



Cisco BTS 10200 Softswitch Release Notes for Release 4.5.1

Revised: October 23, 2007

The Cisco BTS 10200 Softswitch is a class-independent software switch (softswitch) that provides next-generation integrated voice and data switching solutions for packet networks.

For an overview of the components, functions and signaling protocols supported by the Cisco BTS 10200 Softswitch, see the [System Description \(Release 4.5\)](#).

For descriptions of network features, subscriber features, class of service (COS) functions, outgoing call barring (OCB), feature interactions, and interactive voice response (IVR) features, see the [Network and Subscriber Feature Descriptions \(Release 4.5\)](#).



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© <year> Cisco Systems, Inc. All rights reserved.

Contents

These release notes for the Cisco BTS 10200 Softswitch describe the enhancements and new features provided in Release 4.5.1 (900-04.05.01.Vxx).

Also, these release notes describe the enhancements and new features provided in Release 4.5.1, Maintenance Releases 1 and 2 (MR1, MR2).

This document includes the following sections:

- [System Requirements, page 3](#)
 - [Hardware Requirements, page 3](#)
 - [Software Requirements, page 7](#)
- [Caveats, page 14](#)
- [New or Enhanced Features for Release 4.5.1, page 21](#)
- [Previous 4.x Releases, page 78](#)
- [Cisco Field Notices, page 105](#)
- [Obtaining Documentation, page 105](#)
- [Obtaining Technical Assistance, page 106](#)

These release notes are updated periodically on an as needed basis. Please read these release notes in their entirety, because they contain important operational information that can impact your network.

System Requirements

This section details the Cisco BTS 10200 Softswitch supported hardware platforms, their supported options and configurations, and the supported software releases.

Multiple hardware options are available. Service providers should consult with their Cisco account team and choose the option that best suits their network applications and traffic levels. Refer to [Table 1 on page 4](#) for host hardware options.

The physical plant requirements for installation of the Cisco BTS 10200 Softswitch are documented in the [Cisco BTS 10200 Softswitch Site Preparation and Network Communication Requirements](#).

The Cisco BTS 10200 Softswitch requires the following equipment:

- Call Agent/Feature Server (CA/FS)—Two hardware platforms for redundant operation.
- Element Management System/Bulk Data Management System (EMS/BDMS) server— Two hardware platforms for redundant operation. The EMS minimum requirement for the Release 4.5.1 medium configuration is 4 GB.
- Two Ethernet switches.



Note

Both AC and DC systems require two redundant feeds. We highly recommend that uninterruptible power supplies be provided for both AC and DC systems. For information on the voltage required, refer the Sun Microsystems Web site.



Note

The Cisco Technical Assistance Center (TAC) only supports Cisco software running on Cisco-approved hardware configurations. The software is not supported on any other hardware.

Sun Microsystems hardware can be ordered directly from the vendor or a Sun value added reseller; however, Cisco TAC does not support hardware or operating systems purchased directly from Sun or from any other vendor. Hardware support contracts should be purchased from Sun or the Sun value added reseller.

Hardware Requirements

Hardware available from Cisco Systems Inc. for PacketCable North American customers is listed below. Determine if you need AC or DC, and if you want the hardware in a cabinet or ready to mount in a customer rack. Work with a Cisco BTS 10200 product manager to determine the appropriate load for your situation.

The Cisco BTS 10200 Softswitch is available only in duplex (continuous-service) configurations.

[Table 1](#) lists the hardware requirements for the Cisco BTS 10200 Softswitch Call Agent (CA) and Feature Server (FS) platform.



Caution

Before choosing a hardware configuration, consult with your Cisco representative to determine the hardware that will give you the best results based on your network configuration, proposed traffic, and desired call processing power. In particular, called-number analysis or screening, long call hold times, and service control point (SCP) queries might require additional resources.

**Note**

Cisco Systems announced the end of sale and end of life for the SunFire V120s, Sun Netra 120s, and AXmp hardware and accessories. The last day to order these parts was January 1, 2005. Customers will continue to receive support from Cisco TAC until January 1, 2010. For more information, refer to the following EOS/EOL of BTS 10200 Hardware Web pages.

For Sun Fire V120s and Sun Netra 120:

http://www.cisco.com/en/US/products/hw/vcallcon/ps531/prod_eol_notice0900aecd800fe180.html

For AXmp:

http://www.cisco.com/en/US/products/hw/vcallcon/ps531/prod_eol_notice0900aecd800f896a.html

**Note**

Cisco Systems announced the end of sale and end of life for the Sun Fire V240s, V440s, 1280s, and Sun Netra 240s, 440s, and 1280s. The last day to order these parts was March 16, 2007. Customers will continue to receive support from Cisco TAC until March 14, 2012. For more information, refer to the following EOS/EOL of BTS 10200 Hardware Web page:

http://www.cisco.com/en/US/products/hw/vcallcon/ps531/prod_eol_notice0900aecd80532e24.html

The memory requirement for Release 4.5.1 is 8 GB. Using 4 GB (as in previous 4.x releases) may result in a loss of data while upgrading to Release 4.5.1, and users may need a fresh download if 4 GB memory is used.

For best results, Cisco recommends following the memory requirements listed in [Table 1](#).

Table 1 *Host Hardware Requirements*

Hardware	Processors	Required Memory for R4.x	Recommended Memory for R4.x	Disk Size
Sun Fire V240	2 x 1280	8 GB	8 GB	2 x 73 GB
Sun Netra 240	2 x 1280	8 GB	8 GB	2 x 73 GB
Sun Fire V440	4 x 1280	8 GB	8 GB	4 x 73 GB
Sun Netra 440	4 x 1280	8 GB	8 GB	4 x 73 GB
Sun Netra 1280	4 x 1200	8 GB	8 GB	2 x 73 GB
Sun Netra 1280	8 x 1200	16 GB	16 GB	2 x 73 GB
Sun Fire V1280	4 x 1280	8 GB	8 GB	2 x 73 GB
EMS	2 x 1280	4 GB	8 GB	2 x 73 GB

Installation Parameters

**Caution**

Do not modify any operating system parameters that the Cisco BTS 10200 Softswitch Jumpstart installs.

Interface Options


Note

In Release 4.5.1, the Cisco BTS 10200 system must use the 4/2 configuration.

The Cisco BTS 10200 Softswitch interface configurations are documented in the [Cisco BTS 10200 Softswitch Release 4.5 Cabling, VLAN, and IRDP Procedures](#).

In Release 4.5.1, the Call Agent (CA) requires four physical interfaces, and the Element Management System (EMS) requires two physical interfaces. If ordering your own hardware, make sure to purchase an adequate number of interfaces.

Optional Component (Hardware and Software)

The HTTP feature server (HTTP-FS) is an optional component of the Cisco BTS 10200 Softswitch that enables users to configure user parameters for certain applicable Cisco BTS 10200 features. It enables this by performing ASCII text-based (rather than tones) user-interaction to a CMXML-aware (v3.0 and above) SIP client.

For example, with a CMXML-aware Cisco 7960 IP phone, users can configure the Call Forwarding Unconditional (CFU) number using a text-based menu displayed on its LCD panel.


Note

Even though the LCD is capable of displaying graphical content, the HTTP-FS uses only text-based menus.

The HTTP-FS comprises two subcomponents: the GUI feature server (GUI-FS) and the Mini-Browser Adapter (MBA). To use the HTTP-FS, you must install the GUI-FS software package, which is part of the Feature Server for POTS/Tandem/Centrex (FSPTC). Install the FSPTC if it is not already installed.

Requirements for HTTP-FS

The Sun Fire V240 hardware and Solaris 8 are required to use the HTTP-FS. Load Solaris 8, and then install the MBA software package.


Note

The software for both the GUI-FS and the MBA are included in the software supplied with your Cisco BTS 10200 Softswitch.

Ancillary Hardware

If you are using reference sale hardware, the following pieces of ancillary hardware are required for use with the Cisco BTS 10200 Softswitch.

For AC Systems

You need two AC system switch routers configured as listed in [Table 2](#).

Table 2 *Ancillary Hardware for AC Systems*

Part Number	Description
WS-C2950M-XL-EN	Cisco Catalyst 2950m xl AC 10/100 Autosensing Fast Ethernet Switch

For DC Systems

You need two DC system switch routers configured as listed in [Table 3](#).

Table 3 *Ancillary Hardware for DC Systems*

Part Number	Description
WS-C2950M-XL-EN-DC	Cisco Catalyst 2950m xl DC 10/100 Autosensing Fast Ethernet Switch

or

WS-C2970G-24TS-E-DC	Cisco Catalyst 2970 xl DC 10/100 Autosensing Fast Ethernet Switch
---------------------	---

For All Systems

You need one alarm panel or your own terminal server that allows for console login. The Cisco BTS 10200 alarm panel is listed in [Table 4](#).

Table 4 *Ancillary Hardware for All Systems*

Part Number	Description
BTS10200-ALRM	Cisco BTS 10200 Alarm Panel

Cisco ITP Signaling Gateways

The Cisco IP Transfer Point (ITP) is required for SS7 interconnectivity. ITP is a comprehensive product for transporting Signaling System 7 (SS7) traffic over traditional time-division multiplexing (TDM) networks or advanced SS7-over-IP (SS7oIP) networks. You need Cisco ITP Signaling Gateways to provide SS7 interconnectivity for the Cisco BTS 10200 Softswitch in Release 4.5.1

**Note**

If using SS7 with Release 4.5.1, you must purchase ITP equipment as described here.

The Cisco IP Transfer Point is implemented on the Cisco 2600XM Series Router (2650XM, 2651XM), the Cisco 7200 Series Router (7204VXR, 7206VXR), the Cisco 7301 Router and the Cisco 7500 Series Router (7507, 7513). All hardware models function similarly by performing MTP3 routing over SS7 TDM links or over an IP (or dual IP) network.

The Cisco ITP 2651, 7301, and 7507 Signaling Gateways are carrier class routers with a transparent SS7oIP convergence solution. The 26xx offers 2 or 4 SS7 links, the 73xx supports up to 80 SS7 links, and the 7507 provides from 32 to 256+ SS7 links.

**Note**

When running ITP with Cisco BTS 10200, you may encounter an “Unrecognized Parameter” error message. The message appears because the Cisco BTS 10200 supports an optical SCTP feature that is not supported on the ITP, but it does not affect calls or performance.

Because the Cisco BTS 10200 and ITP both handle SS7 traffic using Sigtran protocols, they must be fully compatible in the version of the SCTP transport protocol used.

For more information on the ITP equipment, see the [Cisco ITP Product Data Sheet](#).

Table Sizes

To check the size of all tables specific to your BTS 10200 configuration, perform the command **show db-usage**.

Software Requirements

The Cisco BTS 10200 Softswitch Release 4.5.1 (900-04.05.01.Vxx) software is required for you to run the Cisco BTS 10200 Softswitch on the hardware platforms.

Definition of Major, Minor, and Maintenance Releases

The following section describes the differences between major, minor, and maintenance releases.

Major Release

A major software release has significant new features, enhancements, architectural changes, and/or defect fixes. The major release number increments with each new version, and numbers may NOT be skipped in deliveries to customers. This release is based on previous Main release and receives defect fixes synced from previous main releases throughout the life of this release.

Minor Release

A minor software release has only a few new features of limited scope, enhancements and/or defect fixes. The minor release number increments as content is added and numbers may be nonsequential (skipped). This release is based on a previous release and receives defect fixes synced from previous major or minor releases throughout the life of this release.

Maintenance Release

A maintenance software release has defect fixes that address specific problems. The maintenance release number increments as content is added and numbers can be nonsequential (skipped).

Release Naming Conventions

The Cisco BTS 10200 product release version numbering is defined as either:

- Cisco BTS 10200 uu.ww.xx.yzz Pxx (for example, in the Release Notes)
- 900-uu.ww.xx.yzz Pxx (as a part number on a CD; also noted in Packaged-IN-XX.XX(XX) DDTS enclosure)

where:

- uu is the (major) Release ID (0–99)—for example: 900-03.ww.xx.yzz
- ww is a point (minor) release (within a major) (0–99)—for example, 900-03.05.xx.yzz
- xx is the maintenance package number (within a point) (0–99)—for example, 900-03.05.03.yzz
- y is the Software State, such that—for example, 900-03.05.03V00
 - D = Development load
 - I = Integration load
 - Q = System test load

- F = Field verification ready
- V = Verified (specified for externally available)
- When Pxx is at the end of the release numbering, a patch has been applied. P is the patch, and xx is the patch number.

Some naming convention examples are:

- 900-04.01.00V03
- 900-04.04.00.V01
- 900-04.04.01.V00
- 900-04.05.00.V01

Network Time Protocol Software



Note

Cisco BTS 10200 automatically installs and runs the Network Time Protocol (NTP) time synchronization software. However, you must specify which NTP servers to use with your installation, and you must use NTP servers that are rated STA 3 or better. For information on how to reconfigure the NTP, refer to the Release 4.5 installation procedure.

NTP software is installed with Sun Solaris. Be sure to configure your Cisco BTS 10200 Softswitch to use NTP or the equivalent time synchronization software.



Caution

Users should never attempt to modify the system date or time in their Cisco BTS 10200 Softswitch host machines while system components (CA, FS, EMS, and BDMS) are running. Doing so can cause the system to have serious problems. Allow the Solaris OS to obtain the time automatically through NTP services.

Sun Solaris Version Upgrade

The Sun Solaris software was upgraded to Version 10; the upgrade is part of the Release 4.5 upgrade. For information about the Netscape browser requirements in Release 4.5, refer to the EPOM datasheets.

Optional Software

The following optional software can also be used with Cisco BTS 10200 Softswitch Release 4.5.1.

Cisco Extensible Provisioning Object Manager

You can use the Cisco Extensible Provisioning Object Manager (EPOM) Release 4.5 software as a provisioning tool for Cisco BTS 10200 Softswitch Release 4.5.1.



Note

EPOM 4.5 is the only version intended to work with Cisco BTS 10200 Release 4.5.1.

EPOM requires its own host server. For more information, refer to the [Cisco EPOM Getting Started Guide](#).

CORBA and OpenORB

The CORBA Adapter (CAD) interface is an object-oriented provisioning tool for the BTS 10200 that parallels the BTS 10200 CLI adapter in capability.

The CAD uses the OpenORB 1.3.1 interface to develop and deploy distributed object-based applications, as defined in the CORBA specification 2.4. OpenORB is a third party software package that leverages the Internet Inter-ORB Protocol (IIOP) using either the Transmission Control Protocol or the User Datagram Protocol (UDP) for connections.

For detailed information on CORBA and OpenORB, refer to the [CORBA Adapter Interface Specification Programmer Guide](#).

Cisco Self-Service Phone Administration

You can use the Cisco Self-Service Phone Administration (SPA), Version 1.1, which allows phones to be organized into accounts and managed by end users to manipulate existing features and query account information without service provider intervention. This reduces service provider costs, while enhancing the end user's product experience. When the service provider has installed Cisco SPA and configured it using the Cisco SPA operation and configuration tool, all that remains is creating accounts for users to manage using their own phones. The Cisco SPA application and the Cisco SPA operation and configuration tool are described in the [Cisco SPA Installation and Users Guide](#).

Component Interoperability

Table 5 lists specific peripheral platforms, functions, and software loads used in system testing for interoperability with the Cisco BTS 10200 Softswitch Release 4.5.x software. Earlier or later releases of platform software might be interoperable, and it might be possible to use other functions on these platforms. This list certifies only that the required interoperation of these platforms, the functions listed, and the protocols listed has been successfully tested with the Cisco BTS 10200 Softswitch.

Table 5 *Component Interoperability Matrix*

Platform(s) Tested	Function(s) Tested	Protocol(s) Tested	Load(s) Tested
Cognitronics CX500	Announcement Server	MGCP 1.0	3.0
IP Unity Harmony 6000	Privacy Director	SIP RFC3261	3.1
IP Unity Harmony 6000	Voicemail Server	SIP RFC3261	3.1
IP Unity Harmony 6000	Announcement Server	SIP RFC3261	3.1
Cisco IAD 242x	Residential/Business Gateway	MGCP 1.0	12.3(21)
Cisco IAD 243x	Residential/Business Gateway	MGCP 1.0	12.4(4)T5
Cisco Cat 3550	Ethernet Switch		121-22.EA6
Cisco Cat 2950	Ethernet Switch		121-22.EA6
Cisco MGX 8850 VISM	Trunking Gateway	MGCP 1.0, TGCP	3.53.30.203
Cisco MGX VXSM	Trunking Gateway	MGCP 1.0, TGCP	5.3.10.201-P2
Cisco AS5300	Trunking Gateway ¹	MGCP 1.0, TGCP	12.4.12
Cisco AS5350	Trunking Gateway ¹	MGCP 1.0, TGCP	12.4.12
Cisco AS5400	Trunking Gateway	MGCP 1.0, TGCP	12.4.12
Cisco PXM45/AXSM	Trunking Gateway	MGCP 1.0, TGCP	5.52(10.255)D
Cisco PXM1-4-155	Trunking Gateway	MGCP 1.0, TGCP	5.3.1
Cisco VISM-PR	Trunking Gateway	MGCP 1.0, TGCP	5.2.00
Cisco RPM	Trunking Gateway	MGCP 1.0, TGCP	12.4(6)T6
Cisco 2651 ITP	SS7 Signaling Gateway	SIGTRAN M3UA/SUA	12.2(25)SW9
Cisco 73xx ITP	SS7 Signaling Gateway	SIGTRAN M3UA/SUA	12.2(25)SW9
Cisco 750x ITP	SS7 Signaling Gateway	SIGTRAN M3UA/SUA	12.2(25)SW9
Cisco uBR7246VXR Router	CMTS	PacketCable EM 08	12.3(13a)BC3
Cisco uBR 10K	CMTS, CALEA	CALEA SII, PCCMTS	12.3(17b)BC3
Cisco MSFC1	IP Core–Cat 6500		6.4-20
Cisco MSFC1	IP Core–Cat 6500		121-26.E4

Embedded MTAs

Table 5 **Component Interoperability Matrix (continued)**

Platform(s) Tested	Function(s) Tested	Protocol(s) Tested	Load(s) Tested
Arris TM402P	eMTA	NCS 1.0, IPSEC	TS040559_022406_MODEL_4_5_TELNET_ON
Motorola SBV5220	eMTA	NCS 1.0, IPSEC	2.16.1.1
Motorola SBV5120	eMTA	NCS 1.0, IPSEC	2.16.1.1
Motorola SBV4200	eMTA	NCS 1.0, IPSEC	2.16.1.1
Scientific Atlanta Dpx2203	eMTA	NCS 1.0, IPSEC	v1.1.2r1151-050224b-5
SIP Endpoints			
Linksys PAP2	SIP endpoint	SIP	3.1.5(Lsd)
Cisco ATA188	SIP endpoint	SIP	3.2.1
Policy Servers			
Camiant Multimedia Service Controller	Policy server		2.3
CableMatrix On-Demand Service Platform (ODSP)	Policy server		1.0.0b6

1. The Cisco AS5300 and AS5350 have also been tested as Announcement Servers

Gateway Caveat

An invalid CRCX (inactive + r:cl) is sent during call waiting scenarios. The Cisco IOS gateway generates error 524 for a CRCX with “L: ..., r:cl” and “M: inactive” on a call waiting scenario when the media gateway for the call waiting subscriber is provisioned to use “CL” for RSVP.

This is a Cisco IOS media gateway issue, not a Cisco BTS 10200 Softswitch issue. The workaround for this is to not use CL for RSVP for the media gateway.

H.323 Applications

H.323 applications are supported in Release 4.5.1, but not Release 4.5.0.

Operator Access

Operator access to the Cisco BTS 10200 Softswitch is available only by secure shell (SSH) session to the EMS over Ethernet. The Cisco BTS 10200 Softswitch does not support nonsecure FTP; in order for you to FTP to any other system, your Cisco BTS 10200 Softswitch system must have secure FTP (SFTP) capabilities.

For security purposes, SSH access is limited to using defined management interfaces.

Installation Notes

Before running an installation, plan accordingly, by using the *Site Preparation and Network Communications Requirement* document, the *Network Site Survey*, and a *Building and Environment Site Survey*.

For detailed installation procedures on installing the Release 4.5.x software, refer to the CD Jumpstart Procedure and Application Installation for Duplex Systems links in the *Cisco BTS 10200 Softswitch Application Installation Guide*.

Installing the Cisco BTS 10200 Softswitch consists of following:

1. Installing and cabling the hardware
2. Running the jumpstart procedure
3. Running the software (application) installation procedure

After installing and cabling the hardware, use the jumpstart procedure to have the system jumpstarted with the proper OS version and kernel patch level. Once the system is configured properly, you can begin the application installation.



Note

The application installation procedure is for duplex systems, the only installation type supported for Release 4.x.

Upgrade Procedures



Note

All customers **must** be on the latest load of a release prior to executing any upgrade procedure.

A procedure is available for customers upgrading between Cisco BTS 10200 releases. The procedures are provided for customers upgrading from the following releases:

- From Release 4.5.0V13 to 4.5.1Vxx
- From Release 4.5.13V06 to 4.5.1Vxx
- From Release 4.5.13V08 to 4.5.1Vxx
- From Release 4.5.1Vxx to 4.5.1Vyy

For additional information about the upgrade or fallback procedures, refer to the “[Enhanced Software Upgrade](#)” section.

The upgrade guide is available from the [Cisco BTS 10200 Release 4.5.x Installation and Upgrade Guides](#) Web page.

Upgrades and SIP Session Timers

SIP Session Timer values configured prior to Release 4.5.1 are reset to the default values after you upgrade to Release 4.5.1. Additionally, you cannot configure the SIP session timers, such as minSE and session_expires_delta_secs, on the CA-CONFIG table.

To configure the SIP timers, you must use the new SIP-TIMER-PROFILE table and reference that in the CA-CONFIG table.

Upgrades and CALEA

The following information is relevant for CALEA users upgrading from Release 3.5.5 to Release 4.5.x.

In some cases, CALEA will not function after upgrade without the CALEA-related components being modified. Use the following steps for Task 7, Continue Upgrade Process, in the Release 3.5.5 to 4.5.x upgrade guide to ensure that CALEA functions properly.

Once side B is active with Release 4.5.x, go to SSDF and make the following modification:

```
MODIFY-AFRI:AFID=Cactus-TWC,IFID=1,IPADDR=qfe0_ip,PORT=14146,VERSION=I08;
MODIFY-AFRI:AFID=Cactus-TWC,IFID=2,IPADDR=qfe1_ip,PORT=14146,VERSION=I08;
```



Note

To use SII architect for wiretapping, leave the CCCID field in IPCC blank in the surveillance provision.

Caveats

Caveats are not listed in the Release Notes. Instead, caveats are available through the online tool, [Bug Toolkit](#), allowing customers to query defects according to their own needs.

Bug Toolkit

To access Bug Toolkit, you need an Internet connection, a Web browser and a Cisco.com username and password.



Note

Use your Cisco.com username and password when accessing Bug Toolkit, not the Cisco BTS 10200 Softswitch documentation username and password. If you access Bug Toolkit from the Cisco BTS 10200 documentation page, the Cisco BTS 10200 documentation username and password are the default. Change the default to your Cisco.com username and password instead.

To use Bug Toolkit, follow this procedure.

Step 1 Click [here](#) to log onto Bug Toolkit. You must have a Cisco.com user name and password.

Step 2 Click the **Launch Bug Toolkit** hyperlink.

Step 3 To find a specific caveat, enter the ID number in the “Enter known bug ID” field.

To view all caveats for Cisco BTS 10200, go to the “Search for bugs in other Cisco software and hardware products” section, and start typing **BTS** in the Product Name field.



Note

Cisco BTS 10200 Softswitch appears after you type the first two letters, B and T.

Step 4 Click **Next**. The Cisco BTS 10200 Softswitch search page appears.

Step 5 Select the filters to query for caveats. You can choose any or all of the available options.



Note

To make queries less specific, use the All wildcard for the Major/Minor release, Features/Components, and keyword options.

Step 6 To query by version (see [Definition of Major, Minor, and Maintenance Releases, page 7](#)):

- Select **Major** for the major releases (that is, 4.5, 4.4, 4.2, 4.1, 3.5, 3.3, 3.2, 3.1).
- Select **Minor Release** for more specific information—for example, selecting Major Version 3.5 and Minor Version 4 queries for Release 3.5.4 caveats.
- Select the **Features or Components** to query.
- Use keywords to search for a caveat title and description.
- Select the **Advanced Options**, including the Bug Severity level, Bug Status Group and Release Note Enclosure options.
- Click **Next**.

Bug Toolkit returns the list of caveats based on your query.

Errata

The Feature Descriptions document for Release 4.5x (http://www.cisco.com/en/US/docs/voice_ip_comm/bts/4.5/feature/description/fd201sft.html#wp1228569) lists an incorrect dial tone duration of 4 seconds for the Call Hold (CHD) feature. The current wording is "If the activating party does nothing, the network waits 4 seconds, then removes the dial tone." However the actual behavior is: If the activating party does nothing, the network waits 16 seconds, then removes the dial tone and provides an announcement.

New or Enhanced Features for Release 4.5.1, Maintenance Release 2

New feature documentation for Release 4.5.x can be accessed at:

http://www.cisco.com/en/US/products/hw/vcallcon/ps531/products_feature_guides_list.html.

The following features were added or enhanced in Release 4.5.1, Maintenance Release 2 (MR2):

- [Colombia ISUP](#)
- [OpenSSH Upgrade](#)
- [Audit Performance Enhancement](#)
- [SIP Diversion Header Enhancement](#)
- [Multiline Hunt Group Call Transfer](#)
- [ISDN Table Size Increase](#)
- [Support for Sun T2000 IPGE Ethernet Interface](#)
- [Privacy Parameters in SIP Diversion Header](#)
- [Account Codes for Local Calls](#)
- [CODEC-NEG-SUPP Token in the Media Gateway Profile](#)
- [MGCP Debug Message Enhancement](#)

Colombia ISUP

Release 4.5.1 MR2 supports the Colombia ISUP Q.767 variant on the BTS 10200 Softswitch.

This feature adds a new value to the installed default variant base. A new id token, Q767_Colombia, is added to the User Part Variant Base and User Part Variant tables.

OpenSSH Upgrade

OpenSSH is a third-party SSH connectivity tool. Prior to Release 4.5.1 MR2, the BTS 10200 Softswitch used the OpenSSH 4.2p1 package. For Release 4.5.1 MR2, the OpenSSH package is upgraded to OpenSSH 4.4.

Audit Performance Enhancement

This enhancement reduces the time of a BTS 10200 EMS-A to EMS-B database audit by two-thirds. In a system with 200,000 subscribers, the audit completes in 7.5 minutes with no impact on EMS operations. The user enters the existing commands, **su-oracle** and **dbadm-C db**, to execute the audit.

SIP Diversion Header Enhancement

The BTS 10200 imposes limits on the decoding of incoming SIP messages. These limitations protect the system from performance problems due to the decoding of extremely large messages.

Prior to Release 4.5.1 MR2, the maximum number of allowable parameters in the SIP Diversion Header was five. Beginning with Release 4.5.1 MR2, the maximum number of allowable parameters is increased to ten. For more detailed information on SIP messages and maximum parameters, refer to the [Cisco BTS 10200 Softswitch SIP Protocol User Guide](#).

Multiline Hunt Group Call Transfer

In Release 4.5.1 MR2, the Multiline Hunt Group (MLHG) call transfer feature allows all members of a MLHG to perform attended call transfers with 3-way calling. Members of a MLHG must be subscribed to call transfer and 3-way calling service in order to use the MLHG call transfer feature.

ISDN Table Size Increase

In Release 4.5.1 MR2, the following BTS 10200 ISDN tables were increased in capacity:

- ISDN DCHAN
- ISDN_INTF
- BACKHAUL_SET
- RUDP_BACKHAUL_SESSION

The BTS 10200 now supports up to 2000 ISDN trunk groups.

Support for Sun T2000 IPGE Ethernet Interface

The Sun Netra T2000 has four 1 GB ipge ports integrated into its motherboard. Beginning with Release 4.5.1 MR2, the BTS 10200 is enhanced to support these new ipge interfaces.

Privacy Parameters in SIP Diversion Header

In Release 4.5.1 MR2 and later, if the SIP diversion feature is enabled, privacy parameters are sent and received in the SIP Diversion header for INVITEs sent out on a BTS 10200 SIP trunk.

Also, if the original called number (OCN) and/or the redirected DN (RDN) are being sent in Diversion headers towards local SIP subscribers, the system applies 'anonymous' to the headers as follows:

- If an OCN exists, it populates the URL as anonymous@anonymous.invalid in the To header.
- If a Diversion header is added, it populates the 'user' part of the header with 'anonymous'.

For more information on the SIP diversion header feature and privacy parameters, refer to the [Cisco BTS 10200 SIP Protocol User Guide \(Release 4.5.x\)](#).

Account Codes for Local Calls

Prior to Release 4.5.1 MR2, the BTS 10200 supported account codes for long distance calls only. In Release 4.5.1 MR2 and later, the BTS 10200 is enhanced to support account codes for local calls in addition to long distance calls.

CODEC-NEG-SUPP Token in the Media Gateway Profile

In Release 4.5.1 MR2, the CODEC-NEG-SUPP token enforcement is updated in the Media Gateway (MGW) Profile table. This parameter specifies a list of codecs common to both sides of a call in the local connection option (LCO) parameter of the create connection (CRCX) message. The default value for this parameter is 'Y'. Available codec types are listed in the Quality of Service (QoS) table, using the codec-type token.

For more information on the CODEC-NEG-SUPP token, refer to “Office Provisioning—Media Gateway Profile Table, page 2-34” of the *Cisco BTS 10200 Softswitch Command Line Interface Reference for Call Processing*.

MGCP Debug Message Enhancement

During certain conditions, debug messages appear in the BTS 10200 call trace logs. This enhancement allows printing the content of MGCP messages that are sent/received at default trace level (INFO3). This can be done under the following conditions:

- When the BTS 10200 receives NACK (return code larger than 299, other than 401/402) for MGCP commands sent to the endpoint, the response message is printed along with the original command sent by the BTS 10200.
- When the BTS 10200 retransmits MGCP commands to the endpoint. An exception is periodically sent keep-alive AUEP messages.
- When the BTS 10200 receives RSIP messages from the endpoint or MGW.
- When the BTS 10200 receives Gateway initiated DLCX commands.

New or Enhanced Features for Release 4.5.1, Maintenance Release 1

New documentation for Release 4.5.x can be accessed at:

http://www.cisco.com/en/US/products/hw/vcallcon/ps531/products_feature_guides_list.html.

The following features were added or enhanced in Release 4.5.1, Maintenance Release 1 (MR1):

- [Fast Audit and Sync Tools](#)
- [Network Loopback Test for ISDN PRI Trunks](#)
- [Block Provisioning](#)
- [Validation of Source IP Address for Incoming SIP Messages](#)
- [Virtual IP Address Functionality for CORBA Adapter](#)
- [Optional Prefix Dialing for Toll and Toll-Free \(8xx\) Calls](#)
- [Media Gateway—Unreachable Condition](#)

Fast Audit and Sync Tools



Note

The `bts_audit` and `bts_sync` process tools should be used only during maintenance windows due to high CPU usage requirements.

The Cisco BTS 10200 Softswitch Fast Audit and Sync Tools feature consists of two expect shell scripts that use other unix scripts and utilities to perform full-database and table audits of the databases on the various network elements of the system, and synchronize the mismatches found. The `bts_audit` tool determines the tables when performing full database audit by analyzing the catalog of the CA, FSPTC and FSAIN databases. The scripts will create copies of the data from the tables in a standardized format. The data files are used to generate a checksum for each table. The check sums are compared, and if they are not equal, the network element data file will be transferred to the EMS. On the EMS, the data is compared row by row, and mismatches are printed to a file that may be used by the `bts_sync` tool to restore synchronization of the table on the network element.

The `bts_audit` tool is able to:

- Find tables with mismatches
- Find rows missing in application database
- Find rows missing in EMS database
- Find rows with data mismatches between two databases
- Generate a report that lists these mismatches
- Generate the SQL to be used to correct the mismatches

The `bts_sync` tool is used to send the generated SQL statements to the appropriate destination to bring the databases into synchronization.

Release 4.5.1 or later of the Cisco BTS 10200 Softswitch software must be installed and operating on the system to utilize the Cisco BTS 10200 Softswitch Fast Audit and Sync Tools feature.

Network Loopback Test for ISDN PRI Trunks

Network Loopback Test for ISDN PRI trunks (ISDN NLB) feature allows operators to conduct network loopback testing originating from shared ISDN PRI trunks. The shared test trunk group accepts both normal and NLB test calls. NLB test calls are identified by provisioning the call-type and call-subtype tokens in the Destination table.

The Cisco BTS 10200 Softswitch cannot perform network loopback test calls that originate from another switch and does not route NLB test calls from a testing device on an H.323 or SIP interface.



Note

The network loopback test cannot be performed if the status of the subscriber to be tested is **unequipped (UEQP)** or **operational-out-of-service (OOS)**.

For detailed information on this feature, refer to the feature module.

Block Provisioning

The Block Session Enhancement allows users of the Cisco BTS 10200 Softswitch to prevent provisioning during an upgrade or maintenance window. The Block Session Enhancement can block/unblock a specific session type, or a specific session user. You can block provisioning from the following interfaces:

- CLI
- FTP
- CORBA
- SNMP

The Block Session Enhancement features two levels of blocking:

- PROVISION—prevents all provisioning commands from executing
- COMPLETE—prevents all commands from executing

Only terminal type “MNT” users can use block provisioning, and “MNT” users are never blocked from provisioning. “MNT” users can block provisioning from either the Active or Standby side of the EMS.

When used, the Block Session Enhancement feature applies to all non-“MNT” users on terminals on either the Active or Standby side of the EMS. The commands of users already logged in, or those who login after the block command is issued, are prevented from executing.

The Block Session Enhancement is designed to remain in effect during the entire upgrade or maintenance window. After the upgrade or maintenance is complete, the unblock command clears the blocked state on both the Active and Standby side of the EMS.

For more information, refer to the [Cisco BTS 10200 Softswitch Operations and Maintenance Guide](#).

Validation of Source IP Address for Incoming SIP Messages

The Cisco BTS 10200 Softswitch can perform source IP address validation of incoming messages received on SIP trunks. This validation process is intended to reduce the risk of security attacks, which can occur if a packet is sniffed in the network and then sent from a different or rogue IP address, or domain, as present in the Via header. By default, IP address validation is disabled on the Cisco BTS 10200 Softswitch. The service provider can enable this capability using the SIA-TG-VALIDATE-SOURCE-IP token in the ca-config table. This is a switch-wide parameter, and applies to all SIP trunk groups.

Provisioning details can be found in the [Chapter 2](#) of the [Cisco BTS 10200 Softswitch SIP Protocol Provisioning Guide](#).

Virtual IP Address Functionality for CORBA Adapter

Beginning with Release 4.5.1, Maintenance Release 1 (MR1), the CORBA Adapter (CAD) installation automatically uses Virtual IP (VIP) Address as the iop.hostname. VIP allows the NameService to listen to all IP addresses on the active EMS. The VIP feature is configured through the CLI.

The CORBA installation automatically selects the VIP (Virtual IP) if the VIP is configured, otherwise the first management IP address is selected. This change will be seen in the `/etc/inittab` folder.

Refer to the [CORBA Adapter Interface Specification Programmer Guide](#) for information on how to change the network configuration for CORBA and for more information on the VIP functionality.

Optional Prefix Dialing for Toll and Toll-Free (8xx) Calls

The BTS 10200 Softswitch can be provisioned to specify whether dialing a prefix 1 for 500, 800 (toll-free), 900, and toll calls is required. If dialing a prefix 1 is required and not dialed, an announcement is played. The following token is updated in the CLI Subscriber Service Profile table:

TOLL-PFX1-OPT

- VARCHAR(3)—1–3 ASCII characters (Default=RQ)
- RQ (Default)—Prefix 1 required
- NR—Prefix 1 not required
- OPT—Prefix 1 is optional (ok to dial if prefix 1 not dialed)

For more information, refer to the Subscriber Service Profile table in the *Cisco BTS 10200 Softswitch CLI Guide*.

Media Gateway—Unreachable Condition

Beginning in Release 4.5.1 MR1, you can provision the BTS 10200 through CLI to release calls if and when the MGW becomes unreachable. This enhancement uses the SPARE1-SUPP token in the MGW-Profile Table.

Prior to this release, the BTS 10200 did not release calls if the MGW was unreachable. This default behavior was not configurable.

This enhancement allows you to configure the SPARE1-SUPP token:

- Y—If the MGW is unreachable, then all active calls on the MGW are released.
- N—If the MGW is unreachable, then all active calls on the MGW are not released.

For more detailed information, refer to the MGW-Profile Table in the *Cisco BTS 10200 Softswitch CLI Guide*.

New or Enhanced Features for Release 4.5.1

The following features were added or enhanced in Release 4.5.1:

- [French ISUP](#)
- [ITU LNP](#)
- [Mexico ISUP](#)
- [Thailand ISUP](#)
- [T.38 Fax with SIP Endpoints](#)
- [Metered Billing Featurette](#)
- [H.323 Support](#)
- [Table Size Increase](#)
- [CORBA SDK](#)
- [EM Privacy Indicator](#)
- [Poland ISUP Support](#)

- [Poland LNP](#)
- [Privacy Manager with Cognitronics](#)
- [Automatic Shared Memory Backup](#)
- [Internal Secondary Authoritative DNS](#)

French ISUP

The French ISUP is an ISUP variant named Q761_ETSIV3_FRENCH ISUP, which is based on the 1997 version of Q.761/ISUP V3. The French ISUP feature supports and works in conjunction with the ITU LNP feature on the Cisco BTS 10200 Softswitch.

ITU LNP

Release 4.5.1 introduced the International Telecommunication Union (ITU) Local Number Portability (LNP) feature for the Cisco BTS 10200 Softswitch.

Local Number Portability (LNP) gives a telephone customer the ability to retain a local phone number if he or she switches to another local telephone service provider either within or outside the same geographic area.

To enable LNP functions on the Cisco softswitches, the Cisco BTS 10200 Softswitch maintains subscriber porting data in an internal database in the DN2RN table. In some countries, the system periodically connects to the country's central database and downloads the most recent set of LNP updates. These updates are stored in the DN2RN table in the Cisco BTS 10200 Softswitch's internal data format.

Mexico ISUP

Release 4.5.1 supports the Mexico ISUP variant, NOM112, on the Cisco BTS 10200 Softswitch. Mexico ISUP support also requires implementation of the Q.767 protocol family.

This feature provides SS7-based connectivity to the PSTNs in various countries, along with a large suite of local subscriber services. The requirement is for support with the ITP SS7 SG providing the SS7 access.

Mexico ISUP provides the service provider full and partial E1 access for delivering small business voice services.

Thailand ISUP

Release 4.5.1 also supports the Thailand ISUP variant, based on the ITU-T Q.761-4 specifications and part of Q767, on the Cisco BTS 10200 Softswitch.

This feature adds a new value to the installed default variant base. It introduces the value Q761_Thailand for the ID token in the User Part Variant Base and User Part Variant tables.

T.38 Fax with SIP Endpoints

In Release 4.5, the T.38 fax relay feature did not support SIP endpoints. However, the feature was updated for this version, and Release 4.5.1 now supports SIP endpoints.

Metered Billing Featurette

The new Release 4.5.1 featurette, metered billing, allows the Cisco BTS 10200 Softswitch to collect metered “pulses” from operators signaled to UPC via SPIROU (French ISUP) ITX messages.

This SS7 messaging is used for audio services that are paid by for by either a flat rate calculation or a time-based calculation. The calls are routed to the operator, and the operator reports the payment amount by the ITX messages. Every ITX has the same value.

For example, if 1 charging unit was equivalent to 0.1 Euro and a caller dialed a service such as a weather forecast with a 1 Euro fee, then the network would send 10 ITX messages.

H.323 Support

H.323 applications were not supported in Release 4.5.0, but are supported in Release 4.5.1. The Cisco BTS 10200 Softswitch implements H.323 interfaces and functions in Release 4.5.1, and also provides H.323 provisioning, operating, and troubleshooting procedures.

In Release 4.5.1, information about the reattempt, route advance, and hairpinning (redirect) functions was updated and enhanced. A new token (SEND-FS-CALLP) was added in the H.323 Trunk Group Profile (h323-tg-profile) and H.323 Terminal Profile (h323-term-profile) tables to control sending of the Fast Start parameter. Previously (in Release 4.4.1 and earlier), this functionality used the MISC-UNSUPP token.

T.38 fax functionality was also enhanced in Release 4.5.1:

- Descriptions of the enhancements were added.
- Tokens for T.38 fax functionality (in the h323-tg-profile and h323-term-profile tables) were changed. The FAX_T38_GWMODE_SUPP and FAX_T38_CAMODE_SUPP tokens were deleted, and the REMOTE-FAX-PORT-RETRIEVAL-MSG token was added.
- In the QoS table, the FAX-PREF-MODE token was deleted and the FAX-T38-ENABLED token was added.
- New information was added on fax procedures, limitations, and prerequisites.

The sample provisioning script was updated.

Table Size Increase

In Release 4.5.1, the following Cisco BTS 10200 Softswitch tables were increased to support future expansion:

- The TERMINATION table
- The SUBSCRIBER-SERVICE-PROFILE table
- The SUBSCRIBER-FEATURE-DATA
- The SLE table
- The CHANGED-NUMBER table

However, with these new limits, a medium configuration must not exceed the 8 GB limit.

With the new table sizes, the Cisco BTS 10200 system generates an informational event when the tables reach their maximum capacity between 80% and 100%.

CORBA SDK

Release 4.5.1 adds support for the CORBA adapter architecture and application programming interface (API) for the Cisco BTS 10200 Softswitch. The CORBA adapter (CAD) interface leverages the adapter architecture of the Element Management System (EMS) component in the Cisco BTS 10200 Softswitch. This architecture allows for a variety of adapters to provide operations, administration, management, and provisioning (OAM&P) by adapting the external interface to a common infrastructure in the EMS.

Beginning with Release 4.5.1, the default idle time for a CORBA interface session is 10 minutes. If you do not execute a valid command within a 10 minute period, the session is declared idle, removed from the interface, and all resources are closed.



Note

You can configure the idle time parameter through the `bts.properties` file of the CIS application. The `bts.properties` file is located on the BTS 10200 in the `/opt/BTScis/etc` directory. The CORBA server must be restarted after `bts.properties` is changed.

For more information, refer to the [Cisco BTS 10200 Softswitch CORBA Adapter Interface Specification Programmer Guide](#).

EM Privacy Indicator

In Release 4.5.1, a privacy indicator is added to the Signaling Start EM. This attribute uses the previously undefined field #12 in PKT-SP-EM1.5-I02-050812. This field is populated if the EM-PRIVACY-IND-SUPP token in the CA-CONFIG table is set to Y.

Poland ISUP Support

Release 4.5.1 adds support on the Cisco BTS 10200 Softswitch for Polish ISUP Version v2, based on the European Telecommunications Standards Institute (ETSI) V2 ISUP.

Poland LNP

Poland LNP is supported in Release 4.5.1.

Privacy Manager with Cognitronics

Release 4.5.1 introduces support for the Privacy Screening with a Cognitronics Application Server (AS) feature. The Privacy Screening feature enables a subscriber to accept or reject an anonymous call based on a short message recorded by the caller. This feature allows the caller to:

- Record a short message—After listening to the message, the subscriber can accept or reject the incoming call or forward it to voice mail.
- Enter a passcode—Entering the correct passcode rings the subscriber, and the call becomes a regular call.

This feature also allows the Privacy Screening subscriber to activate or deactivate the Privacy Screening feature and change his or her PIN.

Privacy Screening works in conjunction with a Cognitronics Privacy Screening Application and Media Server (MS).

Automatic Shared Memory Backup

The Automatic Shared Memory Backup (ASMB) feature provides the user the ability to quickly recover a Call Agent/Feature Server (CA/FS) system in the event of disaster. The ASMB feature periodically backs up the IDX shared memory database on the CA/FS. If the shared memory is corrupted, then the last backup will be used to automatically recover the system.

For more information, refer to the ASMB feature in the Disaster Recovery chapter of the [Cisco BTS 10200 Softswitch Troubleshooting Guide](#).

Internal Secondary Authoritative DNS

The Cisco BTS 10200 Softswitch Internal Secondary Authoritative DNS feature provides the Cisco BTS 10200 Softswitch customers with an internal DNS database identical to the DNS database in the network. In the event of a long DNS outage in the network, or any prolonged network outage, or the external DNS servers fail, the internal DNS server can still provide response to any DNS queries and the Cisco BTS 10200 Softswitch can still perform the usual functions without interruption.

The purpose of internal secondary authoritative DNS server (ISADS) is to shadow the primary DNS server. In case the primary DNS server has a long outage, the ISADS will have a local database in the Cisco BTS 10200 Softswitch system that can provide authoritative response to any DNS queries by Cisco BTS 10200 Softswitch applications.

New Features for Release 4.5

- Telephony Features
 - MLHCentrexGroupName Data for Billing Call Detail Records
 - Temporarily Disconnected Subscriber Status and Soft Dial Tone
 - Block Toll Free Calls per Subscriber
 - Star Code to Access Voice Mail
 - Single Vertical Service Code to Activate or Deactivate Call Forwarding No Answer and Call Forwarding on Busy
 - Stand-Alone Call Redirection to Voice Mail
 - Inter-LATA Option
 - Privacy Director or Calling Identity with Enhanced Screening
 - No Solicitation Announcement
 - Trace Active Call per Directory Number and Trunk Identification
 - T.38 Fax Relay Call Agent Controlled Mode Across SIP Trunk Interface
 - Account/Authorization Code Support on PRI Trunks
 - Alerting Notification to Third-Party Feature Server
- Operational Features
 - Network Continuity Test and TDM Test Enhancements
 - Alarm Correlation Enhancements
 - CDB File Naming Convention
 - Support of SUN 1280 (8 CPUs)
 - Measurement Report on a Per Market (POP) Basis
 - 30 Originating Point Codes
 - Encrypted IPSEC Keys
 - .DONE Indicator After Successful Transmission of Call DB Records to Billing Mediation Server
 - Enhanced Software Upgrade
 - Secure Provisioning for SIP Endpoints
 - Testing Capability Required for 911 FGD-OS Trunks
 - Support for 2048 Bytes in Digit Map
 - Better Management of Alarms
 - Hungarian ISUP
 - ITU Local LNP
 - North American Numbering Plan Administration Audit Feature
 - ISUP Transparency on the Cisco BTS 10200-Cisco PGW 2200 Interface
 - Limited Call Duration Service (Prepaid/Postpaid)
 - Web Report Interface Authentication

- Log Archive Facility
- Other Enhancements
 - IP Addresses
 - Solaris 10
 - Oracle 10g
 - Display of System Status
 - Own Calling Number Announcement
 - Billing Record Cause Codes
 - Billing Record Enhancements
 - Alarms/Events Reported for DNS Failures
 - ACR and SS7 Incoming Calls
 - OverDecadic Digit Support for Generic DN Parser
 - NDC Now Optional
 - Parameters for Noun=User Are Changeable
 - Password Key Added for CLI User Command
 - Provision CA-CONFIG Defaults in Call Agent and Feature Servers
 - Configuring Slot/Sub-Slot/Port for ISDN D-Channel Backhaul
 - Increase Table Size for Region Profile Table
 - Provisioned Subscriber DN and Privacy
 - No Automatic Alarm-status=Off After System Recovery
 - Billing Information for CF Interrogation
 - ACR and 200-OK Message
 - Show Faulty Trunks
 - Speed Call 1 Digit
 - SIM Memory Audit
 - SIP Dynamic Memory Audit
 - SIP Transport
 - INVITE Retries Are Configurable
 - SIP Session Timers
 - SIP Retry
 - Bypass Flag for Time Difference
 - Nodestat Obtains and Shows Status Information from Hub
 - SIP Stack Message Size
 - SIP Trunk Hop Counter
 - Cisco BTS 10200 Sends SDP for SIP Call When rbk=N for Call Waiting
 - SIA Diversion Header
 - SIA Restart
 - SIP Outbound Numbers Require +CC Depending on NOA

- SIP Stack
- DOMAIN-NAME Verified on SIP INVITE Messages
- Time-Out (TO) to Ring Signal for MGCP/NCS
- POP OFFICE SERVICE ID
- SIP Stack Attempts Next Address If TCP Connection Fails for INVITE
- A-Law to U-Law Transcoding Interworking
- SIA Authentication
- SIP NOTIFY Rejected from Unity
- SIM Feature Server Status Saved in Feature Server Table
- Change Counter Names to SIS and SIP for Release 4.5 Measurements
- Change in RACF Service Logic
- Heap Memory Monitor
- VMWI and SDT on Per Line Basis
- Piggybacked MGCP Messages Now Configurable Using MGW-PROFILE
- New Field OSS-SIG-TYPE
- Configurable Field for Sending FastStart in CALL PROCEEDING or ALERTING
- Updated EventObject and Version ID Field
- Updated H.323 Stack
- Ringback on CAS Trunking Gateway
- Measured Rate Flag
- Account Code in Event Message Billing
- New, Modified, or Deprecated Alarms
- Other Features
 - Changes from Previous Releases
 - Vertical Service Code Limitation
 - Measurement Changes

Telephony Features

The following telephony features were added to Cisco BTS 10200 Release 4.5.

MLHCentrexGroupName Data for Billing Call Detail Records

The MLHCentrexGroupName data was added to the Billing call detail record (CDR) for Centrex calls using multiline hunt groups (MLHGs). The data is obtained from subscriber information and divided into mlhg-id and centrex-id fields in the CDR. The Cisco BTS 10200 Softswitch uses field 40 to store the mlhg-id, and field 173 to store the centrex-id. [Table 6](#) describes fields 40 and 173.

Table 6 MLHCentrexGroupName CDR Fields

Field Number	Common Name	Field Type	Field Size*	Potential Values	Data Source	Field Description
40	Multiline hunt group	String	16	Up to a 16 character group name	Subscriber::MlhgId	The multi-line hunt group that this call is associated with. If this field is null, then no data was captured for this record.
173	Centrex Group	String	16	Up to a 16 character group name.	Subscriber:CtngId	The Centrex group that this call is associated with. If this field is null, then no data was captured for this record.

Temporarily Disconnected Subscriber Status and Soft Dial Tone

Release 4.5 allows for marking a subscriber as temporarily disconnected (TD). For example, subscribers with delinquent accounts can be blocked from making any outbound calls other than to an emergency number like 911 by marking them in a TD state. The feature is configurable at the POP level to define a line restriction or suspension profile. Calls disconnected due to a TD hear an appropriate generic announcement.

There are two options for suspended lines:

- Option 1: Service denial; restricts all calls, including emergency calls. With this, MGCP subscribers have no dial tone.

Additionally, no outgoing or incoming calls are allowed for Service Denial, including emergency/911 calls.

The service denial condition is configurable in POP table TDISC-SERVICE-ALLOW token.

When a subscriber has a status = temp_disconnected and the associated POP_ID has temp_disc_service_allowed=N, the Cisco BTS 10200 provides a reorder/fast busy tone immediately upon receiving an off-hook indication. No emergency service is available for a subscriber in that state.

- Option 2: Allow calls to emergency services and specific directory number (DN)s (such as 8xx, 611 or other numbers configured by the service provider)

Cisco BTS 10200 uses a mechanism to block all originating calls except for predefined numbers and call-types. The predefined numbers are based on partial prefix DNs.

The predefined numbers are captured in a COS-restrict table associated with the POP table. If no COS-restrict ID is provisioned against the subscriber’s POP area, the call is blocked.

The Trigger NOD Escape List Table is used to “not trigger” based on the Nature of Dial (or Call Type). For example, if a subscriber is temporarily disconnected or has a COS feature assigned, but dials a 911 (emergency) call, the table can be set up to NOT trigger for 911 calls. When a subscriber dials 911, the call type emergency is converted to NOD emergency.

When COS is triggered, the Cisco BTS 10200 checks the NOD ESCAPE TRIGGER LIST table to see if the dialed NOD (Emergency) is defined for Trigger (COS). If it is, Cisco BTS 10200 ignores the COS Trigger, and continues the call as if the COS Trigger was not assigned to the subscriber.

COS-restrict fields affected:

- TEMP-DISC-COS-RESTRICT-ID: The default value is NULL.
- TEMP-DISC-SERVICE-ALLOWED: The default value is N.

Restrictions:

- If POP.TDISC_SERVICE_ALLOW="Y" and POP.TDISC_COS_RESTRICT_ID=<NULL>, calls are blocked for a TD subscriber.
- For the POP table, TDISC_COS-RESTRICT-ID is a mandatory field if POP.TDISC_SERVICE_ALLOW is set to Y.
- For a TDISC call scenario where the originating subscriber is not in TDISC but the terminating line is an ISDN endpoint on TDISC, then the routing used to reach that subscriber's DN1 must be subscriber routing.
- Trunk-grp routing for TDISC is not supported.



Note

PacketCable Line Service Restriction is the same as it is with the Cisco BTS 10200 COS implementation.

Block Toll Free Calls per Subscriber

In previous releases, the class of service (COS) feature implemented in the POTS feature server could screen calls per subscriber based on call type information. However, the feature did not work for toll free calls even though the call type TOLL_FREE was available for COS provisioning.

In Release 4.5, the COS feature implementation was extended to include toll free calls. The main change is in the SSF library to allow the cos-trigger for toll free calls sent to POTS feature server. The POTS feature server was modified to process calls based on call type TOLL_FREE.

An example of provisioning for the MGCP user:

```
CLI> add service id=8; fname1=COS
CLI> add subscriber-service-profile sub-id=komodo9_1; service-id=8
CLI> add cos-restrict id=test1; NOD_WB_LIST=BLACK
CLI> add nod-wb-list COS_RESTRICT_ID=test1; NOD=TOLL_FREE
CLI> change subscriber id=komodo9_1; COS_RESTRICT_ID=test1
```

Star Code to Access Voice Mail

Subscribers can now activate and deactivate the voice mail sub-features by using star codes; however, this is not required.



Note

This feature is implemented by VM_ACCESS only.

The new star code (*xx) provides end users with a shortcut to voice mail. The code translates to the voice mail pilot number (the 10-digit number reached via the SIP trunk), and routes the call to voice mail.

To use the star code, service providers provision a 2-3 digit string (0-9, *, #) as a valid dial string to access voice mail.

The 10-digit voice mail number is configurable on either a per office, per POP, per subscriber-profile or per subscriber basis, and the Cisco BTS 10200 supports multiple voice mail systems.

An example of defining the star codes in the VSC table for Centrex subscribers:

```
add/change cdp; id=[cdp-id]; fname=VM_ACCESS; DIGIT_STRING=*222; nod=VSC;
CAT_STRING=111111111111111111;
```

After the star code is configured, the Voice Mail ID is assigned at the subscriber, subscriber-profile or the POP level.

Single Vertical Service Code to Activate or Deactivate Call Forwarding No Answer and Call Forwarding on Busy

Cisco BTS 10200 Release 4.5 uses a single vertical service code (VSC) to activate or deactivate the Call Forwarding Combination (CFC). Once activated, the CFC feature forwards incoming calls when the subscriber is either busy or does not answer. For example, the code *68 activates both CFC while the code *88 deactivates CFC.

The CFC allows subscribers to forward incoming calls to a certain directory number (DN) when the end user is busy or does not answer. It includes the following options:

- **CFC Activation:** Activate CFC to a pre-defined DN.
 - The end user cannot change the DN via this feature.
- **CFC Deactivation:** Deactivate the CFC feature.
- **CFC Activation with DN change:** Activate CFC to a user-defined DN.
 - The end user can change the DN via this feature.
- **CFC Interrogation with No DN Verification:** Verify whether CFC is active or not.
- **CFC Interrogation:** Verify whether CFC is active to a certain DN or not.
- **CFC Invocation:** Assigned and activated, this feature forwards incoming calls when the end user is busy, or does not answer.

The feature interactions include the following:

- **CFC Activation/Deactivation and Speed Call/Abbreviated Dial:** Subscribers can set their speed call to the CFC Activation/Deactivation access codes. For example, with One-Digit Speed Call, the subscriber can set the speed call for digit “2” to map to “*68” which can be the CFC Activation access code.
- **CFC Activation and OCB:** CFC Activation to a DN blocked by outgoing call barring (OCB) results in a re-order tone or announcement.
- **CFC Activation with DN Change and OCB:** CFC Activation with DN Change to a DN blocked by OCB results in a re-order tone or announcement.
- **CFC and OCB:** Calls are not forwarded by CFC to DNs blocked by OCB for the subscriber.
- **CFC and CFU:** If a subscriber has both CFC and call forwarding unconditional (CFU) assigned and active, incoming calls are forwarded by CFU.
- **CFC and CFB:** If a subscriber has both CFC and CFB assigned and active, incoming calls on which the subscriber is busy are forwarded by CFB.
- **CFC and CFB, CFB is deactivated:** If a subscriber has both CFC and CFB assigned, and CFC active and CFB inactive, incoming calls on which the subscriber is busy are forwarded by CFC.
- **CFC and CFNA:** If a subscriber has both CFC and CFNA assigned and active, incoming calls on which the subscriber does not answer are forwarded by CFNA.

- **CFC and CFNA, CFNA is deactivated:** If a subscriber has both CFC and CFNA assigned, and CFC active and CFNA inactive, incoming calls on which the subscriber does not answer are forwarded by CFC.
- **CFC and VM:** If a subscriber has both CFC and voice mail (VM) assigned and active, and the subscriber is either busy or does not answer, the call is forwarded by CFC.
- **CFC and VM, CFC deactivated:** If a subscriber has both CFC and VM assigned but CFC is deactivated and VM is active, and the subscriber is either busy or does not answer, the call is terminated to VM.
- **CFC and VMA:** If a subscriber has both CFC and voice mail (always) (VMA) assigned and active, the call is terminated to VM.

**Note**

Voice mail enables the subscriber to forward calls to voice mail when the subscriber is busy or does not answer the phone. Voice mail (always) enables the subscriber to forward all calls to voice mail, irrespective of the state of the phone.

The VSC code can be checked by doing a “show vsc; fname=<feature name>” at the CLI prompt.

Stand-Alone Call Redirection to Voice Mail

Cisco BTS 10200 can assign stand-alone call redirection to voice mail (CR-to-Vmail) to subscribers as a separate feature. It is implemented by the following features:

- VM
- VM_ACT
- VM_DEACT
- VMA
- VMA_ACT
- VMA_DEACT

With this feature, subscribers can forward calls to voice mail if they are busy or do not answer their phones. Using the star code, subscribers can:

- Activate voice mail
- Deactivate voice mail

**Note**

Subscribers cannot make voice mail changes through the handset. Only the operator can change the voice mail DN.

The voice mail sub-features allow subscribers to:

- Forward calls to voice mail when subscribers are busy, or when subscribers do not answer the phone. This is referred to as voice mail.
- Forward all calls to voice mail irrespective of the subscriber’s phone status. This is referred to as voice mail (always).
- Use a VSC (provisionable) to access voice mail to retrieve the message.

The voice mail features are applicable for INDIVIDUAL, CENTREX, and MLHG subscribers.


Note

When assigned, voice mail is considered activated unless explicitly deactivated by either the subscriber or the operator.

If the subscriber does not have any forwarding features active (such as CFU, CFB, or CFNA), the incoming call is forwarded to voice mail. However, if the subscriber has other forwarding features active, calls are forwarded according to those features.

For example, CFNA and CFB take precedence over stand-alone CR-to-Vmail. CFNA and CFB forwarded-to-numbers do not have to be a voice mail number; if activated, CFNA and CFB are invoked before CR-to-VMail. This means that Cisco BTS 10200 can invoke the CR-to-VMail only when the other Call Forwarding(s) are inactive or do not occur.

When CFNA occurs on a busy number, the call continues to CR-to-Vmail. If CR-to-Vmail is active, the call is redirected to voice mail.

Cisco BTS 10200 also allows subscribers to activate or deactivate the CR-to-Vmail Always option so that all incoming calls go to voice mail, providing the subscriber has no call forwarding features activated.

An example of defining the star codes in the CDP table for Centrex subscribers:

```
add/change cdp; id=[cdp-id]; fname=VM_ACT; DIGIT_STRING=*210; nod=VSC;
CAT_STRING=1111111111111111;
```

```
add/change cdp; id=[cdp-id]; fname=VM_DEACT; DIGIT_STRING=*211; nod=VSC;
CAT_STRING=1111111111111111;
```

Inter-LATA Option

Prefix screening tokens provisioned in the Subscriber Profile table determine whether a subscriber must dial 1 when dialing local or long distance calls. LOCAL_PFX_OPT controls calls with call type set to LOCAL, and until Release 4.5, the TOLL_PFX1_OPT controlled both inter-LATA and toll calls. Values for these tokens are required (RQ), not required (NR), and optional (OPT).

Beginning with Cisco BTS 10200 Softswitch software Release 4.5, a new token, INTERLATA_PFX1_OPT was added. Now the functionality is split. The 500, 800, and 900 calls are controlled by TOLL_PFX1_OPT. The 700 call is controlled by INTERLATA_PFX1_OPT.

However, for Service Access Code calls such as 500, 700, 800, and 900, you must dial the 1. The LOCAL_PFX1_OPT, INTERLATA_PFX1_OPT, and TOLL_PFX1_OPT flags do not affect such calls.

The following example turns on the inter_LATA option and intra_LATA option:

```
change subscriber-profile ID=sp1; DIAL_PLAN_ID=cdp1; LOCAL_PFX1_OPT=NR;
TOLL_PFX1_OPT=RQ;
INTERLATA_PFX1_OPT=RQ; POP_ID=69;
```

Privacy Director or Calling Identity with Enhanced Screening

The privacy director/screening enables subscribers to screen all anonymous calls by prompting anonymous callers to record a short message (their identity), or enter a pass-code. If the caller records a message, the message is played back to the subscriber. The subscriber chooses how to handle the call, or how to have the message delivered.



Note

The feature works only with the IP Unity's Privacy Screening Application Server.

If using Privacy Screening with IP Unity servers, please refer to the following defects:

- * CSCsa85923
- * CSCsb76491
- * CSCsb76468
- * CSCsb41635
- * CSCsb55765
- * CSCsb63061

After listening to the message, the subscriber chooses an option to handle the call:

- Accept the call based on the caller entering the correct passcode.
- Accept the call based on the caller's recorded message.
- Reject the incoming call based on the caller's recorded message.
- Send the call to voice mail, if subscribed.

An example of how the privacy director works.

1. An anonymous caller calls the subscriber. The subscriber has Privacy Screening (PS) assigned and activated.
2. PS intercepts the call. The caller hears an announcement asking for a pass-code, or for the caller to wait and record a short message for the subscriber.
3. If the caller enters the correct pass-code, the subscriber receives the call, and the connection is treated as a regular call. If the caller enters an incorrect pass-code, the caller is prompted again for the pass-code.
4. If the caller waits, an announcement is played asking the caller to record a short message.
5. The caller records the message, and hears on-hold music. A call is placed to the subscriber, and the recorded message is played.
6. The subscriber then chooses to accept or reject the call, or send the caller to voice-mail. The system acts according to the subscriber's choice.

The Privacy Screening feature has two sub-features:

- The PS invocation sub-feature, PS feature. This sub-feature:
 - Plays the announcement to anonymous callers.
 - Records the name/message. If the callers have a pass-code, they can use it to override the recording.
 - Delivers the name/message to the subscriber.
 - Connects or disconnects the call depending on the subscriber's choice.
- The PS manage sub-feature, PS_MANAGE. This feature:

- Manages a subscriber's pass-code.
- Activates or deactivates the PS feature.

No Solicitation Announcement

The No Solicitation Announcement (NSA) feature works in conjunction with the Privacy Director feature.

If the subscriber receives an anonymous call and has the PS assigned, NSA features assigned and active, the call is routed to PS. For non-anonymous callers, the call is routed to the NSA feature. NSA allows subscribers to play a message telling callers that the subscriber line does not accept solicitation, and that the caller can press "1" or wait on the line to connect to the subscriber.

Subscribers manage the "no-solicitation" list to contain:

- Full or partial directory numbers (DNs)
- User pass-code (required to access the menu)
- Managing the time-of-day when subscriber wants this service active
- Option to completely turn off NSA

The no-solicitation list can contain full numbers, partial DN's, or extension numbers (if the subscriber is in a CENTREX group).

Subscribers can program up to 25 DN's to bypass the announcement. Either the service provider or the subscriber can provision the service hours when the NSA feature is active, and solicitors hear the message. During non-service hours, there is no announcement, and calls go directly to the subscriber line.

The user PIN (pass code) is optional. The service provider can enable and disable it for the NSA feature. Subscribers are allowed to choose the PIN when the feature is initially assigned to the subscriber. Afterwards, the subscriber must contact the service provider to change the PIN.

Cisco BTS 10200 provides office-wide or subscriber-basis configurations on the NSA time-period; the subscriber basis configuration takes precedence.

Additionally, managing the time-of-day is optional. Subscribers are allowed to always turn on the feature, always turn off the feature, or turn on the feature based on the time-of-day schedule.

Detailed information on this feature is available in the [Cisco BTS 10200 Softswitch Release 4.5 Network and Subscriber Feature Descriptions](#).

Trace Active Call per Directory Number and Trunk Identification

Cisco BTS 10200 allows subscribers to trace an active call based on a directory number (DN) or trunk ID through a CLI command.

The feature identifies a specific in-progress call based on an input parameter, and outputs the call information for viewing. It applies to originating and terminating calls.

The input parameter can be any subscriber-specific information including:

- DN
- Gateway FQDN
- MLHG ID/terminal
- Centrex/ext
- Termination

The input also can be any trunk-specific information, including:

- SIP call ID
- H.323 call ID
- SS7, ISDN or CAS using a combination of trunk group and trunk ID

The call processing information displayed includes the:

- Originating number
- Terminating number
- Media gateway(s) and SDP IP addresses involved
- Trunk group number and CIC as applicable

For a call in progress, the CMS provides the far end information (DN and trunk ID, if applicable) when it knows the local information (DN or trunk ID).



Note

This feature is also known as “far-end identification.”

If you trace the active call from the trunk, you must provide the CIC number, such as in this example:

```
query call-trace; tgn-id=1; trunk-id=23; mode=verbose.
```

However, there is a different command for tracing the number from the subscriber’s DN, such as in this example:

```
query call-trace; dn=35649901; mode=verbose
```

The Active Call Display feature only displays the existing calls (if any) based on the subscriber’s input (DN, trunk ID, FQDN gateway). It also displays the forwarding numbers if this call contains call forwarding.

CLI (Input) Syntax

The CLI input syntax for the feature is `QUERY CALL-TRACE MODE=<VERBOSE | BRIEF>` followed by one of the following options.



Note

If `MODE` is not specified, by default, it is `BRIEF`.

- `DN=<dn>`
- `MLHG-ID=<mlhg-id> TERMINAL=<terminal>`
- `CTXG-ID=<ctxg-id> EXT=<ext>`
- `TG-ID=<tg-id> TRUNK-ID=<trunk-id>`
- `SIP-CALL-ID=<sip-call-id>`
- `H323-CALL-ID=<h323-call-id>`
- `TERM=<term-info>`
- `MGW=<mgw-info>`

CLI Examples

The following are examples of the QUERY CALL-TRACE mode. In the examples, the VERBOSE option is not shown.

```

QUERY CALL-TRACE DN=4695551234 (for POTS/H323/SIP subscriber)
QUERY CALL-TRACE MHLG-ID=mlhg1 TERMINAL=23 (for POTS MLHG terminal)
QUERY CALL-TRACE CTXG-ID=ctxg1 EXT=1234 (for POTS centrex subscribers)
QUERY CALL-TRACE TG-ID=123 TRUNK-ID=456 (for SS7, ISDN and CAS trunks)
QUERY CALL-TRACE SIP-CALL-ID=<sip-call-id> (for SIP trunks)
QUERY CALL-TRACE H323-CALL-ID=<h323-call-id> (for H323 trunks)
QUERY CALL-TRACE TERM=aaln/2@labname.company.com (MGW termination with FQDN)

```

T.38 Fax Relay Call Agent Controlled Mode Across SIP Trunk Interface

In previous releases, Cisco BTS 10200 partially supported T.38 fax relay call agent controlled mode in MGCP and H.323 trunk interfaces. Release 4.5 offers support for the PacketCable environment, as well as extending T.38 fax support to SIP, NCS, and TGCP trunk interfaces.

The Cisco BTS 10200 supports ITU-T T.38 procedures on the following trunk interfaces:

- NCS MTA subscribers
- MGCP subscribers
- MGCP (or TGCP) trunking gateways (SS7, ISDN)
- H.323 trunks

T.38 fax is supported for the following H.323 configurations:

- H.323 trunk using fast connect procedure (fast start)
- H.323 trunk using non-fast connect procedure (slow start)
- H.323 trunk using gatekeeper (H.225 RAS messaging)
- H.323 trunk not using gatekeeper (direct trunks)
- H.323 trunk with and without H.245 tunneling enabled
- SIP trunks

Account/Authorization Code Support on PRI Trunks



Note

The feature is not supported for SS7, H.323 or SIP endpoints.

Cisco BTS 10200 previously offered the account/authorization code on the IAD subscriber line; a similar functionality is now available on the trunk. This enables businesses to use the Account/Authorization code essential in controlling user call placement.

The Account/Authorization Code Support on PRI Trunks feature allows for playing an Interactive Voice Response (IVR) prompt and collecting digits on the trunk, by using a network IVR server.

With the IVR-based COS screening feature, service providers can play either a tone or an interactive voice session to collect authorization or account codes. IVR-based COS also prompts subscribers to enter account/authorization codes on the trunk. IVR-based COS is recommended only in cases where the originating media gateway is unable to play tones to the caller.

When an authorization or account code is required during COS screening, an IVR voice path is established between the IVR server and the IAD at the customer site. The voice path collects digits and terminates when the digit collection concludes and the resources are de-allocated. Once the digits are collected, the call proceeds or is blocked based on COS restrictions.

PRI trunk types are supported in this release.

The feature has some limitations. In this release, the limitations are:

- The feature is not supported for SS7, H.323 or SIP endpoints.
- Cisco BTS 10200 does not support local IVR capability; instead, it relies on IVR capabilities provided from an external IVR server supporting the MGCP BAU package.
- For IVR trunk groups, LOCAL-TRUNK-SELECTION is not used for IVR. This flag is only applicable for Release 4.5 and higher.
- The IVR-based COS feature for ISDN trunk is for the North American market only.



Note

For Cisco BTS 10200 Releases 4.4.x and previous, the COS feature did not support account and authorization code for ISDN lines. However, starting with Release 4.5 and going forward, the account and authorization code are supported with the availability of IVR-based account and authorization codes.

- Auth-Code/Acct-Code reported via IVR is not appended to the DialedDigit parameter issued to the Billing record, because the IVR digits are not processed in CA.
- The COS-RESTRICT-ID should be defined with PROMPT-METHOD set to IVR.



Note

PROMPT-METHOD-TONE cannot be specified for COS-RESTRICT assigned to ISDN lines.

The feature interfaces with, and is dependent on, the services of an IVR server.

Detailed information on this feature is available in the [Cisco BTS 10200 Softswitch Release 4.5 System Description](#) and [Cisco BTS 10200 Softswitch Release 4.5 Provisioning Guide](#).

Alerting Notification to Third-Party Feature Server

The Cisco BTS 10200 Softswitch can interface to an FCP-based feature server using SIP messaging. The immediate application is delivery of alerting notification (and the associated call data) to a third-party feature server, introduced in Release 3.5.4.

Release 4.5 supports advertising of an externally addressable FQDN to an external third-party feature server when necessary. Previously, the FQDN advertised in Contact and Via headers in a SIP INVITE message resolved to an internal management network IP address.

The feature works as follows. At the CALL_ACCEPTED trigger detection point (TDP) in the call, the called party (a subscriber on the Cisco BTS 10200 Softswitch) receives ringing or a call-waiting tone. At this same TDP, the Cisco BTS 10200 Softswitch generates a trigger (CALL_ACCEPTED_NOTIFY), and sends a SIP Invite message directed to a third-party feature server. The SIP Invite message includes an FCP attachment containing the call data.



Note

In Release 4.5, certain SIP or H.323 devices may not send an explicit Alerting Indication (180 Ringing for SIP and Alerting for H.323). In these cases, the Call Agent does not report the new trigger (CALL_ACCEPTED_NOTIFY) to the third-party feature server.

In Release 4.5a new feature name “STCID” is added to the Feature Table for this feature. A new token is also added to the Feature Server (feature-server) table. If this token, EXTERNAL-FEATURE-SERVER, is set to yes (Y), the Cisco BTS 10200 Softswitch sends the externally addressable FQDN in the Contact and Via headers. If it is set to no (N), the system sends the internal FQDN.

The value of the externally addressable FQDN is based on information provided in the *Network Site Survey* document (available from your Cisco account team), and is provisioned in the DNS at the time of Cisco BTS 10200 Softswitch software installation. The addresses used against this FQDN are the same logical IP addresses used for SIP applications on the Cisco BTS 10200 Softswitch.

Detailed information on this feature is available in the [Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions](#).

Operational Features

Network Continuity Test and TDM Test Enhancements

In Release 4.5, Cisco BTS 10200 allows for NCS endpoints configured as test-initiated endpoints. Calls initiated from the endpoints are either Network Loop-Back (NLB) or Network Continuity Test (NCT) calls, with the tested-endpoints grouped together as trunk-like endpoints.

For example, in “network loop-back” mode, the audio signals received from the connection are echoed back on the same connection. The “network loop-back” mode simply operates as an RTP packet reflector.

With NLB, subscribers can perform a network loop-back test on any line side NCS/MGCP Residential Gateways (or MTAs) initiated from designated Test endpoints (test trunks) using NCS for call signaling. The feature is applicable to both cable MSOs and non-PacketCable environments.

The feature allows for using a testing device to perform NLB and NCT tests on any MGCP/NCS subscriber endpoints controlled by the Cisco BTS 10200. However, the feature can test the line and trunk sides, but subscribers cannot perform network loop-back tests across a SIP or H.323 network. The feature does allow for IP testing, and has enhanced TDM test capabilities.

Cisco BTS 10200 accommodates two types of test equipment or devices. The first is IP-based (such as acting as an MGCP/NCS-based media gateway interface). The IP test type can be either NLB or NCT. The NLB simply operates as an RTP-packet reflector, and the NCT involves the eMTA DSP capability before looping back the signals.

The second type is a TDM-based testing device (such as an MF CAS TDM trunk interface, which requires that an MGCP-based trunk gateway exists). The TDM test type is the traditional 1xx test type, with an additional enhancement in Release 4.5—the ability to route the test call to a specified DN on a given trunk circuit.

This feature with the testing and tested devices are assumed to be configured on same Call Agent.

Alarm Correlation Enhancements

Release 4.5 introduces correlation enhancements for Alarm 36, Alarm 68, and the Signaling 79 alarm. Release 4.5 also introduces two new alarms, Signaling 151 and Signaling 152.

Alarm 36 is for administratively blocked terminations or trunks. Controlling a termination out of service (OOS) generates the alarm. The change in Release 4.5 is that the alarm now shows individual numbers for the terminations, rather than just a range. For example, if five trunks were terminated, you would see the individual numbers 6, 7, 8, 9, and 10, rather than a range of 6-10.

Alarm 68 addresses terminations or gateways that are OOS. The change in Release 4.5 is that there is now a hierarchy; if the termination is OOS, you receive an alarm 68 for that termination. If one gateway goes OOS, then the other gateway is turned off. Every termination housed within that gateway also becomes OOS. The hierarchy is set to On.

Alarm correlation is important in understanding true faults in the Cisco BTS 10200 and their impacts to the system. The application programs do not directly generate alarms; rather, a report is issued as an event that directly maps to an alarm. An event also may map to higher layer alarms or implied actions that generate alarms.

With the Event Management and Alarm Correlation feature, there is a relational effect when different types of errors occur in a system. The feature tracks and verifies those states within the Cisco BTS 10200 Element Manager, Bulk Data Manager, Call Agent and Feature Servers.

In Release 4.5, the Event and Alarm subsystem functionality was enhanced, and the existing event and alarm capabilities modified.

All components in the Cisco BTS 10200 have a two-stage component definition referred to as the “Component ID” including the following items.

- Component type—The defined value providing the entity class, and providing the logical reference of where that resides within the Cisco BTS 10200.
- Component label—The textual reference to the entity instance, providing a reference of the entity within the scope of a single Cisco BTS 10200 instance.

All Cisco BTS 10200 entities have a component hierarchy which defines the “path” to internal or external entities in the whole system. These are two main segments into which components fit in the architecture of the Cisco BTS 10200:

- Internal components—An internal component is a distinct and integral part of the Cisco BTS 10200. This includes Solaris nodes, NICs, and application software instances.
- External components—An external component is an associated part of the Cisco BTS 10200. It has a logical representation on the Cisco BTS 10200 as an interface or database entry. Examples include media gateways and terminations.

Changes were made in Release 4.5 to alarm 68 and alarm 36.

- Cisco BTS 10200 clears the “Signaling 68” alarm when a media gateway is restored to service. The Signaling 68 alarm now reports:
 - A “Down” state for a Media Gateway
 - A “Down” state for an endpoint on a Media Gateway
- Similarly, Cisco BTS 10200 clears the “Signaling 36” alarm.

Other Alarm 68 rules include:

- When an alarm(68) is issued for a gateway (alarm ON), all alarm(68)s are turned OFF for the endpoints.
- When an alarm(68) is canceled for a gateway (alarm OFF), all alarm(68)s are turned OFF for the endpoints.

Events generated in the SIGNALLING category occur on devices such as the media gateway or MTA terminations, as well as trunks and trunk groups. An outage on a single trunking gateway can generate hundreds of valid alarms.

Alarm correlation breaks these down into fewer, more meaningful alarms. However, the alarms generated must match with a clear and specific “off” condition for the alarm to be cleared:

- The SIGNALLING event must contain the new component ID, based on the component definitions above.

- The SIGNALLING event must use a consistent value for the reported entity. This is the database ID value for the entity name.

Release 4.5 also modifies the Signaling 79 alarm. In this release, Signaling 79 is generated when a media gateway becomes unreachable. The alarm clears when the endpoint or gateway becomes reachable.

The new alarm Signaling 151 is generated when an endpoint returns a permanent error code, and an endpoint is placed in FAULTY state. The alarm clears when the endpoint is manually or automatically recovered.

Another alarm new to the release is the Signaling 152 event. Signaling 152 conveys transient protocol errors only. It is an info level event.

For a list of new or changed alarms, refer to the [“New, Modified, or Deprecated Alarms”](#) section on [page 67](#). Detailed information on these alarms will also be available in the *Cisco BTS 10200 Softswitch Release 4.5 Operations and Maintenance Guide*.

CDB File Naming Convention

The Cisco BTS 10200 system stores raw call detail blocks (CDBs) in a flat file, ASCII-based format, on the persistent store associated with the Bulk Data Management System (BDMS) for retention purposes. The Cisco BTS 10200 stores a minimum of 10 megabytes of billing records in a circular file implementation. This data is subsequently sent to the specified remote accounting office, billing server or mediation device via the File Transfer Protocol (FTP) or optional Secure File Transfer Protocol (SFTP).

Cisco BTS 10200 provides a configurable option for how CDB file names are constructed. The file-name format is either the current native format or a new format based on the alternate CDB file naming feature. This is based on the PacketCable EM file naming convention which includes ECN #EM-N-04.0186-3.

The Native format (Default) CDB File-Naming format is outlined as follows.

By default, the Cisco BTS 10200 names CDB files according to this format:

```
<prefix>-<CA ID>-yyyymmdd-hhmmss<counter>-<state>
tb06-CA146-20050112-1134120-S
```

where:

- <prefix> is the billing file prefix from billing-acct-addr
- <CA ID> is the Call Agent ID where the records were generated, e.g. CA146
- yyyymmdd-hhmmss is the time the file was created
- <counter> is a number from 0 to 9
- <state> is a letter indicating the state of the file
 - P = primary (i.e., complete but untransferred)
 - S = secondary (i.e., complete and transferred)
 - O = open (i.e., currently collecting CDB records, incomplete, and untransferred)

The Cisco BTS 10200 can optionally use the ALT CDB File-Naming format, which is based on the Alternate CDB FILE Naming feature. That is based on the PacketCable EM file naming convention, which includes ECN #EM-N-04.0186-3.

The Cisco BTS 10200 uses the following format [R-0431] if -CdbFileName PacketCable is specified in platform.cfg:

```
<prefix>_yyyymmddhhmmss_3_<record type>_<CMS ID>_<sequence num>.ascii[.tmp]
tb06_20050112121948_3_0_55555_000002.ascii.tmp
```

- <prefix> is the billing file prefix from CLI> billing-acct-addr
- yyyymmddhhmmss is the file creation date/time stamp
- 3 is the priority of file. It does not change and is hardcoded to 3
- <record type> = 0 untransferred, 1 transferred
- <CMS ID> is the CMS ID provisioned from CLI>call-agent-profile
- <sequence num> is the 6-digit number from 000001 to 999999
- <.ascii> is the file format. It does not change, and is hard-coded to .ascii
- [.tmp] is the temporary extension used by the Cisco BTS 10200 to indicate that the file is the current/open file. The .tmp extension is stripped off before the file is sent to the BMS

Support of SUN 1280 (8 CPUs)

Starting with Release 4.5, Cisco BTS 10200 now supports the SUN 1280 (8 CPUs) as the processor engine for both the Cisco BTS 10200's Call Agent and EMS.

For information about the SUN 1280, refer to Table 1, the [Host Hardware Requirements](#).

Measurement Report on a Per Market (POP) Basis

Cisco BTS 10200 provides a trunk group usage measurement report on a per market (POP) basis.

The Centum Call Second (CCS) reporting fields are generated on a per market or POP basis.

Customer traffic engineers pull reports for hourly usage data from other Class 5 switches, including the following fields.



Note

Bold face fields are new to Release 4.5.

- Exchange Name: CLLI code for POP (i.e., RONLVA31GT0)
- **Trunk Group ID**: tgn-id (i.e., 1001)
- Trunk Group Name: <Remote Switch CLLI>_<Type> (i.e., RONKVACSDS0_LC)
- **Total Usage (CCS)**: Incoming and outgoing usage CCS (TRKGRP_INCOM_BUSY_TRK, TRKGRP_OUTG_BUSY_TRK)
- Maintenance Usage (CSS)
- **Total Attempts**: TRKGRP_INCOM_ATTMP + TRKGRP_OUTG_ATTMP
- Outgoing Attempts: TRKGRP_OUTG_ATTMP
- Incoming Attempts: TRKGRP_INCOM_ATTMP
- Overflow Attempts: TRKGRP_TOTAL_OVERFLOW
- **Glare Count**: Count of attempts to use the same CIC on a two-way trunk group
- **Circuits in Service**: Count of Trunks (DS0) with a status of INS

Cisco BTS 10200 also adds the following CCS-based counter fields to the measurement-tg-usage-summary report:

- TRKGRP_EXCHANGE: An 11-character field from the POP or TRUNK-GRP table that describes the CLLI code for the site (i.e., RONLVA31GT0).

- **TRKGRP_NAME:** A 20-character field from the TRUNK-GRP table that describes the remote switch CLI code and trunk group type (i.e., RONKVACSDS0_LC)
- **TRKGRP_MAINT_TRK:** A field that contains a CSS value for trunks that are MAINT, OOS, UEQP, local block or remote block for the reporting period.
- **TRKGRP_GLARE_COUNT:** Count of attempts by the local and remote switches to use same CIC on a two-way trunk group. Outgoing attempts should not be incremented on a glare.
- **TRKGRP_TOTAL_INS_TRK:** Count of trunks with a status of INS for the reporting period.

The CLI table and POP table where the CLI goes must have 11 characters. To getting the information for these measurements, complete the following steps:

1. Add the CLI_CODE to the CLI table.
2. Add the CLI Code to the POP table.
3. Add the CLI code to the trunk group table.
4. Add the trunk group name to the trunk group table.

An example of the new reporting option to gather statistics on a per POP basis:

```
add CLI_CODE; id=RONLVA31GT1
change pop; id=1; cli_code_id=RONLVA31GT1
change trunk-grp id=6001; TG=RONKVACSDS0_LC (tg 6001 is part of pop=1)
change trunk-grp; id=6001; CLI=RONLVA31GT1
```

```
CLI>report measurement-tg-usage-summary; tgn-id=6001; start-time=2005-02-23
16:30:00; end-time=2005-02-23
16:50:00; TRKGRP_EXCHANGE=RONLVA31GT1; trkgrp-name=RONKVACSDS0_LC; call-agent-id=CA146; output
=tg-report; output-type=csv;
```

```
Reply :Success:Look in the report directory for Tm_tg-report.csv
CLI>
```

Or to view in CLI by exchange:

```
report measurement-tg-usage-summary; TRKGRP_EXCHANGE=RONLVA31GT1;
```

30 Originating Point Codes

With Release 4.5, the Cisco BTS 10200 system now supports up to 30 originating point codes (OPCs) when the Sigtran Signaling Gateway supports SCCP User Adaptor (SUA) in a D-link configuration. The 30 OPC support is for medium- and large-sized configurations; small configurations support only 8 OPCs.

The 30 OPCs are supported for all subsystem numbers (SSNs). The subsystems are features or services such as toll-free, LNP CNAM or AC/AR, and each service has an associated subsystem number. The change applies only to configuring the Transaction Capabilities Application Part (TCAP) SS7 communications which include SUA. ISUP supports 30 OPCs without any additional changes.

Support includes:

- Single PC shared by multiple Cisco BTS 10200s for ISUP messages.
- Each Cisco BTS 10200 with unique PC for TCAP messages.

In addition to supporting multiple OPCs in a D-link configuration, multiple Cisco BTS 10200s can share the same ISUP PC. However, each Cisco BTS 10200 has its own TCAP PC; hence, the support of multiple OPCs at each Cisco BTS 10200.

Encrypted IPSEC Keys

In Release 4.5, IPSEC keys are stored in an encrypted format. Previously, the keys were not encrypted; however, for security reasons, this was changed in Release 4.5. Now only privileged users can see the keys in decrypted form.

This feature is not provisionable, and the change is transparent to the end user.

The IKE-KEY was enhanced for Release 4.5. In this release, the system encrypts the value of the IKE-KEY token and stores the encrypted value as IKE-KEY-ENCR.

IKE-KEY-ENCR is the IKE preshared key in encrypted form (system generated). The system encrypts the value of the IKE-KEY token and stores the encrypted value as IKE-KEY-ENCR. It is then decrypted and displayed only when accessed by a privileged user.

To show the IKE-KEY-ENCR token in encrypted form, use a command in the form of:

```
show radius-profile;
```

To show the IKE-KEY token in unencrypted form, use a command in the form of:

```
show radius-profile-unencr;
```

Detailed information on this feature is available in the “PacketCable Media Security” chapter of the *Cisco BTS 10200 Softswitch Release 4.5 Command Line Interface Reference Guide*.

.DONE Indicator After Successful Transmission of Call DB Records to Billing Mediation Server

Release 4.5 includes a configurable option to transmit a final CDB file with a .done extension, indicating the CDB file transfer is complete.

After a file of usage records (such as CDR, AMA, or EM) is successfully transmitted, a second file with the same name but a .done extension is immediately sent.

The extension assures the mediation system that the entire data file was received, with no losses due to a network failure, FTP failure or delay. It provides reliability for billing and revenue protection.

Enhanced Software Upgrade

Cisco BTS 10200 Release 4.5 provides an enhanced upgrade procedure that is more automatic, reducing the number of steps significantly. However, the benefits take place starting with Release 4.5 going forward for patches to that release. These benefits include a reduction in manual steps to perform, and significantly less time to upgrade, audit, and fall back.



Note

Customers upgrading from previous releases (such as Release 3.5.4, for example) will not benefit initially from the automated upgrade process. They must first upgrade to Release 4.5; after migrating to Release 4.5 and setting up a stable infrastructure, they will benefit from the automated upgrade process going forward.

The goals for the enhanced software upgrade are to:

- Reduce time to perform upgrade during maintenance window.
- Automate steps that were previously manual steps, reducing the possibility of mistakes.
- Continue support for in-service upgrades with minimal loss of service.
- Provide for patch installation, as well as for a full release upgrade.

- Reduce time to perform upgrade to meet Service Level Agreements (SLAs).

Some of the key enhancements to the software upgrade include:

- Pre-install health check
 - Checks for proper health of the system prior to starting the upgrade procedure.
 - Users can specify the necessary upgrade inputs via a configuration file prior to upgrade.
 - Upgrade utility checks for package contents and reports to user all the components that are modified.
- Checkpoints
 - Checkpoints are recorded during upgrade process.
 - In case of an upgrade step failure, the upgrade can resume from the last successful checkpoint.
- Fallback
 - All components that changed during upgrade process are archived.
 - Archived files are used during fallback to return the system to the pre-upgrade state.
- Centralized upgrade logging
 - All installation and upgrade activities are logged to in a dedicated log file.
 - Central application reports currently installed Cisco BTS 10200 package versions.
- Migration paths
 - Pre-documented and well-published upgrade migration paths are supported.
 - V-load upgrades are supported on a given release from any Vxx load to any Vyy load (where yy > xx), and a V-load upgrade is installed as an incremental patch upgrade.
 - Major release upgrades are supported from the last maintenance release of the last two major releases, including database conversion.
 - Maintenance release upgrades are supported for all maintenance releases of the current major release, but no database conversions.
- Documentation
 - All installation and upgrade documentation is complete in and of itself.
 - Installation and upgrade errors are mapped by unique error codes for clarity.
 - After the incremental patch upgrade is completed, a report is generated listing the newly installed components on the system.

Secure Provisioning for SIP Endpoints

Enhanced SIP Registration was added to Release 4.5 to ensure that a SIP REGISTER message to the Cisco BTS 10200 is from a provisioned endpoint. The feature also ensures that the source IP address and contact parameter for all originating calls are from the provisioned SIP endpoint, and that no calls can originate from an unregistered endpoint.

In previous releases, SIP endpoint registration was based on Address of Record (AOR), UserID and Password; there was no verification of the origination of the REGISTER message. The DSL market requires that the source IP address of SIP requests be verified against a provisioned Fully-Qualified Domain Name (FQDN) of the endpoint to address the possibility of theft of VoIP service.

Secure provisioning implies that only the user subscribed to the service can download the ATA configuration file, and that the user can only register with Cisco BTS 10200 to make and receive calls if connecting from the provisioned circuit.

To provision the subscriber on the Cisco BTS 10200, the relevant subscriber and service information must be configured on the Cisco BTS 10200.

The Cisco BTS 10200 can indicate that Secure-FQDN provisioning for a specified SIP term-type subscriber. When set, a Fully Qualified Domain Name (FQDN) is needed and must be associated with the Subscriber Address of Record (AOR). The FQDN is the address/location of the SIP endpoint and is added to the AOR table. The FQDN will not have a service port.

To enable or disable Secure-FQDN on a successfully registered subscriber:

1. Take AOR Out-Of-Service to remove all registered contact.
2. Enable or disable secure-fqdn for the subscriber.
3. Bring AOR back In-Service.
4. Reboot the ATA.

A secure provision subscriber has the following characteristics:

- One and only one AOR is associated to the endpoint.
- Does not have any static-contact associated with it.
- UserId and Password Authentication are supported.
- One FQDN.
- No service port allowed.
- The DNS lookup of the FQDN should result in one and only one IP address.

Testing Capability Required for 911 FGD-OS Trunks

When you are turning up 911 FGD-OS trunks (based on MO MGCP package), the ILECs require the exchange of Off-hook/On-hook signaling and the passing of tone back and forth without a complete call setup.

In order to support this functionality, the gateway itself must be able to provide the test capability to send and monitor the reception of the signaling and passing tone without a call setup involvement.

Once this gateway test capability on 911 trunk is in place, it needs to be determined whether it can be invoked remotely across the MGCP interface where Cisco BTS 10200 is involved. Upon receiving a CLI command or Test Access request, Cisco BTS 10200 sends the request to the gateway via MGCP signaling to trigger the test capability on 911 trunk at the gateway (not part of a call setup sequence). Cisco BTS 10200 reports the result to the operator upon receiving the notification from the gateway (e.g., receive off-hook, on-hook).

Support for 2048 Bytes in Digit Map

In previous releases, Cisco BTS 10200 only supported 1023 Bytes of digit map on all of the telephony interfaces. In Release 4.5, support was increased to 2048 Bytes.

Better Management of Alarms

Release 4.5 introduces better alarm management. The basic event report includes an expanded “REPORTED” identity information. The report is also supported for both the “C” and Java language interfaces, and for shell tools. The shell interface provides more flexibility in management of third party interfaces such as Solaris and Oracle.

The functionality extension of the Event and Alarm subsystem may result in some behavioral changes experienced externally. Events had been generically throttled and thresholded with no regard to the instance information of the entity being reported. As a result, alarms were occasionally left “ON” when in fact the condition had cleared, and there was no correlation of the reports problems and their resolution.

Additionally, other changes were made to improve alarm management. These changes include:

- Release 4.5 defines and deploys a new hierarchical component ID structure. The structure allows clearing alarms for subordinate components for an on/off event of the parent component.
- An event triggers an on or off event for the subordinate component.
- Events not yet propagated from an NE to the EMS are not required to be preserved when the NE restarts.
- When the NE restarts, preservation is not required if the events have not yet propagated from an NE to the EMS.
- The default alarm history holds 50,000 entries.
- Any event for trunk CIC components can specify a range of CIC(s) in the component ID label.

Hungarian ISUP

Release 4.5 introduces Hungarian ISUP, which is a variant ETSI v3 ISUP based on the 1997 version of Q.761. This ISUP version impacts only customers using the Hungarian ISUP variant.

In Cisco BTS 10200, Hungarian ISUP is provisioned the same as all other existing ISUP variants.

ITU Local LNP

With Release 4.5, Cisco BTS 10200 now supports two Local Number Portability (LNP) options:

- ANSI North America LNP (available in prior releases)
- ITU local LNP (new to Release 4.5)

The difference between ITU local LNP and the pre-existing ANSI North America LNP is that ANSI North America LNP queries an external database known as a Service Control Point (SCP) to determine the Location Routing Number (LRN) of the recipient exchange.

In Release 4.5, ITU local LNP supports functionality described in the ITU Number Portability document Q.769. In ITU local LNP, the Cisco BTS 10200 “local” on-board database is queried to determine the Network Routing Number (RN) of the recipient exchange. Query methods supported by the Cisco BTS 10200 include:

- All Calls Query (ACQ) polling mechanism to local database
- Query on Release (QoR)
- Onward Call Routing (OCR, also known as Onward Donor Based Routing, or ODBR)

Queries to an external database using ITU TCAP are not supported.

Cisco BTS 10200 ITU local LNP also provides support for:

- Service Portability—Ability to keep the same directory number (DN) after changing services or charge plan with the same service provider (SP).
- Local Number Portability—Ability to keep the same DN after switching SPs, and staying within the same geographical area.
- Non-Geographic Number Portability for Service Numbers—Ability to keep the same service DN (for example, 800, 900) after switching SPs. The translated DN may be either the same or different.
- Service Interworking: CLIP/CLIR—The Routing Number (RN) or any Routing Info is never presented to the Calling entity. The Called Party Number (CDPN) is always presented regardless of whether it is ported in/out or not.
- Query based on general criteria—Cisco BTS 10200 can optionally allow or prevent a query based on general criteria. For example, for international incoming calls, the queries are based on a combination of the trunk group and Destination provisioning. For the international calls, if the Cisco BTS 10200 serves the gateway at the Point of Interconnect, it must perform the LNP function.
- Call Forwarding behavior—When attempting to complete the call (Call A) to a forwarded-to number that has been ported out (Call C), it is the forwarding exchange's (Call B's) responsibility to perform LNP. For example, if Caller A dials Caller B, and Caller B forwards the call to Caller C, then the query occurs when the call is forwarded from Caller B to Caller C.
- IAM Message Parameter Coding—NOA is coded, in addition to RN+DN included in the CDPN field. This behavior is part of the ITU local LNP variant.

NoA coding requirements are national, and the NoA value is provisionable.

North American Numbering Plan Administration Audit Feature

This feature allows the Cisco BTS 10200 Softswitch to generate a North American Numbering Plan Administration (NANPA) report for audit purposes. The NANPA report provides data based on the DN2SUBSCRIBER table for the Numbering Resource Utilization/Forecast (NRUF) report.

The NANPA audit report provides information on data that is provisioned in the switch concerning Code Holder, Block Holder, Native, and Non Native. The report input can be 10 digits or NPANXX, which requires the import capability of LERG updates as well as LCADS for FCC-required NANPA audit compliance.

This feature allows the Cisco BTS 10200 Softswitch to have a Number Block table that has no dependencies for routing or call classification. The Number Block Table is a single, customizable table that is the sole reference for NANPA audits. Updates to Number Block tables can come from data imported from other tables, changes from office-code updates, or manual updates.

The Number Block Table fields consist of the following:

- Number Block: NPA to NPA-NXX-XXXX
- Code Holder = Y/N
- Block Holder = Y/N
- Native = Y/N
- Non-Native = Y/N

ISUP Transparency on the Cisco BTS 10200-Cisco PGW 2200 Interface

ISUP transparency provides the capability to transfer Generic Transparency Descriptor (GTD) messages and information elements from a Cisco BTS 10200 Softswitch across an IP network to a Cisco PGW 2200. The Cisco PGW 2200 maps the GTD messages to ISUP messages, repackages them, and sends them out to the PSTN/SS7 network.

ISUP transparency is important because it enables the transport of calls from a SIP network through an IP network and out to a PSTN network without any loss of signaling information. ISUP transparency is achieved with the use of Cisco's GTD mechanism. GTD provides a means to specify messages of various protocols used in the PSTN network in plain text format. This is so they can be easily understood by the network elements within the IP network or on the boundary between PSTN and IP.

The ISUP Transparency on the Cisco BTS 10200-Cisco PGW 2200 Interface feature passes normalized parameters to expedite mapping at the PSTN interconnect side and any feature invocation necessary on either the Cisco PGW 2200 or the Cisco BTS 10200. It adds support for GTD attachments to SIP-T trunk messages to allow the Cisco BTS 10200 to interwork with the Cisco PGW 2200 for interconnection to the PSTN.

When the Cisco BTS 10200 Softswitch generates SIP messages to be sent out on SIP-T trunks, a GTD attachment is generated based on the GTD parameters defined in the GTD-PARMS token in the Softswitch Trunk Group Profile (softsw-tg-profile) table. GTD attachments of incoming SIP messages are decoded by the Cisco PGW 2200, and all GTD parameter contents are converted to the equivalent ISUP values in the appropriate information element on the outgoing PSTN side.

In addition, this feature adds support to map Progress Indication messages from the Cisco BTS 10200 Softswitch to SIP INFO messages with GTD attachments containing Call Progress (CPG) messages when the egress trunk is a SIP-T trunk. This supported feature applies only to SIP subscribers.

When a SIP INFO or RE-INVITE message is received over a SIP-T trunk with a GTD attachment containing a CPG message, a Progress Indication message is generated and sent to the system.

A network model configuration illustrates the need for an interface that allows SS7 information to be passed and, in some cases, acted upon or generated by the Cisco BTS 10200. In the deployment model, the Cisco PGW 2200 is the PSTN gateway, and the Cisco BTS 10200 provides a residential or Centrex application platform. This model is analogous to a TDM-based deployment where the Cisco BTS 10200 acts as the CLASS 5 switch, and the PSTN gateway is the trunking interface on that switch.

ISUP Transparency Requirements

The following PSTN supplementary services are enabled by this feature:

- Number ID Supplementary Services
 - Direct Dial In (DDI)
 - Calling Line Identification Presentation (CLIP)
 - Calling Line Identification Restriction (CLIR)
- Call Diversion Supplementary Services
 - Call Forwarding Busy (CFB)
 - Call Forwarding No Reply (CFNR)
 - Call Forwarding Unconditional (CFU)
 - Call Waiting (CW)
 - Call Hold (HOLD)
- Multiparty Supplementary Services

- Three-Party Service (3PTY)
- Transparency Requirements
 - Ability to provision which parameters to transport over GTD
 - Call Forwarding No Answer (CFNA)
 - Call Waiting (CW)
 - Call Transfer (SIP Refer is not supported with SIP subscriber Hold signaling)
 - Ability to Correlate Billing Records
- Functionality Provided by the Cisco PGW 2200
 - Number Portability (NP)
 - NoA Relay
 - Information/Information Request (INF/INR) and Identification Request/Identification Response (IDR/IDS) Messaging
 - ITU Method 2 Circuit Selection
 - NoA Modification and Routing
 - Calling Party Category (CPC) Based Routing
 - Ability to Modify A-Number Based on B-Number and B-Number Based on A-Number
 - Cause Analysis
 - Redirecting A-Number Screening
 - Virtual VPN Behavior
 - Calling Party Number (CGPN) Address Presentation Indicators

Limited Call Duration Service (Prepaid/Postpaid)

Cisco BTS 10200 Softswitch Release 4.5 supports the limited call duration (LCD) feature, including both prepaid and postpaid services. This support includes interfaces to an authentication, authorization, and accounting (AAA) server, and an interactive voice response (IVR) system. The LCD feature can be assigned to any Cisco BTS 10200 Softswitch subscriber with any phone type, including MGCP-based, SIP-based, and NCS-based phones.

Network Interfaces

The Cisco BTS 10200 Softswitch uses the following signaling interfaces for this feature:

- RADIUS-based interface to an AAA server.
- MGCP-based interface to a network IVR server.
- Additional interfaces for call-control signaling, including communications with MGCP-based and TGCP-based media gateways (MGWs), IP Transfer Points (IPT) via SIGTRAN (for SS7), and PacketCable-based CMTSs and eMTAs.
- SFTP interfaces to external third-party billing servers for transfer of billing records, and RADIUS interfaces to external record keeping servers (RKSSs) for transfer of PacketCable-based event messages (EMs).

Feature Description

The LCD feature supports both prepaid and postpaid services for subscribers.

- Fixed-prepaid (debit) service is an outgoing call management feature that allows a subscriber to pay for call charges in advance. Each time the subscriber makes a call, the charges for the call are deducted from the balance of the advance payment. If the subscriber uses up all of the advance payment, the Cisco BTS 10200 Softswitch blocks all further calls from this subscriber (until more money is added to the account).
- Postpaid-with-limit (credit) service is an outgoing call management feature that limits the calls originated from the subscriber so that total outstanding balance of charges for all the calls originated from the subscriber is less than a predefined limit. If the subscriber reaches the predefined limit, the Cisco BTS 10200 Softswitch blocks all further calls from this subscriber (until money is paid on the account or the limit is increased).



Note

This feature uses data from the automatic number identification (ANI) service to identify the calling party.

Web Report Interface Authentication

An enhancement was made to add authentication into the Web report interface in Release 4.5. In this release, the user name and password are the same as CLI login.

Web authentication uses the Pluggable Authentication Module (PAM) framework, so users can configure `/etc/pam.conf` to enable other authentication methods, such as RADIUS/LDAP.

To access the Web interface, complete the following steps:

1. Use the URL `https://hostname`.
2. Accept the certificate.
3. The Authentication Window appears.

Once authenticated, users can browse the Web page as usual, but in a secure channel.

Log Archive Facility

The Log Archive Facility (LAF) (optionally implemented at the customer site) allows for the automatic transfer/archival of Cisco BTS 10200 trace log files from each Cisco BTS 10200 network element to an external archive server running Solaris. For you to use this feature, the LAF parameters must be set up in `optcall.cfg` during the installation/upgrade.

For details, please refer to the Release 4.5 Network Site Survey and the Release 4.5 Network Information Data Sheet (NIDS). `Optcall.cfg` should specify the hostname or IP address of the external archive server, the target directory where the traces are to be stored, and the maximum disk usage allowed for storage. These must be specified for each Cisco BTS 10200 network element.

Also, the access authorization must be set up in the external archive server for the Cisco BTS 10200 network elements to log in non-interactively in order to transfer the files. For details, refer to the Release 4.5 Application Installation Procedure.

Once the archive server and the Cisco BTS 10200 are set up, the feature is enabled by use of a tool called “enableLAF.” Since there is usually a lot of pending data to transfer when the feature is enabled, Cisco recommends transferring the data during a maintenance window.

To disable the facility, use the “disableLAF” tool.

Other Enhancements

This section describes changes to all other enhancements made to Release 4.5. These are not new features, but rather enhancements or changes made to existing features.

The descriptions in this section are brief; for more information, refer to the Cisco BTS 10200 documentation. You can view the Document Change History table in the Preface of each book to see what changes have been made to the book for this release.

IP Addresses

Previous Cisco BTS 10200 releases required four IP addresses to be associated with each domain name (POTS, SIM, ASM). These IP addresses are now preserved for upgrade or fallback purposes only. The addresses are not used by these processes in Release 4.5. New domain names, each mapping to two logical IP addresses, must be defined for each of these processes.

In Release 4.5, these processes use newly-created migrating logical IPs instead.

Solaris 10

The Sun Solaris software used with Cisco BTS 10200 was upgraded to version 10.

For more information, refer to the [“Sun Solaris Version Upgrade” section on page 8](#).

Oracle 10g

The Cisco BTS 10200 EMS database was implemented with Oracle Release 8.1.7.4. Oracle Corporation announced the end of Error Correction Support for Oracle Database Version 8.1.7.x (8i) on Solaris SPARC Operating Systems, effective 31-DEC-2004. In order to provide Cisco BTS 10200 customers with the most current Oracle product support, Cisco BTS 10200 Release 4.5 is upgraded with Oracle Release 10g (10.1).

The Rule-Based Optimizer (RBO) implemented on previous Cisco BTS 10200 releases is obsolete in Oracle 10g. It is replaced by the Cost-Based Optimizer (CBO). To support the Oracle optimizer, a statistics collection process is scheduled to run weekly, by default on Sunday at hour 0. The Database Alarm 21 is issued if the statistics collection process fails.

Display of System Status

The commands that request the state of an element no longer report FAULTY; in Release 4.5, the commands replace FAULTY with the commands OOS-ADMIN or OOS-FAULTY, depending on the cause of the OOS state. The OOS-ADMIN state results only when the operator shuts down an application; all other non-manual causes of OOS are flagged as OOS-FAULTY. This information is reported on state requests such as a CLI “status” or the UNIX command “nodestat.”

Additionally, the operational state (FORCED/ACTIVE) is no longer used in Release 4.5 when you are using the “control” switchover command. This applies to “FORCED_ACTIVE_STANDBY,” “FORCED_STANDBY_ACTIVE” or “NORMAL.” A component can now reach a stable state of “ACTIVE” or “STANDBY” without any qualifier. The CLI commands are changed too.

In this example, the new version is dropping “forced,” so that:

```
control call-agent id=CA146;target_state=forced-active-standby
```

becomes:

```
control call-agent id=CA146;target_state=active-standby
```

The new version no longer uses “forced.”

Own Calling Number Announcement

A normal test and turn-up function for analog line installation is to provide a universal number that a technician can use to verify that the correct ANI was assigned to the line. This function is definable in the Cisco BTS 10200, and involves the announcement server playing the ANI to the analog user.

In order for you to use calling number announcement, the ANNOUNCEMENT table must be provisioned to assign announcement resource. The announcement can then be triggered through either the DESTINATION table or the DN2SUBSCRIBER table.

Billing Record Cause Codes

Previously, billing records for OCB did not indicate the service denial status when calls were blocked due to OCB.

The billing-cause codes now correspond to the following release cause codes:

- 1115 SERVICE_DENIED
- 1116 SERVICE_DENIED
- 1117 SERVICE_DENIED

Billing Record Enhancements

New billing fields and other billing record changes are required for Release 4.5 or were made in Release 4.5.1. For specific changes, refer to the [Cisco BTS 10200 Softswitch Release 4.5 Billing Guide](#).

Alarms/Events Reported for DNS Failures

A network management system is used to track failing instances of devices whose DNS name resolves to several IP addresses or SRV entries. Cisco BTS 10200 generates an event when all request retransmission attempts fail. The SIP stack raises a WARNING event, when the retransmissions are exhausted.

Two new events are defined as part of this enhancement:

- SIGNALING(146): Ensures the DNS server is up and running for host name resolution, and provisioned properly to resolve to correct order of IP addresses. Also ensures that the previous hop network component is alive and in healthy state for failures related to SIP responses.
- SIGNALING(147): Adds an entry to SRV in the DNS server, and fixes Cisco BTS 10200 provisioning.

Additionally, Protocols 12 and 13 were added to the report.

FDT and SDT Flags

Release 4.5 now accepts the tone-type (STUTTER, DIAL, CONFIRM, NONE) for the SDT and FDT flags in the Feature table. This addresses changes in the following modules:

- Service-Logic-Activation-Deactivation-Interrogation-Framework (sl-adi-framework)
- Activation/Deactivation/Interrogation of Call Forwarding Unconditional/No Answer/Busy features (cf-adi)

No other features were impacted by this change.

ACR and SS7 Incoming Calls

Incoming calls without calling-party information are allowed to complete to users with the Anonymous Call Rejection (ACR) feature assigned and activated. As a result, users with ACR can receive calls with unknown calling party information.

This feature is working as per LSSGR GR-567. The request was to enhance the feature implementation to customize the feature behavior.

OverDecadic Digit Support for Generic DN Parser

EMEA networks use OverDecadic Digits for LNP and some emergency services. To support OverDecadic Digits, the Generic DN Parser was modified to support provisioning of digits A-F, in addition to digits 0-9, *, and #.

NDC Now Optional

Some countries do not use NDC (area codes), and as a result, cannot provision subscribers without NDC.

If NDCs are not used in the country, the enhancement was made to split the exchange code into NDC, EC, and DN-GROUP. Since it is in the office code table, call processing assumes a 4-digit office code index, and the DN-GROUP in the office code table is provisioned as 1xxx, 2xxx, etc.

Parameters for Noun=User Are Changeable

After a new user is created via the command line interface (CLI), the parameters Days_valid and Warn, for the noun “user” can now be changed by a CLI user with the highest privilege (such as btsuser).

Password Key Added for CLI User Command

The parameter Password for the noun “user” is now a required parameter when you are adding a new user. This is a security enhancement.

Provision CA-CONFIG Defaults in Call Agent and Feature Servers

Previously, the default values for all CA-CONFIG parameters were hard coded in the Call Agent and Feature Server. The CA-CONFIG-BASE table identified the default value, but did not always match with what was used by the application.

The enhancement also included a fix to load the CA-CONFIG-BASE table in DBM when the system is initialized by reading a file. When the DBM API is invoked to read a CA-CONFIG value, the API returns the configured value in CA-CONFIG, or the default value if it is not configured in the CA-CONFIG table. The application no longer uses the hard coded values.

Configuring Slot/Sub-Slot/Port for ISDN D-Channel Backhaul

Prior to Release 4.5, you could only see the slots in the CLI; in this release, you now can see the slot and port. Also in this release, the ISDN D-channel backhaul can be configured three ways:

1. Slot and port (configure DCHAN-FORMAT as SLOT-PORT in ISDN-DCHAN table). This is the configuration similar to previous release where DCHAN-SLOT and DCHAN-PORT were used to configure the D-channel.
2. Port (configure DCHAN-FORMAT as PORT in ISDN-DCHAN table). This is generally used for an ISDN gateway that has more than 255 D-channels (such as VXSM). In this mode, only the DCHAN-PORT field from ISDN-DCHAN is used to configure the D-channel, and the DCHAN-SLOT field is set to 0.
3. Slot, sub-slot and port (configure DCHAN-FORMAT as SLOT-SUBSLOT-PORT in ISDN-DCHAN table). This is a new feature in Release 4.5, where the user can specify slot, sub-slot, and port for the D-channel.



Note

Option 3 is only supported in certain IOS gateways with certain features, such as the 28xx, 37xx, or 38xx, with NM HDV2 (Soprano) module plus a 2MFT-T1-DI card (HumVee).

Increase Table Size for Region Profile Table

The Region Profile Table defines regions associated with ANI. This particular application requires approximately 1 million ANI records to be associated with multiple regions. The policy-region routing prefixes appropriate OLI digits to the ANI before routing the call. The size was increased from 125,000 records to 1 million records.

The Region Profile table was increased to 1 million records in Release 4.5 for the ROUTE-SERVER mem.cfg. The new record size is only applicable for the ROUTE-SERVER related mem.cfg.

Provisioned Subscriber DN and Privacy

In previous Cisco BTS 10200 releases, subscribers were unable to use the sendbilling_DN parameter in the subscriber table. As a result, the ANI may not have been sent for some subscribers.

In Release 4.5, you can now change the sendbilling_DN parameter. For an individual subscriber, if the SEND-BDN-AS-CPN is set, Cisco BTS 10200 delivers Billing DN (Charge Number) as the Calling Party Number in the setup message for all calls, including Emergency Calls.

The Cisco BTS 10200 now performs the following operations:

1. Reading SEND-BDN-AS-CPN from the subscriber table for incoming calls from an individual subscriber/PBX, and sending the calling party number accordingly.
2. Reading SEND-BDN-FOR-EMG from the subscriber table for incoming 911 calls from the subscriber, and sending the calling party accordingly.
3. Reading the Privacy field from the Subscriber table, and performing an appropriate action for the value USER.

No Automatic Alarm-status=Off After System Recovery

In previous releases, the system did not automatically change the alarm-status to OFF for Database alarm numbers 3, 4, 6, 7, 8, 9, 10, 11, and 12 after the system recovery even when the event condition cleared.

Show alarm now shows the alarm-status=off.

Billing Information for CF Interrogation

In this enhancement, the CFx Interrogation billing record does not show that it is a forwarding interrogation attempt if the feature is deactivated. This is as per design. The Call Forwarding Unconditional Interrogation (CFUI) feature does not send the Furnish Charging Information (FCI) message when the interrogation fails (if, for example, the CFU is not active, or active to a different DN).

When the CFU is deactivated in the SIP phone subscriber, and a subscriber uses `*#57*B number#`, the correct announcement is received, “Call forwarding is activated, but the number is not programmed.” However, the billing record service should show the same results that occur when CFUI with CFU is activated, including ServiceID, ServiceStatus information.

ACR and 200-OK Message

The ACR feature was changed so that it does not send a 200-OK in the beginning without checking if a call can be rejected or not.

Previously, the ACR feature sent the 200-OK irrespective of the check. However, the ACR should send the 200-OK only if the call is rejected, not if the call is allowed.

Show Faulty Trunks

Previous to Release 4.5 reports could be run to show all faulty trunks in a trunk group. However, ringing phones appeared “off normal,” as the following command shows:

```
status tt tgn-id=50199; cic=all;off-normal=yes
```

In Release 4.5, ringing is now included as a normal trunk state.

Speed Call 1 Digit

Previously, subscribers were blocked from making international calls through COS restrict IDs. When trying to make international calls, the subscriber received announcements.

The subscriber was blocked from making international calls through Class Of Service (COS) restrictions. However, subscribers could bypass that restriction by subscribing to the Speed Call feature and provisioning the international number as a speed call digit.

Now, the speed-call digit is translated into the actual number, and COS restrictions (including international call restrictions) are applied on that number for the subscriber.

SIM Memory Audit

The SIM memory audit is done periodically for the active feature relationships to clear any stale relationships. Audits on the entire feature relationship table are also performed at a configurable fixed time every day to clean the orphaned table elements.

The periodicity and start_time for the SIM memory audits are configurable in the Activity table via CLI. For more information, refer to the [Activity table](#) section in the *Cisco BTS 10200 Command Line Interface Reference Guide*.

SIP Dynamic Memory Audit

This is an enhancement to clear stale call blocks or register blocks if found. The advantages for auditing SIP dynamic memory include:

1. The ability to catch errors early in the development cycle if the dynamic memory is being leaked.
2. A graceful resources recovery.
3. Avoiding field problems.

The SIP Memory Audit is done periodically for the Active Calls to clear the stale Call Blocks and at a fixed time for the active Register Contact Blocks. Audits on the entire Call Block table and RegContact Block table are also performed at a configurable fixed time every day to clean the orphaned Table elements. The periodicity and start_time for the Audits are configurable in the Activity table via CLI. For more information, refer to the [Activity table](#) section in the *Cisco BTS 10200 Command Line Interface Reference Guide*.

SIP Transport

When a 503 response is received, the entity receiving the response proceeds by submitting the same request as a new transaction (with new branch ID) to the next IP address in the SRV list. Previously, when SIA received the 503 response, it tore down the call.

As a result, some calls may not have completed if one of the nodes in an SRV list returned the 503, while other nodes in the list were capable of handling the request successfully.

If an SRV server receiving the INVITE does not respond within the retransmission timer period, this enhancement allows for configuring the Cisco BTS 10200 to send the next retransmission of the same request to either the same server (as recommended in RFC 3263) or the next server in the SRV list (legacy Cisco BTS 10200 behavior) using a provisionable flag `DNS_SRV_ADV_ON_RETRANS_TIMEOUT` on the Softswitch Trunk Group Profile table.

INVITE Retries Are Configurable

The SIP protocol adaptor enables the configuration of the number of INVITE and non-INVITE retries on timer expiry (instead of the fixed 6), and also make the retry timers configurable. This improves route advancing and completes calls more quickly if one IP address is down.

SIP timers are configurable on a per trunk basis, or on a system wide basis for all non-trunk messages. The number of retries and the retry interval can be tuned using RFC3261 timers. The guidelines and recommendations on configuring SIP timers are available in the *Cisco BTS 10200 SIP Protocol User Guide*.

The timers are configurable on a global basis through the Softswitch Trunk Group Profile (SOFTSW Trunk Group Profile) and Call Agent Configuration (CA-CONFIG) tables. For more information, refer to the [SOFTSW Trunk Group Profile](#) and [CA-CONFIG](#) sections in the *Cisco BTS 10200 Command Line Interface Reference Guide*.

SIP Session Timers

SIP Session Timer values configured prior to Release 4.5 are reset to the default values after upgrading to Release 4.5.

For more information, see the [“Upgrades and SIP Session Timers”](#) section on page 13.

SIP Retry

SIP responses received from a Re-Invite or Update sent during an active call that contain a Retry-After header invoke the SIA retry mechanism. Currently, this includes only the SIP 500 class response. The check has been expanded to include other responses.

Bypass Flag for Time Difference

In previous releases, a platform failed to start on command, reporting Reason=MATE TIME OUT OF SYNC. The solution is to synchronize the time of the two mates.

Release 4.5 added a specific bypass flag for the time difference alone on startup. The name of the flag is `-notimecheck`.

For example:

```
platform start -notimecheck
```

The platform start script can start the platform while ignoring time differences with mate. Timecheck should not be used—use only in emergency situations.

Nodestat Obtains and Shows Status Information from Hub

When an OMS hub communication link status changes (active or inactive), the nodestat now reports the status promptly.

SIP Stack Message Size

Previous to Release 4.5, the SIP stack could only send and receive messages up to 1500 bytes in size from the network. If a message was bigger than 1500 bytes, only the first 1500 bytes were read and parsed.

Release 4.5 fixes the limitation imposed on the maximum size of the SIP messages which can be sent or received. The SIP stack can now receive/send SIP messages up to 3000 bytes in size.

SIP Trunk Hop Counter

The SIP Trunk Hop Counter feature was added into Cisco BTS 10200 Release 4.1, but was not provisionable. However, the feature's provisionable components are available in Release 4.5, and are provisionable using the SOFTSW Trunk Group Profile table.

The MAX-Forward for the SIP hop counters specify when an outbound SIP INVITE message requires an initial maximum forwards value. The default is 70.

Additionally, seven SIP hops are equivalent to one SS7 hop.

For more information, refer to the [“SOFTSW Trunk Group Profile”](#) section in the *Cisco BTS 10200 Command Line Interface Reference Guide*.

Cisco BTS 10200 Sends SDP for SIP Call When rbk=N for Call Waiting

When a SIP call inbound to the Cisco BTS 10200 is routed to a local subscriber, and this call causes “call waiting” at the subscriber, the originator is provided local ringback indication. However, in this case, the SIP interface was providing remote ringback indication. This may result in the originator not hearing ringback or possibly hearing the discussion of the other dialog.

The SIP interface was corrected to provide local ringback.

SIA Diversion Header

Previously, when one diversion header was received in the initial SIP Invite message, the Original Called Number (OCN) was populated. To be consistent with other adaptors, the value is now copied to the Redirect Number (RDN) as well.

SIA Restart

Prior to Release 4.5.1, it was not possible to restart a SIA process. If a SIA process failed, a failover from an active BTS 10200 Call Agent (CA) to the standby mate occurred. If a standby CA was unavailable, the platform continued to run without a SIA process.

Beginning in Release 4.5.1, the SIA Restart enhancement allows the BTS 10200 to restart a failed SIA process. After a SIA process restart, new calls can be set up, and calls that were established (answered) prior to a SIA process failure continue to be handled. Also, any transactions that were pending at the time of a SIA process failure are not processed after the SIA restart.

A SIA process restart can occur a maximum of three times every 30 minutes. If a restart happens more than three times in 30 minutes while running a BTS 10200 duplex environment, a failover from an active CA to a standby CA occurs. In a simplex environment, or if a standby CA is unavailable, the CA platform shuts down.

SIP Outbound Numbers Require +CC Depending on NOA

RFC 3398 states that any outbound SIP number with a NOA of NATIONAL must be prefixed with “+CCnumber” which is an international format, and any number with NOA=subscriber must be formatted also with international significance. This was not done in previous releases.

Sending Full E.164 is enabled by a flag in softsw-tg-profile to enable interworking with downstream devices that require this number format.

SIP Stack

SIP message loop detection was removed in Release 4.5. Previously, the SIP stack did not allow receipt of an un-changed Request URI on hairpinned INVITES. This required the entity that was hairpinning the SIP call back to Cisco BTS 10200 to modify the user portion of the Request-URI, so that Cisco BTS 10200 does not detect a loop.

Since the Digman feature was added, the digit manipulation is performed within Cisco BTS 10200, thereby preventing a requirement for this check. As such, this check is a configurable option that can be toggled through SIA's configuration file for SIP stack.

DOMAIN-NAME Verified on SIP INVITE Messages

SIP INVITE messages are now validated. This helps detect invalid provisioning or configuration, as well as providing a basic check against intrusion from unauthorized call-agents.



Note

This is applicable to the CP environment only.

An alarm is generated when an invalid SIP INVITE is detected due to an invalid domain name. The event is corrected with the following steps:

1. Verify the provisioned domain name and the one used by SIM to process the command-line parameter.
2. Verify the message source, whether it is on-net request or a potential unspoofed intrusion attempt.

A “403 FORBIDDEN MSG” is returned in response to an “INVITE MSG” from an unauthorized/unrecognized CP. The CP processes the call as a basic call.

Due to a change in the Logical IP Migration feature, this feature is suppressed by default in Release 4.5. To turn on the DOMAIN NAME validation feature, use the `-enable_dnv` option included in `Args=` of the `platform.cfg` for POTS and ASM.

Time-Out (TO) to Ring Signal for MGCP/NCS

Previously for ring and ringback signal to the MGCP Gateway, Cisco BTS 10200 always specified infinite timeout (encoded as ‘to=0’). If the no answer timer is started by Cisco BTS 10200, after timeout Cisco BTS 10200 stops ring/ring-back and releases the call.

With this enhancement, the service provider can configure whether Cisco BTS 10200 controls the ring/ring-back timer or lets the gateway use its default configuration. When `MGCP-TO-SUPP` in `MGW-PROFILE` is configured as `Y`, Cisco BTS 10200 sends a ring/ring-back signal to MGCP gateway with no timeout (`to=0`), as previous release.

When `MGCP-TO-SUPP=N`, then Cisco BTS 10200 does not specify any timeout parameter to MGCP gateway and the gateway chooses the timeout configured locally (generally defaults to 180 seconds).

POP OFFICE SERVICE ID

Changes were made to support the office service ID in the POP table.

Now, the office service ID provisioned in the POP table is used, when available, rather than the default office service code provisioned in the `CA-CONFIG` table.

SIP Stack Attempts Next Address If TCP Connection Fails for INVITE

When provisioning a SIP trunk-grp, the `SOFTSW-TSAP-ADDR` is usually set to a FQDN that resolves to two or more IP addresses for the destination SIP endpoint(s). Prior to Release 4.5, when a SIP request was transmitted, if the `NON-SRV-TRANSPORT` of the `softsw-tg-profile` was set to `TCP` and there was a failure to communicate with the first IP address of the FQDN, then no other IP address was tried.

In Release 4.5, the software has been enhanced so that each of the IP addresses that the FQDN resolves to is tried in succession when there is a failure to communicate with the destination SIP endpoint.



Note

This functionality has always worked when UDP is the selected transport.

A-Law to U-Law Transcoding Interworking

Previously, the Cisco BTS 10200 could only be switched globally between A-law and U-law voice encoding. However, depending on the brand of PBXu, the setup was either rejected with “incompatible destination,” or the call was completed but did not sound right, because there was no transcoding of the B channel due to mismatched A-law or U-law voice encoding.

Two new fields were added to the TRUNK-GRP table to allow voice encoding between the Cisco BTS 10200 and different PBXs.

The new fields are:

- VOICE-LAYER1-USERINFO (AUTO, G711-ULAW, G711ALAW)
 - AUTO (same as configured/received for incoming leg) - DEFAULT
 - G711-ULAW
 - G711-ALAW
- VOICE-INFO-TRASFER-CAP (AUTO, SPEECH, 3POINT1KHZ-AUDIO)
 - AUTO (same as configured/received for incoming leg) - DEFAULT
 - SPEECH (If voice call, override with Speech)
 - 3POINT1KHZ-AUDIO (If voice call, override with 3.1 KHz audio)

SIA Authentication

This is an enhancement for efficient lookup while processing requests targeted for SIP subscribers. It involves internal caching of the Serving Domain Name of the user sending a SIP request and using it for subsequent messages instead of doing a separate table lookup for each request.

SIP NOTIFY Rejected from Unity

In previous releases, if a request was received from a trunk that had the same domain name as the Cisco BTS 10200 serving domain name in the from header, the call failed, and the MWI Notify from Unity was rejected.

This is resolved in Release 4.5. In Release 4.5, it performs the trunk identification before subscriber identification, and thus identifies the trunk correctly.

SIM Feature Server Status Saved in Feature Server Table

The enhancement saves the Feature Server (FS) communication state in the FS table, instead of on heap memory, with no externally visible impact to call processing. The Feature Server's communication status was previously held in heap memory by the SIM process. The fields in the Feature Server table for this data are now updated with the status.

Change Counter Names to SIS and SIP for Release 4.5 Measurements

The PEG Counters names were changed to match industry terminology. There are two types of SIP counters, those used by multiple stacks related to SIP, and those used by the SIP Adaptor.

The Cisco BTS 10200 documentation uses the new names for several counters. In Release 4.5:

1. SIP common counters now begin with SIS_ instead of SIP_ for the SIA, SIM, POTS, and AIN categories.
2. SIA-specific counters now begin with SIA_ instead of SIP_.
3. AUDIT_SIP counters in the SIA category now begin with SIA_AUDIT instead.

Change in RACF Service Logic

Previously, the Remote-Activation-Call-Forwarding (RACF) feature worked successfully, but call-forwarding failed. This caused RACF users to think their activation was successful, even if they had entered incorrect or partial numbers. However, users who call these RACF users heard failure announcements and the calls weren't forwarded.

With this new enhancement in Release 4.5, RACF checks for the validity of the forwarded number.

Heap Memory Monitor

There are three new alarms now generated when any process heap memory usage is nearing its limit. These allow for taking precautionary measures in the Cisco BTS 10200.

The alarms include:

- AUDIT 16, "Process Heap memory usage exceeds minor threshold level." This alarm is issued when the process heap usage exceeds 70% of its max heap limit.
- AUDIT 17, "Process Heap memory usage exceeds major threshold level." This alarm is issued when the process heap usage exceeds 80% of its max heap limit.
- AUDIT 18, "Process Heap memory usage exceeds critical threshold level." This alarm is issued when process heap usage exceeds 90% of its max heap limit.

VMWI and SDT on Per Line Basis

The current configuration parameters essentially specify whether or not the media gateway can provide visual and audible (stutter dial tone) message waiting indication.

After implementing the feature, in addition to MGW-PROFILE level configuration service, the provider must configure two new fields in SUBSCRIBER table to provide visual or audible message waiting indicator.

MGW-PROFILE

To support the visual message waiting indicator (VMWI), use the following CLI commands to enable VMWI and/or SDT at the media gateway level:

```
CLI> change mgw-profile id=<mgw-profile-name>; mgcp-vmwi-supply;
```

To support Stutter Dial Tone (SDT), also known as Message Waiting Indicator (MWI):

```
CLI> change mgw-profile id=<mgw-profile-name>; mgcp-mwi-supply;
```

To view the current provisioning data of the MGW-PROFILE:

```
CLI> show mgw-profile id=ms-profile
```

For example:

```
ID=ms_profile
VENDOR=Cisco
MGCP_VARIANT=NONE
RBK_ON_CONN_SUPP=Y
PACKET_TYPE=IP
AAL1=N
AAL2=N
AAL5=N
PVC=N
```

```

SVC=N
SPVC=N
EC_SUPP=N
SDP_ORIGFIELD_SUPP=Y
SDP_SESSNAME_SUPP=Y
SDP_EMAIL_SUPP=Y
SDP_PHONE_SUPP=Y
SDP_URI_SUPP=Y
SDP_BANDWIDTH_SUPP=Y
SDP_INFO_SUPP=Y
SDP_TIME_SUPP=Y
SDP_ATTRIB_SUPP=Y
MGCP_ERQNT_SUPP=N
MGCP_HAIRPIN_SUPP=Y
MGCP_QLOOP_SUPP=Y
MGCP_3WAY_HSHAKE_SUPP=Y
MGCP_CONN_ID_AT_GW_SUPP=Y
MGCP_VMWI_SUPP=Y
TERMINATION_PREFIX=ivr/
PORT_START=0
MGCP_VERSION=MGCP_1_0
MGCP_RSVP_SUPP=N
MGCP_RSIPSTAR_SUPP=Y
MGCP_TERM_INIT_LEVEL=0
MGCP_HAIRPIN_Z2_SUPP=N
DTMF_OOB_SUPP=N
MGW_TYPE=UNSPECIFIED
OSI_SUPP=N
MGCP_DIALTONE_TO_SUPP=Y
MGCP_MWI_SUPP=Y
SPARE1_SUPP=N
IPTOS_RTP_SUPP=Y
USE_STATIC_PROFILE=N
REFRESH_DIGIT_MAP=N
MGCP_XDLCX_SUPP=N
MGCP_CAS_BLOCK_SUPP=N
CODEC_NEG_SUPP=Y
MGCP_DEFAULT_PKG=NONE
MGCP_KEEPALIVE_INTERVAL=60
MGCP_KEEPALIVE_RETRIES=3
MGCP_T_TRAN=400
MGCP_MAX1_RETRIES=2
MGCP_MAX2_RETRIES=3
MGCP_T_LONGTRAN=5
PC_MPTIME_SUPP=Y
MGCP_CAP_NEG_REQ=Y
RBK_ON_INACTIVE_CONN_SUPP=N
MGCP_NAS_SUPP=Y
DOMAIN_NAME_CACHING_SUPP=Y
BTXML_SUPP=N
CONN_MODE_REQUIRED_IN_MDCX=N
MGCP_NE_LOCALNAME_SUPP=N
KRB_REEST_FLAG=Y
IPSEC_SA_ESP_CS=3DES-MD5, 3DES-SHA1, NULL-MD5, NULL-SHA1
IPSEC_SA_LIFETIME=86400
IPSEC_SA_GRACE_PERIOD=21600
IPSEC_ULP_NAME=IP
IKE_GROUP=2
IKE_SA_LIFETIME=86400
IKE_CS=3DES-MD5, 3DES-SHA1
MGCP_EP_SPECIFIC_CAP_SUPP=N
KEEPALIVE_METHOD=AUEP
MGCP_MAX_KEEPALIVE_INTERVAL=600
MGCP_REQ_ID_SUPP=N

```

```

MGCP_PIGGYBACK_MSG_SUPP=Y
MGCP_QDISCARD_SUPP=Y
MGCP_TO_SUPP=Y
MGCP_TEST_CONN_SUPP=Y
PARALLEL_TEST_CONN_SUPP=N
T38_FXR_LOOSE_SUPP=AUTO
FAX_INBAND_METHOD=GW_SPECIFIED
SDP_CAP_ENCODE_TYPE=AUTO

```

Subscriber Level

At the subscriber level, use the following CLI commands to enable VMWI and/or SDT.



Note

Both MGW-PROFILE and SUBSCRIBER must be provisioned to “Y” to receive VMWI and/or SDT.

To support VMWI:

```
CLI> change SUBSCRIBER ID=<subscriber-id>; VMWI=Y;
```

To support SDT/MWI:

```
CLI> change subscriber id=<subscriber-id>; sdt-mwi=Y;
```

To show the SUBSCRIBER PROVISIONING DATA:

```
CLI> show subscriber id=vm-sub2;
```

For example:

```

ID=vm_sub2
CATEGORY=PBX
STATUS=ACTIVE
DN1=9722331288
PRIVACY=NONE
TGN_ID=80033
PIC1=NONE
PIC2=NONE
PIC3=NONE
GRP=N
USAGE_SENS=Y
SUB_PROFILE_ID=sub_pmlhg_prof1
TERM_TYPE=TG
IMMEDIATE_RELEASE=N
TERMINATING_IMMEDIATE_REL=N
SEND_BDN_AS_CPN=N
SEND_BDN_FOR_EMG=N
PORTED_IN=N
BILLING_TYPE=NONE
VMWI=Y
SDT_MWI=Y

```

All of these options default to **Y** in both the MGW-PROFILE and SUBSCRIBER tables. To disable the feature(s), simply replace the **Y** in the above CLI commands with **N**.

Piggybacked MGCP Messages Now Configurable Using MGW-PROFILE

Previously, Cisco BTS 10200 had a configuration in platform.cfg for MGCP subsystem to enable/disable sending of MGCP commands piggybacked in ACK message toward the media gateway.

This configuration was moved to the MGW-PROFILE table so it can be configured via CLI.

The CLI command for this is MGCP-MSG-PIGGYBACK-SUPP, and it is applicable to Release 4.5 and above.

New Field OSS-SIG-TYPE

Release 4.5 introduces a new field, OSS-SIG-TYPE. The field changes provisioning for Operator trunk groups, and is used instead of OSS-SIG in the MGW-PROFILE. OSS-SIG-TYPE allows for configuring NBEC, MOSS, and EAOSS on the CAS-TG-PROFILE table in OSS-SIG-TYPE.

Configurable Field for Sending FastStart in CALL PROCEEDING or ALERTING

The H.323 FastStart parameter is always sent in as a backward message to the originating side (CALL PROCEEDING or ALERTING).

The newly-defined schema field SEND-FS-CALLP fields from the H323-TERM-PROFILE and H323-TG-PROFILE tables are configurable for sending the FastStart element in an ALERTING or CALL PROCEEDING message.

Updated EventObject and Version ID Field

Previously, Cisco BTS10200 sent Event Messages to the DF server with the incorrect version number in the EM Header field of every Event Message. This impacted the Cisco BTS10200-DF inter-operability where the Event Messages sent by the Cisco BTS 10200 to the DF server were ignored by the DF server.

There were two changes for this enhancement.

1. The Version ID and Event Object fields in the EM Header are implemented per the recommendation provided by latest PacketCable specifications.

The previous implementation was:

- Version_ID: Always set to 1. (for example, Event object is not used.)
- Event Object: Always set to 0, as this object is not used.

This was changed to a new implementation:

- Version_ID: Always set to 2 for CALEA (for example, Event object is used.)
- Event Object: set to 0 for messages going to RKS, set to 1 for messages going to DF.

2. The Electronic Surveillance Attribute in Signaling Start Message was updated.

Updated H.323 Stack

This enhancement incorporates a new version of the Cisco IOS H.323 stack into the Cisco BTS 10200 H.323 code-base. The new stack contains bug fixes pertaining to stability and reliability.

In addition, the new stack contains the infrastructure needed to implement new Cisco BTS 10200 H.323 features.

Ringback on CAS Trunking Gateway

Prior to this enhancement, for outgoing calls on CAS interface, Cisco BTS 10200 tried to provide ringback on connection from terminating CAS Gateway. This was because some CAS PBXs do not provide inband ringback information. When connected to switch or operator services, the far-end may provide inband ringback/announcement.

In CAS signaling there is no parameter to indicate “inband information available” (equivalent of Progress Indicator). This enhancement allows service providers to configure (per CAS-TG-PROFILE), whether or not remote switch/PBX provides inband information during alerting/ringing.

Measured Rate Flag

A flag was inserted in the Subscriber table to indicate flat versus measured rate. This is then put into the EM stream and in the CDB. The flag is sent to the billing system so subscriber knows whether it was a flat or measured rate.

Account Code in Event Message Billing

The subscriber’s Account Code appears in Event Message billing. A new group of call information needs is now accounted for with PBX terminated customers.

Support for Account Code and Authorization Code was added.

Account code/Authorization code is an existing feature in Cisco BTS 10200, and it is recorded on CDR. This enhancement adds these codes in EM per PacketCable specifications.

Account codes allow call charging to user projects, departments or special accounts, etc. A subscriber may activate the Account Code service capability when initiating a call (usually a long distance call) in order to have the call accounting recorded under a special project or account.

Authorization codes provide the capability for a subscriber to override call restrictions for a single call. A subscriber may be restricted from making toll calls and may decide to activate the Authorization Code service capability when placing a long distance phone call in order to remove the default call restrictions for that one call.

New, Modified, or Deprecated Alarms

The following is a list of events that are new, modified or deprecated from Release 4.4.x to 4.5.x.

New

- Audit 16
- Audit 17
- Audit 18
- Signaling 146
- Signaling 147
- Signaling 151
- Signaling 152
- System 13
- System 14

Modified

- Signaling 36
- Signaling 68
- Signaling 79
- Audit 5

Deprecated

- Audit 9
- Billing 39
- Signaling 2
- Signaling 3

Other Features

Changes from Previous Releases

In Release 4.5, users can no longer change ntp-server from the CLI, but still can view it. The command has been marked as obsolete in the Release 4.5 CLI Guide.

Vertical Service Code Limitation

If there is more than one entry in the Vertical Service Code table with the same leading feature activation code, the feature server can map the feature activation (from the handset) to the wrong feature. For example: the feature activation codes for CPRK and CWD are "*58" and "*58#". When a subscriber activates CWD from the handset by dialing "*58#", the feature server can activate the CPRK feature instead.

Measurement Changes

This section describes the measurement changes. For more information about measurement changes, refer to the [“Traffic Measurements”](#) chapter of the *Cisco BTS 10200 Softswitch Operations and Maintenance Guide*.

The following counters added new fields.

- **Call Processing Counters new fields:**
 - CALLP_TOTAL_TDISC_ORIG_ATTMP
 - CALLP_NLB_TEST_SUCC
 - CALLP_NLB_TEST_FAIL
 - CALLP_NCT_TEST_SUCC
 - CALLP_NCT_TEST_FAIL
 - CALLP_LB_TEST_SUCC
 - CALLP_TEST_ROUTE_SUCC
 - CALLP_T38_FAX_MEDIA_SETUP_SUCC
 - CALLP_T38_FAX_MEDIA_SETUP_FAIL
- **Service Interaction Manager Counters new fields:**

- SIM_AUDIT_CCB_FREED
- SIM_AUDIT_SIP_CCB_FREED
- **POTS Local Feature Server Counters new fields:**
 - POTS_CFC_ACT_SUCC
 - POTS_CFC_ACT_FAIL
 - POTS_CFC_ACT_ATTMP
 - POTS_CFC_DN_CHG_ACT_SUCC
 - POTS_CFC_DN_CHG_ACT_FAIL
 - POTS_CFC_DN_CHG_ACT_ATTMP
 - POTS_CFC_DEACT_SUCC
 - POTS_CFC_DEACT_FAIL
 - POTS_CFC_DEACT_ATTMP
 - POTS_CFC_INTERROG_SUCC
 - POTS_CFC_INTERROG_FAIL
 - POTS_CFC_INTERROG_ATTMP
 - POTS_CFC_FORWARD_SUCC
 - POTS_CFC_FORWARD_FAIL
 - POTS_CFC_FORWARD_ATTMP
 - POTS_NSA_INVOKE_SUCC
 - POTS_NSA_INVOKE_FAIL
 - POTS_NSA_INVOKE_ABANDON
- **POTS Miscellaneous Feature Server Counters new fields:**
 - POTS_PS_SUCC
 - POTS_PS_FAIL
 - POTS_PS_MANAGE_SUCC
 - POTS_PS_MANAGE_FAIL
 - POTS_VM_ACT_SUCC
 - POTS_VM_ACT_FAIL
 - POTS_VM_DEACT_SUCC
 - POTS_VM_DEACT_FAIL
 - POTS_VM_ACCESS
 - POTS_VM_ATTMP
 - POTS_LCD_AUTH_ATTMP
 - POTS_LCD_AUTH_SUCC
 - POTS_LCD_AUTH_FAIL
 - POTS_LCD_REAUTH_FAIL
 - POTS_LCD_FORCED_DISC
- **POTS Class of Service Feature Server Counters new fields:**

- POTS_COS_TOLLFREE_BLOCKED
- POTS_TDISC_CALLS_OUTG_BLOCKED
- POTS_COS_TOT_AUTH_IVR_SESSION
- POTS_COS_TOT_ACCT_IVR_SESSION
- POTS_COS_TOT_IVR_FAIL
- **TCAP Protocol Counters new fields:**
 - TCAP_OPERATION_REQ_RX
 - TCAP_OPERATION_CONFIRM_RX
 - TCAP_OPERATION_IND_RX
 - TCAP_COMPONENT_REQ_RX
 - TCAP_COMPONENT_CONFIRM_RX
 - TCAP_COMPONENT_IND_RX
 - TCAP_DATA_IND_RX
 - TCAP_UDATA_IND_RX
 - TCAP_DATA_REQ_RX
 - TCAP_DELIMITER_REQ_RX
 - TCAP_DELIMITER_IND_RX
 - TCAP_OPEN_IND_RX
 - TCAP_OPEN_CONFIRM_RX
 - TCAP_STATUS_IND_RX
 - TCAP_DIALOG_CONFIRM_RX
 - TCAP_CLOSE_IND_RX
 - TCAP_ABORT_IND_RX
 - TCAP_BIND_CONFIRM_RX
 - TCAP_STAT_CONFIRM_RX
 - TCAP_NOTICE_IND_RX
 - TCAP_STAT_IND_RX

- **ISUP Protocol Counters new fields:**

The following Signaling Gateway-based ISUP protocol counters are provided in Release 4.5. This is a superset of all the possible counters across all of the supported ISUP variants.

- ISUP_MSG_TX
- ISUP_MSG_RX
- ISUP_ACM_TX
- ISUP_ACM_RX
- ISUP_ANM_TX
- ISUP_ANM_RX
- ISUP_ARR_TX
- ISUP_ARR_RX

- ISUP_BLA_TX
- ISUP_BLA_RX
- ISUP_BLO_TX
- ISUP_BLO_RX
- ISUP_CCL_TX
- ISUP_CCL_RX
- ISUP_CCR_TX
- ISUP_CCR_RX
- ISUP_CFN_TX
- ISUP_CFN_RX
- ISUP_CGB_TX
- ISUP_CGB_RX
- ISUP_CGBA_TX
- ISUP_CGBA_RX
- ISUP_CGU_TX
- ISUP_CGU_RX
- ISUP_CGUA_TX
- ISUP_CGUA_RX
- ISUP_CON_TX
- ISUP_CON_RX
- ISUP_COT_TX
- ISUP_COT_RX
- ISUP_CPG_TX
- ISUP_CPG_RX
- ISUP_CQM_TX
- ISUP_CQM_RX
- ISUP_CQR_TX
- ISUP_CQR_RX
- ISUP_CRA_TX
- ISUP_CRA_RX
- ISUP_CRM_TX
- ISUP_CRM_RX
- ISUP_CRG_TX
- ISUP_CRG_RX
- ISUP_CVR_TX
- ISUP_CVR_RX
- ISUP_CVT_TX
- ISUP_CVT_RX

- ISUP_EXM_TX
- ISUP_EXM_RX
- ISUP_FAC_TX
- ISUP_FAC_RX
- ISUP_FAR_TX
- ISUP_FAR_RX
- ISUP_FOT_TX
- ISUP_FOT_RX
- ISUP_FRJ_TX
- ISUP_FRJ_RX
- ISUP_FWT_TX
- ISUP_FWT_RX
- ISUP_GRA_TX
- ISUP_GRA_RX
- ISUP_GRS_TX
- ISUP_GRS_RX
- ISUP_IAM_TX
- ISUP_IAM_RX
- ISUP_IDR_TX
- ISUP_IDR_RX
- ISUP_INF_TX
- ISUP_INF_RX
- ISUP_INR_TX
- ISUP_INR_RX
- ISUP_IRS_TX
- ISUP_IRS_RX
- ISUP_LPA_TX
- ISUP_LPA_RX
- ISUP_LPM_TX
- ISUP_LPM_RX
- ISUP_NRM_TX
- ISUP_NRM_RX
- ISUP_OPR_TX
- ISUP_OPR_RX
- ISUP_PAM_TX
- ISUP_PAM_RX
- ISUP_PRI_TX
- ISUP_PRI_RX

- ISUP_REL_TX
- ISUP_REL_RX
- ISUP_RES_TX
- ISUP_RES_RX
- ISUP_RLC_TX
- ISUP_RLC_RX
- ISUP_RSC_TX
- ISUP_RSC_RX
- ISUP_SAM_TX
- ISUP_SAM_RX
- ISUP_SGM_TX
- ISUP_SGM_RX
- ISUP_SUS_TX
- ISUP_SUS_RX
- ISUP_UBA_TX
- ISUP_UBA_RX
- ISUP_UBL_TX
- ISUP_UBL_RX
- ISUP_UCIC_TX
- ISUP_UCIC_RX
- ISUP_USR_TX
- ISUP_USR_RX
- ISUP_ABNORMAL_REL_TX
- ISUP_ABNORMAL_REL_RX
- ISUP_UNEXPECT_MSG_RX
- ISUP_UNRECOG_MSG_RX
- **Audit Counters new fields:**
 - AUDIT_FS_TOTAL_SIP_RESP_TMO
 - AUDIT_FS_TOTAL_SIP_NOACK_TMO
 - AUDIT_FS_TOTAL_CA_SWITCHOVER
- **SIP Interface Adapter Counters modified fields:**
 - SIA_OUTG_INIT
 - SIA_OUTG_SUCC
 - SIA_OUTG_FAIL
 - SIA_INCOM_INIT
 - SIA_INCOM_SUCC
 - SIA_INCOM_FAIL
 - SIA_TOTAL_SUCC

- SIA_TOTAL_FAIL
- SIA_TOTAL_OUTG_MSG_FAIL
- SIA_TOTAL_INCOM_MSG_FAIL
- SIA_REFRESHES_TX
- SIA_TOTAL_SESS_TIMER_FAIL
- SIA_CALL_FAIL_BY_EXPIRED_REG
- SIA_MWI_NOTIFY_TX
- SIA_MWI_NOTIFY_TX_FAIL
- SIA_MWI_NOTIFY_RX
- SIA_AUDIT_CCB_FREED
- SIA_AUDIT_CALL_RELEASED
- SIA_AUDIT_BCM_CALL_RELEASED
- SIA_AUDIT_REGCONTACT_FREED
- SIA_SECURE_FQDN_VIOLATION_REQ
- SIA_SECURE_FQDN_VIOLATION_RESP
- **Call Detail Block Counters new fields:**
 - BILLING_TOTAL_INTL_OPR
 - BILLING_TOTAL_NAT_OPR
 - BILLING_TOTAL_AIRLINES
 - BILLING_TOTAL_RAILWAYS
 - BILLING_TOTAL_SVC_CODE
 - BILLING_TOTAL_INTL_WZ1
 - BILLING_TOTAL_CNA
 - BILLING_TOTAL_DA_INTER
 - BILLING_TOTAL_DA_INTL
 - BILLING_TOTAL_UAN
 - BILLING_TOTAL_MOBILE
- **Trunk Group Usage Counters new fields:**
 - TRKGRP_EXCHANGE
 - TRKGRP_NAME
 - TRKGRP_GLARE_COUNT
 - TRKGRP_TOTAL_INS_TRK
 - TRKGRP_MAINT_TRK_USAGE
 - TRKGRP_OOS_TRK_USAGE
 - TRKGRP_UEQP_TRK_USAGE
 - TRKGRP_LBLK_TRK_USAGE
 - TRKGRP_RBLK_TRK_USAGE
- **Announcement Counters new fields:**

- ANM_EMG_CKT_UNAVAIL

The following counters modified existing fields:

- **Session Initiation Protocol Counters modified fields:**

- SIS_TOTAL_INCOM_MSG
- SIS_TOTAL_SUCC_INCOM_MSG
- SIS_TOTAL_OUTG_MSG_ATTMP
- SIS_TOTAL_SUCC_OUTG_MSG
- SIS_REQ_RETRAN_RX
- SIS_REQ_RETRAN_TX
- SIS_RSP_RETRAN_RX
- SIS_RSP_RETRAN_TX
- SIS_T1_TIMER_EXPIRED
- SIS_T2_TIMER_REACHED
- SIS_INVITE_RX
- SIS_INVITE_TX
- SIS_CANCEL_RX
- SIS_CANCEL_TX
- SIS_BYE_RX
- SIS_BYE_TX
- SIS_ACK_RX
- SIS_ACK_TX
- SIS_OPTIONS_RX
- SIS_OPTIONS_TX
- SIS_REGISTER_RX
- SIS_REGISTER_TX
- SIS_INFO_RX
- SIS_INFO_TX
- SIS_NOTIFY_RX
- SIS_NOTIFY_TX
- SIS_100_RX
- SIS_100_TX
- SIS_18x_RX
- SIS_18x_TX
- SIS_200_RX
- SIS_200_TX
- SIS_3xx_RX
- SIS_3xx_TX
- SIS_4xx_RX

- SIS_4xx_TX
- SIS_5xx_RX
- SIS_5xx_TX
- SIS_6xx_RX
- SIS_6xx_TX
- SIS_7xx_RX
- SIS_7xx_TX
- SIS_PROV_RSP_RETRAN_RX
- SIS_PROV_RSP_RETRAN_TX
- SIS_PRACK_RX
- SIS_PRACK_TX
- SIS_SUBSCRIBE_RX
- SIS_SUBSCRIBE_TX
- SIS_REFERER_RX
- SIS_REFERER_TX
- SIS_REFERER_W_REPLACES_RX
- SIS_INVITE_REPLACES_TX
- SIS_INVITE_REPLACES_RX
- SIS_REL100_RX
- SIS_REL100_TX
- SIS_UNSUPPORTED_RX
- SIS_UPDATE_RX
- SIS_UPDATE_TX
- **Audit Counters modified fields:**
 - TRUNK_STATE_SYNCED was changed to AUDIT_SS7_TRUNK_STATE_SYNCED
 - LONG_DUR_EXCEEDED was changed to AUDIT_SS7_LONG_DUR_EXCEEDED

New Documentation

New and Updated Documentation for Release 4.5.x

Release 4.5.x introduces a new set of user documentation specifically written for the Cisco BTS 10200 Softswitch Release 4.5.x software and hardware. To access the documents for Release 4.5.x, go to the following website:

http://www.cisco.com/en/US/products/hw/vcallcon/ps531/tsd_products_support_series_home.html.

When used in conjunction with the complete documentation set, these *Release Notes* provide a comprehensive guide to the Release 4.5.x features and operations.

All Cisco BTS 10200 Softswitch user documentation, including prior releases, can be accessed at the following location:

http://www.cisco.com/en/US/products/hw/vcallcon/ps531/tsd_products_support_series_home.html.

Previous 4.x Releases

The following information was implemented in prior 4.x Cisco BTS 10200 Softswitch releases. The features are not new to Release 4.5.

Release 4.4.1

Release 4.4.1 contains the following enhancements or new features.

Configurable ACM Timer Based On Incoming Trunk Group

Originating carriers allow providers a certain amount of time to find a destination for a call before the carrier does a route advance and attempts the call with another provider. In calls to some destinations, it takes longer than allocated to set up the call.

The configurable ACM timer based on incoming trunk group feature introduces the ability for the Cisco BTS 10200 Softswitch to generate an ANSI SS7 ISUP Address Complete Message (ACM) for calls that terminate to remote destinations that require longer times to identify and seize an outgoing trunk. A configurable timer starts as soon as the IAM is received and triggers the sending of an ACM back to the originating switch after the timer expires, if the Cisco BTS 10200 has not received an ALERT message from the terminating switch.

If there is interworking with continuity testing, the activation of this timer is postponed until the Continuity Test result message (COT) is received.

For more information about the ACM timer feature, including how to turn the ACM timer on or off, and setting the value for the ACM timer, refer to the *Configurable ACM Timer Based On Incoming Trunk Group* feature module.

Physical Interface 4/2

Previously, users could configure a 9/5 or 2/2 network configuration. Release 4.4.0 introduced the Physical Interface 4/2 configuration, which separates signaling traffic from management traffic on the Call-Agent/Feature Server and the EMS/BDMS hosts.

In Release 4.4.1, only the 4/2 physical interface is supported.

For more information, see the [“Physical Interface 4/2” section on page 88](#) section.

OCB Enhancements

Previously, Cisco BTS 10200 supported three levels of Outgoing Call Barring (OCB). The feature was enhanced to increase the levels and make the feature more flexible. The following enhancements were made to the feature:

- Cisco BTS 10200 now supports seven levels of OCB. The number of levels used vary from country to country and is operator configurable.
- OCB feature remains on a per subscriber basis.
- K value mapping to call-type is configurable on a POP basis and/or Office basis. If the POP basis is not configured, the system checks the Office basis. If no K mapping value number is provisioned, it defaults to the current hard-coded mapping of 3 K values. K value mapping does not need to be configured on a per subscriber basis.

- If OCB-Profile is assigned to the POP, but K value mapping to call-type is not defined in the OCB-K-Value table, then all calls are allowed.
- Users can skip defining K value mapping to call-type in the OCB-K-Value table.
- K values are independent of each other, and not cumulative.
- There are optional K-values defined to restrict all calls so that the operator does not have to enter multiple commands.
- A different announcement is played if the user activates OCB for the same value more than once.
- Users can select a 4 digit PIN number, used for authorization to activate or deactivate the OCB feature.
- If users forget their passwords, the operator (after proper authorization) can set the feature to default.

These enhancements are applicable to forwarded calls.

LNP Enhancement

In some implementations, Cisco BTS 10200 resides behind a switch that acts like a PSTN gateway. Cisco BTS 10200 handles incoming calls for numbers that are ported out by releasing the call with cause code 14 back to the switch.

The whole LNP implementation is required when direct interconnect is planned. However, sometimes a subscriber changes providers, but wants to keep his or her number. Calls to that number then go to the Cisco BTS 10200, which sends back the cause code 14.

In some countries, QoR and Concatenated addressing are the LNP methods used. When the call goes to the native provider, and if the subscribers are ported, then the originator switch receives the cause code 14. The originator switch then queries its database, which is synchronized to a central national database, and goes to the new service provider. The originator switch adds the two-digit provider and equipment codes to the beginning of the subscriber's number, and sets the NOA to 8.

ETSI v2 ISUP

The European Telecommunications Standards Institute (ETSI) v2 ISUP feature provides support for the ETSI v2 ISUP variant, based on the ETS 300 356 specification, on the Cisco BTS 10200.

The following requirements are supported:

- Basic Call Requirements
- Generic Signaling Procedure for Supplementary Services
- Supplementary Services Requirements

For more information, refer to the [ETSI v.2 ISUP](#) feature module.

Replaced Commands

The following two commands were replaced in Release 4.4.1:

- Status aor2sub was changed to **show aor2sub**.
- Control aor2sub was changed to **Change aor2sub**.

Non-Facilities Associated Signaling

Non-Facilities Associated Signaling (NFAS) is an ISDN feature for sharing one ISDN D channel across multiple ISDN PRI lines.

Starting with Release 4.4.1, Cisco BTS 10200 supports NFAS and the backup D-channel feature. This feature is based on the normal availability of two D-channels within one NFAS group, each residing on a separate interface. It allows the D-channel entity to assign calls to channels on more than one interface, including the one containing the D-channels. Out of the two D-channels, one is normally active to convey the layer 3 signaling and the other one is in standby mode. When the active D-channel fails, there is a switchover and the standby D-channel becomes active and resumes the transmission of the call control signaling previously handled by the failed D-channel. The backup D-channel is not being used for load sharing purposes. It can back up the same signaling functions provided by the active D-channel.

Cisco BTS 10200 supports a maximum of 32 T1s within one NFAS group. Both the D-channels within one NFAS group must be configured in the same gateway.

To configure NFAS, set the `nfas-supp` token to Y in the ISDN trunk group profile. Additionally, both the primary and backup D-channels must be provisioned within the same trunk group.

The following example shows an NFAS provisioning on the Cisco BTS 10200 side:

```

CLI> add isdn-tg-profile id=nfas; type=swv-us-ni2-pri; interface-type=network;
isdn-restart-chan-supp=n; isdn-restart-interface-supp=n; isdn-farend-init=n; nfas-supp=y;
bchan-neg-supp=y; isdn_restart_pri_supp=n; isdn-service-supp=n;
CLI>add trunk-grp id=1; call-agent-id=CA146; tg-type=isdn; glare=all; tg-profile-id=nfas;
dial-plan-id=dp1; mgcp_pkg_type=IT;
CLI>add isdn-intf tgn-id=1; intf=0;
CLI>add isdn-intf tgn-id=1; intf=1;
CLI>add isdn-intf tgn-id=1; intf=2;
CLI>add isdn-dchan tgn-id=1; set-id=dp-bh-set1; dchan-slot=0; dchan-port=1;
dchan-type=primary; dchan-intf=0;
CLI>add isdn-dchan tgn-id=1; set-id=dp-bh-set1; dchan-slot=0; dchan-port=2;
dchan-type=backup; dchan-intf=1;
  • CLI>add termination prefix=ds/s-0/ds1-0/; port-start=1; port-end=23; type=trunk;
mgw-id=bfg1;
CLI>add termination prefix=ds/s-0/ds1-1/; port-start=1; port-end=23; type=trunk;
mgw-id=bfg1;
CLI>add termination prefix=ds/s-0/ds1-2/; port-start=1; port-end=24; type=trunk;
mgw-id=bfg1;

CLI>add trunk cic-start=1; cic-end=23; tgn-id=1; mgw-id=bfg1;
termination-prefix=ds/s-0/ds1-0/; termination-port-start=1; termination-port-end=23;
intf=0;
CLI>add trunk cic-start=24; cic-end=46; tgn-id=1; mgw-id=bfg1;
termination-prefix=ds/s-0/ds1-1/; termination-port-start=1; termination-port-end=23;
intf=1;
CLI>add trunk cic-start=47; cic-end=70; tgn-id=1; mgw-id=bfg1;
termination-prefix=ds/s-0/ds1-2/; termination-port-start=1; termination-port-end=24;
intf=2;

```

Release 4.4.0

Release 4.4.0 contains the necessary functionalities to support both North American Cable and T1 accesses.

The following sections briefly describe the features, and how they enhance Release 4.4.0. For more detailed information on the features, including how to provision them, refer to the relevant feature modules or manuals, located on the [Cisco BTS 10200 Softswitch Release 4.4.x](#) documentation page.

NSCD Enabled on All Platforms

The Name Server Cache Daemon (NSCD) is a configurable high-performance caching service interposed between applications calling `gethostbyname()` and the actual synchronous query launched toward an external DNS server.

The Solaris 8 implementation of NSCD had a fatal flaw when used in a cable environment due to the excessive CPU consumption when flushing cached names accumulated over a short period of time.

The issue was reported to Sun and eventually led to Sun bug ID 4743876 being opened 10-Sep-2002. Ultimately the lack of a fix led to NSCD being removed from Cisco BTS 10200 Release 3.x.

However, the fix for this problem was released by Sun as patch ID 110710-02 dated 05-Mar-2004. As a result of this, the following changes were made to Release 3.5.5:

- A new parameter was added in `optical.cfg`, called `MARKET_TYPE`, with two valid values, T1 and CABLE.
- `NSCD_NAMED_ENABLED` was removed from `optical.cfg`.
- A new parameter was added, `NAMED_CONF`, to allow user flexibility to enable or disable the “named” caching server.
- If the user chooses `MARKET_TYPE=T1`, one set of `nscd.conf` is used, and if the user chooses `MARKET_TYPE=CABLE`, another set is used.

PacketCable Certified CMS, MGC

In Release 4.4.0, Cisco BTS 10200 is qualified in CW27 for both call management server (CMS) and media gateway controller (MGC) functionalities.

In a PacketCable-based network, the Cisco BTS 10200 Softswitch functions as both a CMS and an MGC. New feature is CW27. It provides call control, call routing, and signaling for several types of multimedia terminal adapters (MTAs and embedded MTAs [EMTAs]), cable modem termination systems (CMTSs), and trunking gateways (TGWs) in PacketCable-based networks. It provides interfaces to record keeping servers (RKSs) and key distribution centers (KDCs). The Cisco BTS 10200 Softswitch also communicates with announcement servers, SS7-based signaling gateways, MGCP-based media gateways (MGWs), and SIP networks.

For more information, refer to the [Cisco BTS 10200 Softswitch Release 4.4 PacketCable Feature Guide](#).

Simultaneous Support for CALEA Methods: PacketCable + SII

Cisco BTS 10200 Softswitch supports both the PacketCable CALEA and SII methods on the same platform so that IAD subscribers can be wire-tapped in addition to the wiretapping at the PacketCable subscriber. Note that a call can involve both IAD and EMTA, and both subscribers can be tapped.

Additionally, the Cisco BTS 10200 Softswitch supports the CMSS CALEA extensions (SIP headers) to indicate that a call is under surveillance when the call is redirected out/hand over to another softswitch.

But if the call is received by Cisco BTS 10200 Softswitch with these headers, the Cisco BTS 10200 Softswitch invokes CALEA tapping using the appropriate CALEA method associated for the terminating subscriber who is being tapped.

In Release 4.4 V05, the CALEA port number was changed to 14146 to make it consistent with Release 3.5.x. If using the SS8 DF, you can change the port by doing a modify-afri for the desired Cisco BTS 10200 and interface, and set the port to equal 14146.

If running a duplex Cisco BTS 10200, modify all interface IDs for the Cisco BTS 10200 by running the following commands from the SS8 command line:

```
modify-afri:afid=CALEA_BTS,ifid=1,port=14146;
modify-afri:afid=CALEA_BTS,ifid=2,port=14146;
```



Note

If you are not using an SS8 DF, consult the documentation for the DF model in use for the commands to change the RADIUS port.

SIP Features

SIP Trunk Audit

Release 4.4.0 adds audit capability to SIP Trunk Group. The audit mechanism verifies the operational status of a trunk, and is triggered when communication issues are detected on the trunk.

Changes were made to the following tables and fields:

- TRUNK_GRP Table:
 - STATUS-MONITORING field was added.
 - The DBM-only fields COMM-FAIL-COUNT, LAST-COMM-TIME, and AUDIT-STATE were added.
- SOFTSW_TG_PROFILE table: The AUDIT-THRESHOLD field was added.
- CA_CONFIG table: The TRUNK-AUDIT-INTERVAL entry was added.

Using SIP trunk audit triggers another Cisco BTS 10200 feature, route advance. Route advance was previously available for non-SIP trunks, but the SIP trunk audit feature enables route advance for SIP trunks as well.

For more information, refer to the [Cisco BTS 10200 Softswitch SIP Protocol Support Guides](#).

Configurable SIP Timer

In previous releases (3.5.x), the SIP stack request timeout logic was based on explicitly counting the number of retransmissions. In Release 4.4.0, which is based on RFC 3261, an overriding transaction timer is started for each request, which controls the number of retransmissions.

The inability to control retransmission counts ultimately results in a slower route advance if timely response is not received on a SIP trunk.

This feature was implemented to provide a faster route advance, resulting in faster call-setup under timeout conditions.

In Release 4.4.0, the following new command line arguments have been introduced to the SIP subsystem, to provide for decreases in request transaction timers, which control the number of retransmissions that occur before a timeout.

**Note**

When you are performing a software upgrade from Release 3.5.4 to Release 4.4.0, any alterations made to the default retry counts in Release 3.5.4 are not automatically propagated. Alterations must be propagated manually by computing appropriate Timer B and Timer F values during Release 4.4.0 installation. Default values (as specified in RFC 3261) for Timer B and Timer F prevail if none are specified.

The timer values can be configured during installation time in `optcall.cfg`.

- **-timerB** [Timer B in milliseconds]
 - Minimum: 1000 msec.
 - Maximum: 64000 msec.
 - Default: 32000 msec.

Timer B is an INVITE transaction timer as specified in RFC 3261. It controls, on a system wide basis, the number of INVITE retransmissions before a request timeout occurs.

- **-timerF** [Timer F in milliseconds]
 - Minimum: 1000 msec.
 - Maximum: 64000 msec.
 - Default: 32000 msec.

Timer F is a Non-INVITE transaction timer as specified in RFC3261. It controls, on a system wide basis, the number of retransmissions of all requests other than INVITE, before a timeout occurs.

**Note**

The enhancement will not be applicable to Release 4.5, because a separate enhancement, Configurable SIP timers, will be available in that release, allowing configuration of these timers (and therefore, the retry counts), on a per trunk basis through the CLI interface.

SIP Trunk Route Advance

You can use the previous features, SIP trunk audit and configurable SIP timers, to take advantage of the SIP trunk route advance feature.

Using SIP trunk audit triggers another Cisco BTS 10200 feature, route advance. When the Cisco BTS SIP interface sends out an initial INVITE message for a new call, and receives no response, the message is re-transmitted a number of times according to standard. Once the maximum number of retransmissions is sent, the call is released towards the originator with a SIP cause code of 408 Request Timeout or a Q.850 cause code of Recovery on timer expiry (102).

You can now specify a Route Advance action on this cause code using the Cause Code Mapping table. This allows the call to route to another destination trunk within the route set, if provisioned that way. In prior releases, you could not specify a Route Advance action for this situation.

To make the initial INVITE retransmission duration smaller, you can change the SIP protocol T1 timer as low as 200 ms. The default is 500 ms.

Cisco Self-Service Phone Administration

The new feature added to Cisco Self-service Phone Administration (SPA) is secured socket layer (SSL) support.

Cisco BTS 10200 supports secured CORBA for provisioning activity by activating the use of the SSL, such as XML/CORBA over SSL.

Secured CORBA over SSL is supported on SPA in communicating with Cisco BTS 10200, but is available in SPA 1.1 only.

For more information, refer to the [Cisco Self-Service Phone Administration](#) guide.

Range of Channels for TGCP Endpoints

In Cisco BTS 10200 Release 3.5.5, PacketCable TGCP now supports a range of channels specified in RSIP messages. In addition to the current naming conventions, local endpoint names for PSTN trunking gateway endpoints of type “ds” now adhere to the following:

- Wherever the “all” wildcard is permitted, the range of channels “[N-M]” wildcard can be used in the last term (i.e., <channel-#>) of the local endpoint name instead.
- The “range” wildcard then refers to all of the channels from N to M. The rules and restrictions that apply to using the “all” wildcard also apply to the use of the “range” wildcard.

Architecture Enhancements

The following architecture enhancements are available in Release 4.4.0.

Signaling Gateway Support

Signaling gateway support in Release 4.4.0 involves no embedded SS7 cards, and users can now disable sending ICMP ping messages to MGCP/NCS/TGCP media gateways.

Operational Enhancements

The following operational enhancements are available in Release 4.4.0.

Translation Verification Tool

Release 4.4.0 provides a Translation Verification Tool (TVT) via CLI command. The tool is used to find, diagnose, trace route, and translate call flow path decisions through the Cisco BTS 10200’s Call Agent processing. The TVT simulates a call from an originator to a specific destination based on dialed digits. The originator can be a line or a trunk. The translate function verifies that the translations for a given call are set up correctly. The behavior of the translate command is to show the name of each entry in each table used to evaluate the route determined based on the dialed digits. This tool does not actually set up a call; it only traverses through the tables to determine if the provisioning is correct.

For more information, refer to the [Query Verification Tool and Translation Verification Tool Features](#) document.

Query Verification Tool

Release 4.4.0 provides a Query Verification Tool (QVT) via CLI command that allows an operator to generate TCAP queries to an SCP database and verify the query results.

Queries generated using the QVT help in verifying a query sent to SCP, and the response received from the SCP. It is also possible to generate queries optionally with non-standard values by overriding the default value on any QVT command. Queries generated during actual calls depend on additional call-processing related provisioning and typically use standard parameter values.

For more information, refer to the [Query Verification Tool and Translation Verification Tool Features](#) document.

Suppress Sending of Internet Control Message Protocol Ping

Release 4.4.0 introduces a feature that provides the ability to block ICMP messages from the Call Agent to MGCP Gateway and from the Call Agent to the MGCP gateway (MGW). Previously, you could perform both an AuditEndpoint (AUEP) ping and ICMP ping together; there was no method to perform one without the other. Release 4.4.0 provides the ability to run an AUEP ping alone, and to disable the transmission of an ICMP ping.

For more information, refer to the [ICMP Message Blocking](#) feature module.

Support for Sun Netra 1280

Cisco BTS 10200 supports the SUN Netra 1280 (one processor card with 4 CPUs) as the processor engine for the Cisco BTS 10200 Softswitch Call Agent and EMS. The SUN Netra 20 is supported for the EMS, although the Call Agent is 1280-4cpus.

Security Enhancements

This section describes the Cisco BTS 10200 System Security Extensions available in Release 4.4.0.

HTTPs Support

Cisco BTS 10200 Release 4.4.0 uses secure HTTP (HTTPS) for the Web access to the EMS. The Web access is used to obtain system reports.

Key generation is done during installation. This also creates a self-signed certificate for use by those connecting to the server.

Administrative Login Authentication Using LDAP and RADIUS

Release 4.4.0 enables LDAP and RADIUS Authentication clients to validate user login to Cisco BTS 10200, which is a UNIX-based login mechanism. The functionality is applicable to EPOM and SPA.

For more information, refer to the [Cisco Self-Service Phone Administration](#) or [Cisco Extensible Provisioning and Operations Manager Getting Started](#) guides.

Login Authentication Using RSA Secure ID

Cisco has verified that with Release 4.4.0, you can deploy LDAP and RADIUS services on the Cisco BTS 10200 Softswitch. You can deploy an RSA RADIUS implementation without impacting the Cisco BTS 10200 Softswitch applications.

Hardened Solaris and SPA

In Release 4.4.0, the Cisco BTS 10200 runs on a “reduced” version of Solaris, referred to as “Hardened Solaris.” In this version, extra Solaris packages that create security risks, or are completely unnecessary for the operation of the Cisco BTS 10200, have been removed.

Separation of OAMP Traffic from Signaling

Cisco BTS 10200 allows a configuration that separates OAMP traffic from the signaling traffic to protect the call processing activity.

Secure CORBA

Release 4.4.0 features secure socket layer (SSL) support for CORBA. This includes the following sections:

- System Context for System Security Extensions
- Certificate and Key Password

The system provides a secure CORBA transport using an SSL module in the CORBA Adapter program CORBA interface servant (CIS). The Object Management Group (OMG) organization defines the Common Secure Interoperability Specification, Version 2 (CSIv2) that defines the Security Attribute Service (SAS) that enables interoperable authentication, delegation, and privileges.

For more information about the CORBA changes in Release 4.4.0, refer to the [Cisco BTS 10200 Softswitch Release 4.1 and 4.4 CORBA Adapter Interface Specification Programmers Guide](#).

Secured FTP Support for Billing Interface

Release 4.4.0 allows for using secured FTP (sFTP) in billing traffic, and has a new flag, `sftp-supp=n`. Before you can enable SFTP, the Cisco BTS 10200 and BMS must be configured to allow non-interactive SSH login as described below; however, once non-interactive SSH login has been setup, you must enable SFTP (thereby disabling FTP) by executing the CLI command `change billing-acct-addr sftp-supp=y`.

The BILLING 6 and Billing 33 alarms also changed in Release 4.4.0. The BILLING 6 (Failed to make ftp transfer) and BILLING 33 (Billing FTP Parameters Invalid) alarm definitions have been modified to read *Failed to make FTP/SFTP transfer* and *Billing FTP/SFTP parameters invalid*, respectively.

Also worth noting in Release 4.4.0 is that during initial set up, the security keys must be manually built in. To set up the public and private keys for the connection between the Cisco BTS 10200 Softswitch and a mediation device, complete the following steps.

For sFTP to work, manually configure Cisco BTS 10200 and BMS to allow non-interactive SSH login.

To perform SFTP as root or as BMS user ‘xyz’ refer to the [Release 4.4 Cisco BTS 10200 Softswitch Billing Interface Guide](#).

Billing Changes in Call Agent Profile Table

The Cisco BTS 10200 Softswitch can be provisioned to generate the following types of billing data:

- Call detail blocks (CDBs), which are assembled into call detail records (CDRs) by an external billing server.
- PacketCable-based event messages (EMs), which are transferred to an external RKS that assembles CDRs from the EMs. The applicable tokens in the CALL-AGENT-PROFILE table are CDB-BILLING-SUPP and EM-BILLING-SUPP. Cisco recommends that you set at most one of these to Y, and the other to N.

**Caution**

Cisco recommends that you do not set both CDB-BILLING-SUPP and EM-BILLING-SUPP to Y. Attempting to generate both types of records simultaneously can significantly degrade system performance.

**Note**

To set both tokens to Y, you must also include the new parameter, FORCED=Y, in the command line.

Two-Level Automatic Recall

Automatic Recall (AR) is an incoming call management feature that allows a customer to perform an activation procedure to automatically set a call to the last incoming number. The AR subscriber does not need to know the telephone number or the calling party of the last incoming call. If the party is busy when AR is activated, call setup is performed automatically when that party's phone becomes idle.

When AR activation is offered as a one-level procedure, the feature is activated after the customer successfully dials the proper access code. The Cisco BTS 10200 previously supported one-level AR activation; the new two-level AR Activation feature is an extension to the current AR feature.

The two-level automatic recall activation feature permits service providers to offer customers a choice of one- or two-level activation for the automatic recall feature. The level of activation option is set on either a system-wide basis, or on a POP-wide basis.

With the one-level AR activation procedure, customers do not know the last calling party number when activating the AR feature. With the two-level AR activation procedure, the customer hears the voice back announcement of the last incoming calling party number, the date and time the call was received, and a voice instruction for activating the AR call to that party.

For more information, refer to the "Automatic Recall" section of the [Cisco BTS 10200 Softswitch System Description](#).

TCAP Signal Adaptor Recovery from Signaling Link Failure

Starting with Release 4.4.0, the TCAP gateway subsystem monitors the signaling link interfaces for failures. This monitoring is done on both the active and standby side for both FSPTC and FSAIN. If both the signaling links go down, TSA brings down the platform.

Adjustable Timer for COS-Restrict Feature Confirmation Tone

In prior releases, a select few pieces of PBX equipment connecting to the Cisco BTS 10200 through an IAD device did not hear a confirmation tone when they made calls requiring an access code. This occurred because the PBX may not have cut the audio through to the PBX phone in time to hear the tone. The confirmation tone signal on the gateway delayed using the new CLI provisioning parameters provided in Cisco BTS 10200.

In Release 4.4.0, this enhancement to Cisco BTS 10200 allows configurable delays in the MGCP requests to play the prompt tone for account and authorization codes on the media gateway. The delayed request solution applies to trunk groups without main-subscriber or trunk groups with main-subscriber whose category is PBX. Using this feature the PBX users can hear a confirmation tone when they make calls requiring an access code. The delay information is provisionable via CLI using the following tokens in the CA-CONFIG table:

- ACCT-CODE-PROMPT-DELAY

- AUTH-CODE-PROMPT-DELAY

Refer to the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide* for more details on the tokens.

Physical Interface 4/2

Previously, users could configure a 9/5 or 2/2 network configuration. Release 4.4.0 introduces the Physical Interface 4/2 configuration, which separates signaling traffic from management traffic on the Call-Agent/Feature Server and the EMS/BDMS hosts. The feature also supports redundancy in signaling and management paths, and enhances management traffic security by separating it from signaling traffic.

The “4/2 Network Configuration” has two physical network interfaces on the EMS/BDMS hosts, and four physical network interfaces on the Call-Agent/Feature-Server hosts. Cisco recommends putting redundant interfaces on separate interface cards for added reliability.

In a 4/2 configuration, the signaling and management paths are on different physical interfaces. The internal traffic is routed through management interfaces, and the IRDP advertisement on the router is enabled only for signaling subnets to support signaling link fault management.

To separate management traffic from signaling traffic, the administrative access to the Cisco BTS 10200 system is controlled via the management network. Static routes are added for each network for administrative purposes via the management network, because outgoing administrative traffic from Cisco BTS 10200 should not be routed through the default route, or signaling network. There should be only one static route for such networks.

SSH Version 2

Release 4.4.0 has implemented SSH Version 2 as the default SSH version. Cisco BTS 10200 only supports SSH Version 2.

Systems such as CALEA may use SSH Version 1. For information on changing SSH back to Version 1, refer to the *Cisco BTS 10200 Softswitch Provisioning Guide*.

Distributed Message Transfer Part Level 3

Release 4.4.0 supports Distributed Message Transfer Part Level 3 (Distributed MTP3) by using the Cisco IP Transfer Point (ITP) group feature to provide hardware redundancy between the Cisco BTS 10200 and the SS7 Network.

An ITP-Group consists of two ITPs. In an ITP-Group (Distributed MTP3) configuration, each ITP acts as a physical Signaling Gateway Process (SGP). SGPs are connected together to form one logical Signaling Gateway (SG).

With the Distributed MTP3 feature, the Cisco BTS 10200 and both ITPs of a single ITP-Group share the same SS7 point code value.

In Release 4.4.0, each ITP-Group can only represent a single point code; if there are multiple OPCs on the BTS, this will require a separate ITP-Group for each BTS OPC. Also in this release, the ITP-Group feature is only available for the case where the ITP connects to the Service Provider SS7 Network via A links.

Basic Network Loop-Back Test for NCS/MGCP End-Points

The loop-back feature provides for a testing device to perform a network loop-back test on any MGCP/NCS subscriber endpoints controlled by the Cisco BTS 10200. With this release, the feature can test line side only.

The identification of Network loopback call is performed under the following condition:

- Configuration on originating line (Media Gateway profile). This can be performed by:
 - Configuring the media gateway for testing device as RGW (MGW-PROFILE::TYPE=RGW)
 - Associating the media gateway to MGW-PROFILE specific to network loopback test origination (MGW-PROFILE::SPARE2-SUPP=Y)
 - Configuring all test lines in the testing device as Subscriber terminations.

Feature testing and tested devices are assured to be configured on the same Call Agent. The loopback feature does not provide for performing network loopback test devices across a SIP or H.323 network.

Originating Point Codes

Previously, the Cisco BTS 10200 Softswitch configuration supported five Originating Point Codes (OPCs) with a maximum of 16 subsystem numbers. In Release 4.4.0, the medium configuration now supports eight OPCs and 32 Subsystem Records. This enables service-providers to use all eight OPCs to have all of four SSNs. Cisco BTS 10200 supports a total of five subsystems:

- Toll-Free-AIN
- Toll-Free-IN1
- CNAM
- LNP
- AC-AR

Out of the two Toll-Free subsystems, only one is needed for any OPC, so the maximum number of subsystems any OPC can have is four. Out of these, Toll-Free and LNP subsystems are supported from FSAIN platform, and the CNAM and AC-AR subsystems are supported from the FSPTC platform.

Each OPC has two subsystems (Toll-Free and LNP) on the FSAIN platform, and each OPC will have each subsystem (CNAM or AC-AR) on the FSPTC platform.



Note

Provisioning the Subsystems must be done carefully to avoid provisioning more than 16 Subsystems for FSPTC, and to avoid provisioning more than 16 subsystems for FSAIN platforms. In a correctly provisioned system, the number of subsystems for FSPTC or FSAIN platforms should not be more than 16, and the combined total not more than 32.

Also, you must provision Toll-Free, LNP, CNAM and AC-AR to a server. Take care when provisioning; toll-free and LNP must be provisioned to an AIN server, but CNAM and AC-AR must be provisioned to a POTS server. If you provision them otherwise, they will not work.

VXSM Gateway

The VXSM gateway was experiencing problems when the Cisco BTS 10200 sent MGCP messages for active calls and idle terminations (not involved in the call). This occurred when the VXSM gateway switched over and sent RSIP (rm:disconnected) for the entire gateway.

In Release 4.4.0, to isolate the call flow changes to VXSM, a special configuration field, MGCP-SPARE1-SUPP in MGW-PROFILE, is used.

The flag should be used for high density gateways, such as VXSM (the MGCP-SPARE1-SUPP field in MGW-PROFILE should be set to Y for VXSM gateways).

The only special behavior for VXSM currently known is what the Cisco BTS 10200 does when receiving RSIP rm:disconnected (which happens when VXSM stateful fails over).

- If the endpoint is IDLE (in Cisco BTS 10200 resource state), Cisco BTS 10200 sends DeleteConnection to the endpoint (same as other gateways).
- If the endpoint is ACTIVE (in Cisco BTS 10200 resource state), and if MGCP-SPARE1-SUPP= Y in MGW-PROFILE, Cisco BTS 10200 sends a ModifyConnection message to all connections (one after another without waiting for ACK) that exist in the Cisco BTS 10200 connection memory for the affected endpoint, and includes information CallIdentifier and ConnectionIdentifier stored in Cisco BTS 10200 connection memory. If the MGW returns the error code “Invalid connection”, the wild-carded DeleteConnection is sent to that endpoint, failing the call in Cisco BTS 10200.

Flash Archive and Disk Mirroring

Flash archive does not work well with Disk Suite mirroring; therefore, Cisco recommends that users create the archive without disk mirroring.

Exchange Code Table

Release 4.4.0 adds new functionality that validates the minimum and maximum DN length restrictions based on the Exchange Code table. The default value of min_dn_length and max_dn_length is set to 10.

If the length of DNs you are using is different from 10, then you must correct the max_dn_length and min_dn_length in the exchange-code table.

During upgrade, the values from the previous release are carried over to Release 4.4.0. So, after upgrading, you must change the max-dn-length and min-dn-length to reflect the correct length of DNs. Otherwise, you cannot add any new numbers shorter or longer than 10 digits.

Feature Profile Base and FEATURE-CONFIG Tables

Both the Feature Profile Base table and the FEATURE-CONFIG table are visible in Release 4.4. However, while available, the tables are not supported until Release 4.5.

Command Line Interface Guidelines

The “show measurement-prov type=all” is not supported for measurement provisioning. To get all the measurement provisioning details at the CLI interface, you must execute the command “show measurement-prov.” The “type=all” is not a valid key for the command “show measurement-prov.”

This applies for Release 4.4.x and releases going forward.

User Side State Machine Enabled

Cisco BTS 10200 has implemented ISDN user side state machine. The ISDN PRI User-Side interface on the Cisco BTS 10200 is used by setting the interface_type field in ISDN-TG-PROFILE table to USER-SIDE.

RSC Coordination Behavior

In Release 4.4, a special configuration field SPARE1-SUPP in MGW-PROFILE isolates call flow changes to VXSM.

After receiving RSIP rm:disconnected (when VXSM stateful fails over), Cisco BTS 10200 acts accordingly:

- If the endpoint is IDLE, Cisco BTS 10200 sends DeleteConnection to the endpoint.
- If the endpoint is ACTIVE and if MGCP-SPARE1-SUPP=1 in MGW-PROFILE, Cisco BTS 10200 sends a ModifyConnection message to all connections that exist in the Cisco BTS 10200 connection memory for the affected endpoint, including CallIdentifier and ConnectionIdentifier information stored in the Cisco BTS 10200 connection memory. If the media gateway returns the error code “Invalid connection,” Cisco BTS 10200 sends a wild-carded DeleteConnection to that endpoint and fails the call in Cisco BTS 10200.

Increased ISDN Trunk Groups

Previously, Cisco BTS 10200 had a limit of 1100 maximum D channels to support for a medium configuration. This enhancement allows Cisco BTS 10200 to now support 1500 ISDN trunk groups (and D-channels) in a “medium” memory configuration.

9 Bits Used for ISDN D Channel Port

Previously, the BSM and CLI implementation had the ISDN D channel slot represented by 8 bits, and the D channel port also represented by 8 bits, for a total of 16 bits. The requirement to interface with BFG set the slot to 0 when the port was greater than 255 (8 bits).

The enhancement is to now use 15 bits for the D channel port instead of 8 bits. The range restriction of ISDN-DCHAN table in the CLI was also changed from 255 to 32768 for the D channel port.

Release 4.2

The Cisco BTS 10200 Softswitch contains the following new features in Release 4.2:

- [H.323 Video, Routing, and Transparency Features](#)
- [New Call Detail Record Field](#)
- [SIP-T](#)
- [Calling Party Number Options for Outgoing SETUP Message](#)

H.323 Video, Routing, and Transparency Features

This section describes the H.323 video, routing, and transparency feature enhancements for Release 4.2 of the Cisco BTS 10200 Softswitch. It also describes the tasks and commands for provisioning and using these capabilities. The following enhancements are provided in this release:

- Support for video capability on H.323-based subscriber phones
- Support for video on H.323-based trunk groups
- H.323 routing enhancements for inbound and outbound call legs
- ANI-based screening and routing enhancements
- Additional H.323 and video-related billing records
- Enhanced interoperability with other endpoints, including Cisco CallManager, using H.323 protocol interface
- Improved message tunneling and protocol transparency for H.323-based transit traffic
- Additional H.323-related feature enhancements

These enhancements can be applied to managed H.323 networks that contain the Cisco BTS 10200 Softswitch and the following network element types:

- H.323-based IP PBX systems, including Cisco CallManager
- Analog phones connected to customer premises equipment (CPE) such as integrated access devices (IADs)
- H.323 primary rate interface (PRI) gateways (GWs)
- H.323 IP-to-IP GWs
- H.323-based gatekeepers (GKs)
- H.323-based video phones
- H.323-based audio phones

For information on how to provision and use these capabilities, refer to the [Cisco BTS 10200 Softswitch H.323 Video, Routing, and Transparency Features for Release 4.2](#) document.

New Call Detail Record Field

An Original Originating number was added to the Call Detail Records (CDR).

SIP-T

Changes were made to the SIP trunk PRACK flag in Release 4.2. Provisional responses in SIP telephony calls represent backward alerting and progress signaling messages, which are important when you are interoperating with PSTN networks. Therefore, for SIP-T calls on the Cisco BTS 10200, reliable provisional responses are mandatory. They are optional for regular SIP calls.

For more information about the change, refer to the Reliable Provisional Responses sections of the *Cisco BTS 10200 Softswitch SIP Protocol User Guide* and the *Cisco BTS 10200 Softswitch SIP Protocol Provisioning Guide*.

Calling Party Number Options for Outgoing SETUP Message

This feature allows the service provider to control the calling party number (CPN) data sent in the outbound SETUP message on redirected calls outbound from the Cisco BTS 10200 Softswitch to the PSTN. You can provision this option (via CLI command) using the SEND-RDN-AS-CPN token in the TRUNK-GRP table.

For more information about this feature, refer to the [Calling Party Number Options for Outgoing SETUP Message](#) feature module.

Enhancements for Release 4.2

The following enhancements were made to Cisco BTS 10200 Softswitch Release 4.2.

PacketCable

The PacketCable-based function was enhanced in Cisco BTS 10200 Release 4.2—a new rule was added regarding source and destination identifiers in the IPSEC-POLICY table.



Note

For detailed information on compliance with specific paragraphs of the Internet Engineering Task Force (IETF) standards (for TGCP, IP Security, NCS, and so forth), please contact your Cisco account team.

New Field for Signaling 68 Event/Trap

In previous Cisco BTS 10200 releases, if a media gateway was down, a signaling 68 event was generated. The event contained the gateway description and the TSAP-ADDR. However, it did not contain information about the media gateway location, or the media gateway subscribers.

In Release 4.2, a new field was added to the SNMP Trap Signaling 68 event/trap. The new field contains subscriber information (ID, DN1, ADDRESS1).

CODEC Negotiation

Release 4.2 contains an enhancement for the interworking function to use the standardized/Cisco-supported SDP format for the G723ar53/63 CODEC.

Previously, calls might be blocked if G723ar56/63 was the only CODEC specified. For example, if the CODEC on a SIP gateway was set to G723ar53, and a call was made to an H.323 gateway, the Cisco BTS 10200 might block the call.

T.38 CA Mode Fax

In Release 4.2, Cisco BTS 10200 supports Call Agent controlled T.38 Fax for trunks or lines controlled using the MGCP protocol 'fxr' package. Cisco BTS 10200 supports T.38 call agent controlled mode fax between SS7 trunk, ISDN trunk and Subscriber lines. In Release 4.2, the mode also can be used for either of the following fax scenarios:

- Faxes transmitted between a Cisco IOS MGCP-based MGW and an H.323 GW
- Faxes transmitted between two MGCP-based MGWs

To enable this mode, be sure to configure the following:

1. In the QOS table for Subscriber/trunk-grp:

```
FAX_PREF_MODE=FAX_T38_CAMODE
```

2. In the MGW-PROFILE table for TGW/RGW:

```
MGCP_T38_CAMODE_SUPP=Y
```

3. Enable the T.38 fxr package in MGW (if using Cisco IAD, only specific releases support this).

Hook-Flash with Warmline and Hotline-Variable Feature

In Release 4.2, a subscriber on a warmline call can originate a multi-party call, as well as activate or deactivate certain features by hook-flashing and dialing either a DN or a star code. The system does not block such calls.

For Hotline, Warmline, and Hotline-Variable (HOTV) in Release 4.1.x and prior:

- Users cannot initiate a 3-party call.
- Users cannot invoke VSC features.

For Release 4.1.1 and forward, the above two limitations do not apply. Users can initiate a second call while on a Hotline, Warmline or HOTV by pressing hook-flash. The second call leg initiated after a hook-flash behaves like a basic call line (and not like a Hotline, Warmline or HOTV call respectively). Only the HOTV feature is allowed to invoke VSC features (HOTVA, HOTVD and HOTVI), and is limited to its initial call leg.

Capability for NAS Digital Calls

In previous releases, Cisco BTS 10200 only supported NAS for modem calls. Release 4.2 now allows NAS calls coming in with various BearerCapability settings. The NAS mode (modem or digital) is set according to BearerCapability.

Release 4.1

With Release 4.1, Cisco BTS 10200 Softswitch introduces new features to enhance its capabilities. This section describes the new features available in Release 4.1, which include the following:

- [Reduced Physical Interfaces, page 96](#)

This feature reduces the number of network interfaces on the Cisco BTS 10200 Call Agent/Feature Server and the EMS/BDMS hosts to two network interfaces per host computer.
- [Signaling Capabilities, page 96](#)

The Cisco BTS 10200 Softswitch Release 4.1 provides SIGTRAN SS7 signaling, which allows quick turn-around on the development of new International SS7 variants, such as China ISUP, as well as SS7 support domestically.
- [OpenORB Support, page 98](#)

OpenORB was added as the CORBA interface in an earlier release. Starting with Release 4.1, OpenORB replaces Inprise Visibroker as the CORBA interface for the Cisco BTS 10200.
- [Billing Subsystem Redesign, page 99](#)

The Cisco BTS 10200 Softswitch Release 4.1 can generate either traditional Call Data Block (CDB) or PacketCable Event Message (EM) billing data, but not both simultaneously.
- [PacketCable-Based Features, page 99](#)

New PacketCable-based features and functions have been introduced in the Cisco BTS 10200 Release 4.1 software.
- [H.323 Annex E Redundancy, page 100](#)

The UDP-based Annex E feature of ITU-T Recommendation H.323 is now supported by the Cisco BTS 10200 Softswitch Release 4.1.
- [IP Manager, page 101](#)

IPManager is a UNIX shell script that manages a set of logical interfaces to provide another layer of redundancy.
- [SS7 CIC Audits, page 101](#)

The CIC audit feature enables the Cisco BTS 10200 Softswitch to recognize when an SS7 trunk is in the hung state and to restore the trunk to a usable state.
- [Process Restartability, page 101](#)

Cisco BTS 10200 Softswitch processes might exit due to an internal error or termination by the platform. This new feature enables restart of the processes that shut down, preserving stable calls.
- [SIP Trunks, page 102](#)

Release 4.1 introduces Session Initiation Protocol (SIP) device support, and the changed trunk support.
- [OAMP Enhancements, page 102](#)

Several new commands are supported in Release 4.1.
- [Modified and New Subscriber Features](#)

Information for service providers regarding the modified and new subscriber features.

Reduced Physical Interfaces

The Reduced Physical Interfaces feature reduces the number of network interfaces on the Call Agent/Feature Server and the EMS/BDMS hosts to two network interfaces per host computer. The reduction allows the Cisco BTS 10200 to run on smaller, or less expensive, host computers, since the number of required Ethernet ports is reduced. In addition, it creates redundant local area networks (LANs) for the management of the Cisco BTS 10200 Softswitch.

Signaling Capabilities

Currently, routing on Cisco gateways is based on generic parameters such as originating number, destination number, and port source. Adding support for SS7 ISUP messages allows the VoIP network to use additional routing enhancements found in traditional TDM switches.

Cisco BTS 10200 Release 4.1 implements SIGTRAN-based SS7 signaling and includes the following embedded SS7 ISUP variants:

- SS7 ANSI ISUP
- SS7 ITU ISUP
- SS7 China ISUP
- SS7 Mexico ISUP

SIGTRAN-Based SS7 ANSI Signaling

Release 4.1 introduces SIGTRAN-based ANSI support in the SS7 ANSI implementation.

The Cisco BTS 10200 Softswitch SS7 ANSI ISUP feature implements North America ISUP through a signaling transportation (SIGTRAN)-based ANSI signaling gateway, providing the ability to port SIGTRAN (SCTP/M3UA) and the upper SS7 layers (ISUP, TCAP, AIN) to an IP network.

For more information, see the [Cisco BTS 10200 Softswitch SS7 ANSI Implementation Feature Module](#) and the [Cisco BTS 10200 Softswitch SS7 ANSI ISUP Implementation Feature Module](#).

SS7 ANSI ISUP also implements new traffic statistical measurements for these signaling protocols:

- M3UA
- ISUP
- SCTP
- TCAP

Refer to the [Cisco BTS 10200 Softswitch Release 4.1 Operations and Maintenance Guide](#) for more information about all existing Cisco BTS 10200 Softswitch traffic measurements.

SS7 ITU ISUP

Cisco BTS 10200 Release 4.1 supports ITU-based SS7 ISUP messages based on Q.761 and Q.767. Specific country variants supported include China and Mexico.

China SS7 ISUP

The International Telecommunications Union (ITU) Signaling System 7 (SS7) Integrated Services Digital Network (ISDN) User Part (ISUP) feature implements China ISUP via SIGTRAN to a SIGTRAN-based Signaling Gateway. The Cisco BTS 10200 Softswitch is coupled to the SS7 signaling network via an external SIGTRAN signaling gateway, one of three models of Cisco IP Termination (IPT) devices. The Cisco IPT provides an interconnection to many ISUP and MTP signaling variants.



Note

For the complete list of available ISUP variants, contact Cisco BTS 10200 product management.

The China SS7 ISUP feature allows a Cisco BTS 10200 to connect between an international SS7 network and a local voice network, supporting basic calls, caller identity, call redirection, and voice mail. The same call control and supplementary services provided over an ANSI SS7 network can also be provided over an ITU SS7 network.

China SS7 ISUP also offers support for the following features:

- China and ITU ISUP Conformance
- ITU Channel Management and Circuit Selection
- China ISUP to MGCP/H323/SIP Interworking
- China ISUP to Voice Mail (IP Unity)
- China Supplementary Services via Centrex
- Subscriber Features

The Traffic Management Subsystem provides the following functions:

- Collects statistics
- Clears counters
- Saves 48 hours of statistical data in persistent store
- Displays summary reports
- Provides on-demand report queries
- Issues events as appropriate

For more information, refer to the [Cisco BTS 10200 Softswitch China ITU SS7 Support Feature Module](#).

[Table 7](#) identifies the new ISUP traffic measurements collected for China ISUP support.

Table 7 *China ISUP Measurements*

Measurement	Description
OPRs Transmitted	Count every OPR sent
OPRs Received	Count every OPR received
MPMs Transmitted	Count every MPM sent
MPMs Received	Count every MPM received
CCLs Transmitted	Count every CCL sent
CCLs Received	Count every CCL received

For detailed information about Cisco BTS 10200 Softswitch traffic measurements provisioning and reporting, refer to the [Cisco BTS 10200 Softswitch Release 4.1 Operations and Maintenance Guide](#).

Mexico SS7 ISUP Support

Cisco BTS 10200 Softswitch Release 4.1 introduces the base Q.767 MDL code and the Mexico ISUP variant, based on the ITU-T Q.767 specification, *Application of the ISUP for International ISDN Connections*. The Mexico ISUP variant support is similar to the China SS7 ISUP variant support.

OpenORB Support

In Release 3.5.2, OpenORB was added as an option for the CORBA interface. Starting with this release, and going forward, OpenORB now replaces Inprise Visibroker as the CORBA interface. Inprise Visibroker is no longer supported for Release 4.1 or later.

OpenORB is an open source software, and supports the latest CORBA specifications (OMG CORBA 2.4.2). During installation, you can now select only OpenORB.

Installation



Note

EPOM 2.1 was designed to work with OpenORB. If running previous EPOM releases such as EPOM 1.3, upgrade to EPOM 2.1 and use OpenORB.

The procedure used to install the OpenORB package is virtually unchanged from the Visibroker install package. The old CORBA Interface Servant (CIS) is removed with a package remove command in Solaris, and the “cis-install.sh” command is invoked. Once the installation is complete, all components are installed and the Name Service and CIS application are running. You can perform the process on the active EMS without switching over.

For more information on OpenORB, visit <http://openorb.sourceforge.net/>.

Cisco OSS Applications

The switch to OpenORB by the Cisco BTS 10200 does affect existing Cisco OSS applications that utilize the CORBA interface.



Note

Cisco OSS/NMS applications include EPOM and PTC. Partner applications include CEON IPS and all partner applications which have specific adapters for the particular ORB.

The bulk of OSS application processing involves this interface and this component of the client application should be totally unaffected. Existing customers are affected in that the client side or OSS application must use a fully compliant ORB that can interoperate with an ORB using CORBA 2.4.2 via IIOP. The original Visibroker POA was specific to the vendors’ implementation of the POA.

The IDL and XML interfaces are not affected by the OpenORB migration.

Name Service Feature

You must navigate to the Cisco BTS 10200 EMS by using the Name Service feature in CORBA. At this time, each Cisco BTS 10200 creates a Name Service instance and binds the Cisco BTS 10200 objects to this local name service. Obtaining these object references for the Cisco BTS 10200 requires communication with its local Name Service.

Billing Subsystem Redesign

The billing subsystem has been redesigned in Release 4.1. Enhancements were made to Call Detail File Management, and to the CLI commands for managing the files stored on the BDMS platform at any given time. Examples of the commands include:

- **report billing-file filename=%;**—Displays all file names stored in /opt/bms/ftp/billing.
- **report billing-file filename=xxx;**—Displays the specified filename and the current state of the file.
- **report billing-file state=xxx;**—Displays all filenames that are in the specified state.

The following is a list of the command line tokens associated with this command and the valid values and purpose of each:

- **filename**—Name of the billing file
- **state**—The current state of a given file. Valid values are:
 - OPEN**—The file is currently being written to
 - PRIMARY**—The file has been sent to, and acknowledged by, the billing mediation system.
 - SECONDARY**—The file has been sent to, and acknowledged by, the billing mediation system
- **start-row**—The row to start displaying from in the returned result set. Range is determined by the size of the result set. (Default = 1).
- **limit**—The maximum number of rows to display from the result set. (Default = 50.)
- **display**—The data columns to display from those supported by this command. The default is to display all available columns.
- **order**—The column by which to sort the displayed result set. Valid values are:
 - FILENAME**—Sort by filename.
 - STATE**—Sort by state.
- **auto-refresh**—Specifies if a new result set is to be created or to use the existing one if there is one available. The default value is Y.

Billing Data Generation

The Cisco BTS 10200 Softswitch Release 4.1 has the ability to provision billing support using one of the following billing data generation methods:

- **Call Detail Blocks (CDBs)**—This is traditional post-call billing data, which is assembled into Call Detail Records (CDRs) by an external billing mediation system or billing server.
- **PacketCable event messages (EMs)**—This is real-time call data flow, which is transferred to an external Record Keeping Server (RKS) that assembles CDRs from the EMs.

The Cisco BTS 10200 can be provisioned to generate either EMs or CDBs. For the detailed procedures for provisioning EM or CDB generation of billing data, see the [Packet Cable Feature Module](#).

PacketCable-Based Features

The following PacketCable-based features and functions have been introduced in the Cisco BTS 10200 Release 4.1 software.

- PacketCable-based signaling security features, including implementation of IP security architecture (IPSEC), key management using Internet Key Exchange (IKE), and Kerberos

- PacketCable-based media security
- Common Open Policy Service (COPS) interface measurements
- DQoS gate coordination function
- TGCP support

In addition, the following PacketCable-based features have been updated:

- Alarms and events
- Command line interface (CLI) provisioning


Note

CLI provisioning is disabled by default at Release 4.1 installation. CLI provisioning is not allowed until database licenses are applied to the Cisco BTS 10200.

H.323 Annex E Redundancy

The UDP-based Annex E feature of ITU-T Recommendation H.323 is supported by the Cisco BTS 10200. The Cisco BTS 10200 is a class-independent network switch. In addition to performing switching functions, it can also emulate up to four instances of an H.323 gateway (GW).

Annex E implementation allows for transporting H.323 signaling between the Cisco BTS 10200 and the far-end H.323 end point using UDP (connectionless) signaling instead of TCP (connection-oriented) signaling. The choice of UDP or TCP signaling is important in a Cisco BTS 10200 CA failover scenario.

If a CA failover occurs, a remote H.323 end point using TCP signaling cannot reestablish the connection with the previously-active CA, therefore clearing the stable call(s) on that connection. However, a remote H.323 end point using UDP to communicate with the Cisco BTS 10200 in a connectionless session continues to communicate with the newly-active side of the CA using the same connectionless session. This allows the remote end point to preserve and support the active call.

Using the Annex E feature is optional and configurable in the Cisco BTS 10200. Each H.323 trunk group (TG) in the Cisco BTS 10200 can be independently provisioned to support either Annex E UDP-based signaling or TCP-based signaling. Each H.323 GW instance can have multiple active outgoing TGs, with each TG independently configured for Annex E UDP or regular TCP signaling.

For more information, refer to the [Cisco BTS 10200 Softswitch Annex E Support Feature Module](#) or the “[H.323 Annex E UDP Support](#)” section of Chapter 2, “[Supported Signaling Protocols](#),” in the [Cisco BTS 10200 Softswitch Release 4.1 System Description](#).

Call Manager/H.323 Interworking

Release 4.1 enhances H.323 protocol interoperability between the Cisco BTS 10200 Softswitch, Cisco CallManager (CCM), and Cisco IOS H.323 Gateways. Interoperability of these network elements enhances the delivery of call control features between enterprise and service provider networks.

For more information, refer to the “[Interoperability of Cisco BTS 10200 Softswitch with Cisco CallManager](#)” section of Chapter 2 and “[Supported Signaling Protocols](#),” in the [Cisco BTS 10200 Softswitch Release 4.1 System Description](#).

IP Manager

The Cisco IP manager provides a virtual single IP address to different signaling protocol components (such as MGCP, H.323, SIP) for remote devices in the Primary and Secondary Cisco BTS 10200 Softswitch boxes. The IP Manager is responsible for detecting Cisco BTS 10200 Softswitch platform failover (from Primary to secondary and viceversa) and migrating the IP address to the Current Active side.

In this release, the IP manager is an integral part of each platform (such as Call Agent and Feature Server), and thereby provides faster response to platform failovers. Note that the IP Manager only migrates IP addresses on the same subnet. In the case of a multi-homed platform, when one of the interfaces fails, the IP Manager does not migrate the IP address to a different interface. The IP Manager also now uses logical IP addresses for Call Agent-to-Feature Server communications.

SS7 CIC Audits

The Cisco BTS 10200 Softswitch system may experience a “hung” SS7 trunk when an idle trunk is incorrectly perceived by the Call Agent to be busy. When this occurs, the Call Agent never selects the trunk to service new calls. This condition occurs primarily during a failover when the standby system becomes active. A call is released and the new idle call state is not replicated to the newly active Call Agent, who continues to perceive the trunk as busy.

The CIC audit feature enables the Cisco BTS 10200 Softswitch to recognize when an SS7 trunk is in the hung state and to restore the trunk to a usable state. A CIC audit can be performed in response to a:

- Demand request
- Switchover
- Scheduled audit request
- Long duration call
- Exception event

The CIC audit feature implements the following new audit types for the active call agent:

- Switchover audit
- SS7 audit
- MGCP audit
- Demand audit
- Exception audit
- Long-duration audit

Process Restartability

When a Cisco BTS 10200 Softswitch process exits due to an internal error (such as SIGSEGV on Unix) or is terminated by the platform, the platform restarts the processes that is exited, thereby preserving stable calls. Restarting the process is a preferred alternative to switching over to the mate.

When a process is restarted, the process audits information such as resource states, and attempts to repair inconsistencies. In contrast to a switchover, process restarts preserve transient calls that are not affected by that process.

In the Cisco BTS 10200 Softswitch, the restartability of a process is indicated by the Maximum Restart Rate field in the platform.cfg configuration file. A zero value indicates that the process is non-restartable, and a positive value indicates that the process is restartable.

SIP Trunks

Support for SIP trunks existed in previous releases of the Cisco BTS 10200 Softswitch, but support for SIP endpoints is new to Release 4.1.

The SIP support feature provided in Release 4.1 was built on the existing Cisco BTS 10200 Softswitch software and hardware platform. The Cisco BTS 10200 Softswitch uses SIP and SIP for telephones (SIP-T) signaling to communicate with other SIP-based network elements. The implementation is based upon the evolving industry standards for SIP, including IETF document RFC 3261, SIP: Session Initiation Protocol. The Cisco BTS 10200 Softswitch supports both SIP trunks and SIP-based subscriber lines (SIP endpoints), and provides the following SIP-related functions:

- Protocol conversion between SIP and several other protocols, including SS7, PRI, ISDN, H.323, MGCP, and CAS.
- Tandem back-to-back user agent for direct SIP-to-SIP calls (trunk to trunk, phone to phone, and trunk to/from phone), and SIP-to-SIP-T calls.
- SS7 bridging between Softswitches using SIP-T methods.

Release 4.1 supports SIP endpoints such as software-based phones or SIP IP phones, including authentication and registration management. (For example, the Cisco BTS 10200 Softswitch maintains the current location of SIP subscribers.)

To see the supported SIP endpoints, refer to the SIP Endpoints field in [Table 5](#). For feature details and applicable procedures, see the [Cisco BTS 10200 Softswitch SIP Protocol Guide](#) and the [Cisco BTS 10200 Softswitch SIP Protocol Provisioning Guide](#).

OAMP Enhancements

Several new commands are supported in Release 4.1, including:

- **SNMP Trap Transmission**—The retransmission of traps via SNMP is similar to “controlling” a node ins/oos/equip/etc via SNMP SETs. That is, the trap retransmission table contains the following columns: start time, end time, start sequence number, end sequence number, NMS address, and commit.
- **Morning Report**—Morning reports are stored in a table for 30 days (4 weeks) and can be accessed by the following command:

```
report system_health [start-day=[MM-DD-YYYY]]; [end-day=[MM-DD-YYYY]];
```
- **DB Connection Status and Control**—These commands display the current status and allow control over the DB connection used in Oracle.
- **User login discriminator**—The existing user commands will have new parameters added to them to allow the operator to modify the login control mechanism.

Modified and New Subscriber Features

Release 4.1 incorporates all the features of both Release 3.2 (international features) and Release 3.5 (North America features). In addition, Release 4.1 changed the feature activation experience for the user—providing activation/deactivation/interrogation announcements (instead of success/failure tones) in most cases.

Service providers must provision the new feature-specific announcements to make them available for playback to the end user. This provisioning is covered in [Chapter 10](#) and [Appendix A](#) of the *Cisco BTS 10200 Softswitch Provisioning Guide*. If the service provider does not provision an announcement, and the feature calls it, the user hears a reorder tone.

New Documentation for Release 4.4

Release 4.4 introduces a new set of user documents specifically written for the Cisco BTS 10200 Softswitch Release 4.4 software and hardware. When used in conjunction with the following manuals, these *Release Notes* provide a comprehensive guide to the Release 4.4 features and operations:

- [Cisco BTS 10200 Softswitch Release 4.4 System Description](#)
- [Cisco BTS 10200 Softswitch Release 4.4 Provisioning Guide](#)
- [Cisco BTS 10200 Softswitch Release 4.4 Operations and Maintenance Guide](#)
- [Cisco BTS 10200 Softswitch Release 4.4 Command Line Interface Reference Guide](#)

These Cisco BTS 10200 documents were also modified to reflect the new information for Release 4.4:

- [Release Notes \(Release 4.4.x\)](#)
- [Installation Documentation \(Release 4.4.x\)](#)
 - [Cabling Procedures \(Release 4.4.x\)](#)
 - [Site Surveys \(Release 4.4.x\)](#)
 - [Application Installation Procedure \(Release 4.4\)](#)
 - [CD Jumpstart Procedure \(Release 4.4\)](#)
- [Upgrade Guides \(Release 4.4.x\)](#)
- [Billing Guide \(Release 4.4.x\)](#)
- [System Security \(Release 4.1\)](#)
- [SIP Protocol Support Guides \(Release 4.4.x\)](#)
- [PacketCable Feature Guide \(Release 4.4.x\)](#)
- [ISDN Provisioning and Troubleshooting \(Release 4.1\)](#)
- [ICMP Message Blocking Feature Module](#)
- [Query Verification Tool and Translation Verification Tool Features](#)
- [CORBA Programmer's Specification \(Release 4.4\)](#)
- [Cisco Self-Service Phone Administration](#)



Note

All Cisco BTS 10200 Softswitch user documentation can be accessed through the following location:
http://www.cisco.com/en/US/products/hw/vcallcon/ps531/tsd_products_support_series_home.html.

Cisco BTS 10200 Softswitch Release 4.4 user documentation is password protected. Consult your Cisco representative for access.

New Documentation for Release 4.2

- *Application Installation Procedures (Release 4.2)*
- *Upgrade Procedures (Release 4.2)*
- *Continuous Computing Documentation (Release 4.2)*

Cisco Field Notices

In addition to reading the release notes and querying Bug Toolkit for release caveats and fixes, you also should visit the Cisco Field Notice Web site on a regular basis. The site provides information about updates or other issues that may impact your network.

The Cisco Field Notice Web site is located at:

http://www.cisco.com/en/US/customer/products/hw/vcallcon/ps531/prod_field_notices_list.html

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- <http://www.cisco.com>
- <http://www-china.cisco.com>
- <http://www-europe.cisco.com>

**Note**

Documentation for the Cisco BTS 10200 Softswitch on the World Wide Web sites listed above is currently available only through password access. Contact your Cisco representative for assistance.

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

**Note**

Documentation for the Cisco BTS 10200 Softswitch is not currently available on the Documentation CD-ROM.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:
<http://www.cisco.com/en/US/partner/ordering/index.shtml>
- Registered Cisco.com users can order Documentation CD-ROMs through the online Subscription Store:
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can also e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Attn Document Resource Connection
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

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

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a severity level 3 (S3) or severity level 4 (S4) problem, contact TAC by going to the TAC website:

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

S3 and S4 level problems are defined as follows:

- S3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- S4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

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

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

<http://www.cisco.com/tac/caseopen>

Contacting TAC by Telephone

If you have a severity level 1 (S1) or severity level 2 (S2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

S1 and S2 level problems are defined as follows:

- S1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- S2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0710R)