Cisco BTS 10200 must meet the following conditions and requirements for the FIM/XML tool:

- Java Virtual Machine (JVM) 1.6 or above is installed on the system.
- All three input files (for example param=1, param=2, and param=3) are present in the same directory as the tool .jar file. Refer to [Step 6](#) in the procedure below for the list of input files.

- The service provider or operator has write permission for the directory where the FIM/XML offline tool is located.
- The service provider or operator has read permission for all the input XML files.

Writing an External FIM/XML File

To write an external FIM/XML file, do the following:

-
- Step 1** Use any XML editor.
 - Step 2** Open a new XML file in it.
 - Step 3** Set the schema to the supplied External FIM/XML schema:

```
<external-fimxml xsi:schemaLocation="externalfimxml externalfimxml.xsd"
xmlns="externalfimxml" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

- Step 4** Define new features in XML file.
- Step 5** Save the new external FIM/XML file.

Defining Features

The service provider needs to define new features to ensure that Cisco BTS10200 understands the behavior of the external features. The external feature is defined using the define-external tag in the External FIM/XML file:

```
<define-external feature-name="TAT_5" feature-type="TERMINATING">
</define-external>
```

Each external feature has a unique name. The name has a minimum of 16 characters, and no special characters are allowed. The Feature Type is defined as Originating or Terminating.

Elements in the External FIM/XML File

The external FIM/XML is a subset of the FIM/XML file and contains definitions and behavior of ISC features. The External FIM/XML file is used to define the ISC feature and its properties. The defined external elements are used to add new external features to Plain Old Telephone System (POTS) FC.

The external FIM/XML file contains the following elements:

- [“Define Element” section on page B-4](#)
- [“Precedence-Exception Element” section on page B-4](#)
- [“Inhibit Others Element” section on page B-5](#)
- [“Inhibit Me Element” section on page B-5](#)
- [“Response Profile Element” section on page B-5](#)

Define Element

The properties of the external feature are configured in the Define Element. The FIM/XML tool processes the external FIM/XML file in the Define Element.

```
<define-external feature-name="TAT_1" precedence_lesser_than ="SCR"
billing-name="tat1_as">
```

Table 1 lists the attributes in the Define Element.

Table 1 Attributes of Define Element

Attribute Name	Required	Description
feature_name	Yes	Name of the feature being defined. This is unique for all the features, including FCP or ISC.
billing_name	Optional	The name displayed when the feature is invoked in billing records.
precedence_lesser_than	Yes	The defined feature invoked after the attribute is set in the feature name. Precedence_lesser_than can contain any defined internal or external feature name. For originating features the 'precedence_lesser_than' must contain features defined on OHT_TRIGGER and for terminating 'TERMINATION_ATTEMPT_AUTHORIZED'. To invoke a feature as the first feature, enter the value as NULL in precedence_lesser_than attribute.

Precedence-Exception Element

The Precedence-Exception element defines the exception in the precedence list for the defined external feature. The feature name in the precedence-exception element has a lesser precedence than the defined external feature even after the external feature is defined below it in the precedence list.

The following is the example to define precedence exception:

```
<define-external feature-name="F5" precedence-lesser-than="F4" >
<precedence-exception feature-name="F2" />
...
</define-external>
```

You can have as many exceptions for the precedence as you like (for example, F1>F2>F3>F4>F5>F2, where you can define F5 precedence less than F4 and greater than F2).

Table 2 lists the attributes of the Precedence-Exception Element.

Table 2 Attributes of Precedence-Exception Element

Attribute Name	Required	Description
Feature Name	Yes	Name of the feature that has lesser precedence than the defined external feature.

The FIM/XML tool expects the Precedence-Exception element in External FIM/XML file as follows.

```
<precedence-exception feature-name="CCW" />
```

Inhibit Others Element

The Inhibit Others Element tag defines the list of features that are inhibited when a given feature is in an Assigned or Invoked state. [Table 3](#) lists the attributes of the Inhibit Others Element.

Feature Inhibitions prevent invocation of a given feature if a specified feature is Activated, Deactivated, Invoked, Assigned. For example, when the emergency call is involved then the Call Waiting is inhibited.

Table 3 *Attributes of Inhibit Others Element*

Attribute Name	Required	Description
Feature Name	Yes	Name of the feature that inhibits the external feature
State	Yes	The state of the given feature when it inhibits the external feature

The FIM/XML tool expects the defined element in the External FIM/XML file as indicated in the following sections.

```
<inhibit-others state="ASSIGNED" feature-name="CNAM" />
<inhibit-others state="INVOKED" feature-name="MOH" />
```

Inhibit Me Element

The Inhibit Me element defines the list of features that inhibit the external feature when the features are in the following states: Activated, Deactivated, Assigned, or Invoked. [Table 4](#) lists the attributes of the Inhibit Me Element.

Table 4 *Attributes of Inhibit Me Element*

Attribute Name	Required	Description
Feature Name	Yes	Name of the feature that inhibits the external feature. The state can be either ASSIGNED or INVOKED.
State	Yes	The state of the external feature when it inhibits the given feature.

The FIM/XML tool expects the defined element in the External FIM/XML file as indicated in the following sections.

```
<inhibit-me feature-name="CCW" state="DEACTIVATED" />
<inhibit-me feature-name="CW" state="INVOKED" />
```

Response Profile Element

When the defined external feature is invoked, the system receives different responses or errors, depending on what happened during the feature invocation. This allows the operator to specify what actions need to be taken when specific errors or responses (SIP Responses) are received from the Application Servers.

For example, when an external feature is invoked, an INVITE is sent by Cisco BTS 10200 to the Application Server and no application server can return an error response such as “401 unauthorised” error. You can define the action that Cisco BTS 10200 can take using the Response Profile element.

Error

The list of error elements is matched one by one to see if the error response received during the external feature invocation falls within its specified range. When a match is found, the error handling operation specified within the respective error element is executed.

Table 5 Error Attributes

Attribute Name	Required	Description
range-start	Optional	The start range of the error responses of the element that is matched.
range-end	Optional	The end range of the error responses of the element that is matched.

Operation

This element specifies the action taken when the response condition matches the error element. The parameters of an element can be a list of name or value pairs specified by parameter elements.

Table 6 Operation Attributes

Attribute Name	Required	Description
Name	Yes	Name of the operation performed.
Param-value	Optional	List of the parameter-value pairs used when BTS performs the operation.
Feature	Optional	Feature name used when performing the operation.

The FIM/XML tool processes the defined element in the External FIM/XML file as indicated in the following sections.

```

<response-profile>
  <error range-start="503" range-end="599" type="SIP">
    <operation name="continue-from-dp"/>
  </error>
  <error range-start="403" range-end="403" type="SIP">
    <operation name="disconnect">
      <param name="cause" value="1325"/>
    </operation>
  </error>
</response-profile>

```

Installing the FIM/XML File Using the Offline FIM/XML Tool

Each Cisco BTS 10200 release includes an original FIM/XML file that is installed during system setup and upgrades. The offline FIM/XML tool allows the service provider to define a new external feature or modify existing interactions involving the ISC features. In order to enable the service provider to add external features, a separate XML configuration file is provided. This new FIM/XML file is called an External FIM/XML file. After the operator generates the external FIM/XML file according to the schema provided, the FIM/XML tool generates the FIM/XML file. Use this file as input, along with the schema, to produce the new FIM/XML file with the offline tool. The offline tool is the XML file that is separate from the Cisco BTS 10200.



Note

The system must meet the tool conditions and requirements for the FIM/XML tool as described in “[Tool Requirements](#)” section on page B-2.

The following procedure describes how to generate the configurable FIM/XML file using the offline FIM/XML tool.

- Step 1** Obtain the fiexmxml.zip file from the location specified and then unzip the FIM/XML file on all BTS nodes:
- ```
/opt/OptiCall/tools/fiexmxml.zip
```
- Step 2** Run the fimxml.zip file.
- The external FIM/XML template is external.xml and the external FIM/XML schema is obtained as externalfimxml.xsd:
- ```
hrn29priems:/opt/OptiCall/tools >unzip fimxml.zip
Archive:  fimxml.zip
  inflating:  config.xml
  inflating:  external.xml
  inflating:  externalfimxml.xsd
  inflating:  fimxmlconfig.xsd
  inflating:  FIMXML.xsd
  inflating:  fimxml.jar
hrn29priems:/opt/OptiCall/tools
```
- Step 3** Use any XML editor to create an external FIM/XML file based on the rules from the externalfimxmlfile.xsd schema file provided by the Cisco BTS 10200 during installation. The service provider cannot modify the schema data.
- Step 4** Use the XML editor to edit a sample file provided with the FIM/XML tool. This file becomes the offline FIM/XML configuration file used in [Step 6](#).
- Step 5** You can edit the FIM/XML file so that the emergency features such as 9-1-1, Hostage Negotiation, and Emergency Callback (ECB) cannot be inhibited by the operator after the configurable FIM/XML file is downloaded to the Cisco BTS 10200:

```
<fcp-features> <feature name=E911 inhibition-allowed=false/>
```

You can also configure the schema path for the configurable FIM/XML file:

```
<config-param param=FIMXMLSCHEMA_PATH value=FIMXML.xsd/>
```

If you do not specify a schema path, the Cisco BTS 10200 uses the following default path:

```
/opt/OptiCall/potsctx/bin/FIMXML.xsd
```

Step 6 Run the following Java application:

```
java -jar fimxml.jar param1 param2 param3 param4
```

Where

- param1 = the name of the external FIM/XML file described in [Step 3](#)
- param2 = the name of the original FIM/XML file produced during the Cisco BTS 10200 installation. Copy this file from the following path: /opt/OptiCall/etc/fimxml/FSPTC235/FIMXMLRules.xml.
- param3 = the name of the configuration file described in [Step 4](#)
- param4 = the name of the configurable file to be generated (defaults to merged.xml). This parameter is optional.

If the script runs successfully, the tool returns the following message **SUCCESS!! New FIM/XML generated at path <path>**. The successfully generated configurable FIM/XML files are copied or FTP to the EMS.

If the script does not complete successfully, the system returns a non-zero value and generates a log file which is copied to the same directory as the FIM/XML tool .jar file.



Note The tool produces log files for both successful and unsuccessful attempts.



Note You can troubleshoot the errors from the descriptions provided with the error messages.

Step 7 Run the following command from the EMS:

```
install fimxml file_name=<absolute_path>
```

This command does the following:

- Processes the configurable FIM/XML file on the EMS
- Adds, updates and/or deletes the external feature names from the new fimxml file.
- Copies the new file to the following path:

```
/opt/OptiCall/etc/fimxml/FSPTC235/FIMXMLRules.xml
```

Step 8 Restart the POTS Feature Server on both the CA primary and secondary nodes to load the configurable FIM/XML file.

FIM/XML File and Shared iFC File

A Shared Initial Filter Criteria (iFC) file specifies all the data required to provision a new feature in the Element Management System (EMS). Using the shared iFC file is analogous to provisioning feature data through the CLI. You can provision all the user commands supported through CLI using the shared iFC.

The Cisco BTS 10200 supports the following commands through shared iFC:

- Add/change/delete feature
- Add/change/delete feature-config fname
- Add/ change/delete vsc
- Add/change/delete sip-trigger-profile
- Add/Change/delete subscriber-sip-trigger-profile
- Add/Change/Delete service
- Add/Change/Delete subscriber-service-profile

The following conditions apply to the configurable FIM/XML file and the shared iFC file:

- Any property provisionable through FIM/XML cannot be provisioned through the shared iFC file.
- If an external feature name exists in the FIM/XML file but is not defined in the EMS, then the EMS provisions that external-feature name by reading the FIM/XML file.

Features Defined in FIM/XML and Shared iFC

The Shared iFC file defines the features invoked by Cisco BTS 10200. The FIM/XML defines the information pertaining to interactions between these features.

[Table 7](#) explains the parameter names that can be configured in the FIM/XML and Shared iFC.

Table 7 Parameters in FIM/XML and Shared iFC

Parameters	FIM/XML	Shared iFC
Feature Type (Originating and Terminating)	No	Yes
SIP Trigger Profile	No	Yes
Feature-SIP Trigger Profile Mapping	No	Yes
Feature Config Data	No	Yes
VSC	No	Yes
Precedence Information	Yes	No
Inhibition Information	Yes	No
Response Profile	Yes	No

Provisioning iFC

To enable the operator to provision iFC (s) through the XML file, the service provider must generate and install the new XML file (Shared iFC file).

The XML file allows the operator to provision iFC (s) by allowing

- External feature definition
- Vertical Service Code (VSC) to feature mapping by defining a star-code if necessary for invoking an external Application Server-driven feature
- SIP trigger profile specifies which application server needs to be contacted and how to populate the Route-headers
- Sip Trigger Profiles (Subscriber Specific)

The XML file enables the operator to define the mapping of one sip_trigger_profile to multiple subscribers. The following commands list the CLI commands corresponding to entries in the Shared iFC file:

- [Defining a New feature as the Originating Feature.](#)
- [Defining a VSC](#)

Defining a New feature as the Originating Feature

This command defines the new feature as the originating feature.

```
add/change feature fname=ABC; tdp1=collected_information; tid1=ohd_trigger; ttype1=R;
tdp2=o_exception; tid2=reroute_trigger; ttype2=R; tdp3=collected_information;
tid3=vertical_service; ttype3=R; feature_server_id=FSPTC235;
```

Defining a VSC

This command defines a VSC which when dialed invokes the external feature.

```
add/change vsc digit-string=*72;fname=ABC;
```

Defining the SIP Trigger Profile

This command defines the SIP Trigger Profile used with the external feature.

```
add sip-trigger-profile id=vdial+noivr;
route_guide_id=60001;AS_ROUTE_HEADER_USER=vdial+noivr;
```

Feature Configuration

This command defines the feature configuration.

```
add feature-config fname=ABC; type=DEFAULT-SIP-TRIGGER-PROFILE; value=AS_1;
```

Subscriber-Sip-Trigger-Profile

This command adds the Subscriber-Sip-Trigger-Profile.

```
add subscriber-sip-trigger-profile sub-id=sub_1; fname=ABC; sip-trigger-profile-id=AS_1;
```

Service-Id

This command adds the Service ID.

```
add service id=ohd_vsc; fname1=ABC;
```

Subscriber-Service-Profile

This command adds the Subscriber-Service-Profile.

```
add service id=ohd_vsc; fname1=OHD; fname2=NEW; fname3;
```

Feature Restrictions and Limitations

The FIM/XML tool cannot be used to

- Change the interaction between internal features
- Define feature configuration properties
- Define feature support profile

