



Cisco BTS 10200 Softswitch Release Notes for Release 4.4.1

May 14, 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 detailed descriptions of the features, functions, and applications of the Cisco BTS 10200 Softswitch see the [Cisco BTS 10200 Softswitch Release 4.4 System Description](#).

Contents

The release notes for the Cisco BTS 10200 Softswitch describe the enhancements and new features provided in Release 4.4.1 (900-04.04.01.Vxx).

Each Cisco BTS 10200 Softswitch release may include a series of maintenance Vxx releases following the initial release. The release notes for the Vxx releases are updated only if they contain new information about the release.

This document includes the following sections:

- [System Requirements, page 2](#)
 - [Hardware Requirements, page 3](#)
 - [Software Requirements, page 7](#)
- [Outstanding Issues, page 11](#)
- [New Features for Release 4.4.1, page 12](#)
- [Previous 4.x Releases, page 27](#)
- [Caveats, page 39](#)
- [Cisco Field Notices, page 41](#)
- [Obtaining Documentation, page 41](#)
- [Obtaining Technical Assistance, page 43](#)

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



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

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

System Requirements

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

There are multiple hardware options available. Service providers should consult with their Cisco account team and choose the option that best suits their network applications and traffic levels.

- **Medium Platform AXmp Option**—Requires four Continuous Computing AXmp host machines (AC or DC powered), supplied as part of a complete system ordered directly from Cisco Systems.
- **Medium Platform Netra 20 Option**—Requires four Sun Microsystems Netra 20 hosts machines (AC or DC powered). This hardware option can be supplied as part of a complete system ordered directly from Cisco Systems, or it can be supported as part of a reference sale.
- **Small Platform Option**—Requires four Sun Microsystems SunFire V120 (AC-powered) or four Netra 240s (DC-powered). This hardware option can be supplied as part of a complete system ordered directly from Cisco Systems, or it can be supported as part of a reference sale.



Note

The SunFire V120s and Sun Netra 120 are both supported for existing Cisco BTS 10200 Softswitch installations. However, for new installations (for Release 4.4.1 and going forward), Cisco recommends using the SunFire V240 and Sun Netra 240 rather than using the 120s.

- **2 AXmp/2 AXi Option**—Supported for existing customers in release 4.x (dependent on system load and not going over maximum supported configurations).
- **Sun 1280 Option**—Requires four Sun Microsystems Netra 1280 hosts (AC or DC powered). This hardware option can be supplied as part of a complete system ordered directly from Cisco Systems, or supported as part of a reference sale.

The physical plant requirements for installation of the Cisco BTS 10200 Softswitch are documented in the *Cisco BTS 10200 Softswitch Building Environment and Power Site Survey*.

The Cisco BTS 10200 Softswitch consists of the following equipment:

- Call Agent/Feature Server (CA/FS)—Two application servers.
- Element Management System/Bulk Data Management System (EMS/BDMS) server—Two application servers.
- Two Ethernet switches.



Note

Release 4.1 and later supports only the SIGTRAN ITP configuration for the SS7 interface. Previous versions of the Cisco BTS 10200 Softswitch used Ulticom SS7 interface cards. These Ulticom SS7 interface cards can be decommissioned in place; they do not have to be removed from the Cisco BTS 10200 Softswitch.

- Power distribution unit (PDU) for both AC and DC systems.
 - DC-powered systems require two (redundant) feeds of 40A at -48 VDC.
 - AC-powered systems require two (redundant) circuits of 20A at 120 VAC.



Note

Both AC and DC systems require two redundant feeds. Cisco highly recommends that uninterruptible power supplies be provided for both AC and DC systems.

**Note**

You can order just the Cisco BTS 10200 Softswitch software for use in a Cisco Systems solution where you supply the Cisco-specified hardware. The Cisco TAC will only support 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 when purchased directly from Sun or another vendor. Hardware support contracts should be purchased from Sun, or the Sun Value Added Reseller.

Hardware Requirements

Hardware available from Cisco Systems Inc. for North American Cable and T1 customers is listed below as the CCPU configuration. 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 customer. This base software includes 1,000 subscriber/DS0 licenses and 5 CPS. You will need to order RTU and CPS licenses as appropriate if additional subscribers are needed.

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® announces 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 is January 1, 2005. Customers will continue to receive support from the Cisco Technical Assistance Center (TAC) until January 1, 2010. For more information, refer to the following EOS/EOL of BTS 10200 Hardware Web pages.

For SunFire 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

Table 1 Host Hardware Requirements

Hardware	Processors	Required Memory for R4.x	Recommended Memory for R4.x	Disk Size
AXMPS	4 x 440	4 GB	4 GB	2 x 36 GB
Sun Netra 120	1 x 650	2 GB	4 GB	2 x 36 GB
Sun Netra 20	2 x 1200	4 GB	4 GB	2 x 73 GB
Sun Netra 240	2 x 1280	8 GB	8 GB	2 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 Netra 1280 (2Q2005)	12 x 1200	24 GB	24 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

The Cisco BTS 10200 Softswitch interface configurations are documented in the *Cisco BTS 10200 Softswitch Release 4.4 Cabling Procedures*.

In Release 4.4.1, 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.

If you are currently running a system without enough interfaces, you will need to purchase additional 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 CFU forwarding-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 is comprised of 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 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 the customer uses 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

Part Number	Description
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. Cisco ITP Signaling Gateways are required to provide SS7 interconnectivity for the Cisco BTS 10200 Softswitch in Release 4.4.1.


Note

If using SS7 with Release 4.4.1, 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 and SCCP 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, while 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 does not affect calls or performance.

Since the Cisco BTS 10200 and ITP are both viewed as handling SS7 traffic using Sigtran protocols, they must be fully compatible as to the version of SCTP transport protocol used.

Cisco BTS 10200 has implemented the SCTP stack according to the following RFCs:

- RFC2960
- RFC3309
- RFC3758

However, the ITP does not currently support SCTP Partial Reliability (SCTP-PR), as specified in RFC3758.

[Table 5](#) lists the part numbers and quantities of boxes necessary for the Cisco ITP configurations that support the Cisco BTS 10200 Softswitch in Release 4.4.1. For more information on the ITP equipment, see the [Cisco ITP Product Data Sheet](#).

GTT Population in ITP for Remote SSN and DPC

Currently, when using Cisco ITP as the SS7 signaling gateway in conjunction with Cisco BTS 10200 for a network solution, the ITP SUA protocol layer does not notify the Cisco BTS 10200 SUA layer with any SS7 Network Management (SSNM) messages. These are normally triggered by MTP3 Pause, Resume or status changes affecting the SCCP layer services, unless the GTT is populated.

To trigger the interworking of the ITP SCCP layer with its SUA layer, ensure that the GTT table is populated in the ITP with all the Subsystem Numbers and the associated remote DPC (STP) that perform the Global Title translation.

Step 1 To populate the GTT table:

```
Router#config t
Router(config)# cs7 gtt map 1.10.2 247 sol
```

Step 2 Save the gtt-table to the Flash:

```
Router# cs7 save gtt-table flash:<filename>
```

Step 3 Include the loading of the gtt-table as part of the startup-config:

```
Router#config t
Router(config)# cs7 gtt load flash:<filename>
```

Software Requirements

The Cisco BTS 10200 Softswitch Release 4.4.1 (900-04.04.01.Vxx) software is required to run the Cisco BTS 10200 Softswitch on the hardware platforms listed above.



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 4.4.1 installation procedure.

Network Time Protocol (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. For information on how to reconfigure the NTP, refer to the Release 4.4.1 installation procedure.



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. This can cause the system to have serious problems. Allow the Solaris OS to obtain the time automatically through NTP services.

Optional Software

The following optional software can also be used with Cisco BTS 10200 Softswitch Release 4.4.1.

Cisco Extensible Provisioning Object Manager

You can use the Cisco Extensible Provisioning Object Manager (EPOM) Release 4.4.1 software as a provisioning tool for Cisco BTS 10200 Softswitch Release 4.4.1.



Note

EPOM 4.4 is the only version intended to work with Cisco BTS 10200 Release 4.4.1.

The previous version of EPOM was Release 2.1; the version number jumped from Release 4.2 to Release 4.4.

EPOM requires its own server. For more information, refer to the [Cisco EPOM Getting Started Guide](#) or the [Cisco BTS 10200 Softswitch EPOM Provisioning](#) guide.



Note

The Cisco BTS 10200 Softswitch Release 4.4.1 software uses OpenORB as the CORBA interface.

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 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](#).

Software Only Purchase

When ordering the software-only solution, you will work with the Cisco BTS 10200 Softswitch product manager to determine the correct software load. The base software load includes licenses for 1,000 subscribers/DS0 licenses and 5 CPS. If you need additional RTU and CPS, you'll need to order multiple RTU (in increments of 1K subs) and CPS licenses as appropriate.



Note

Sun hardware can be ordered directly from the vendor or a Sun Value Added Reseller; however, the Cisco TAC does not support hardware or operating systems when purchased directly from Sun or another vendor. Hardware support contracts should be purchased from Sun or the Sun Value Added Reseller when purchasing directly.

Component Interoperability

Table 5 lists the specific peripheral platforms, functions, and software loads that have been used in System Testing for interoperability with the Cisco BTS 10200 Softswitch Release 4.4.1 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	K0.00
IP Unity	Media Server	MGCP 1.0	1.5D.20
IP Unity	Application Server	SIP RFC3261	2.7
IP Unity	Voice-mail Server	SIP RFC3261	2.7
SS8 Networks Xcipio SSDF	CALEA Server	CALEA	3.4.0
Cisco CallManager	Call Processing (IP PBX)	H.323	4.0(1)
Cisco ATA	Residential Gateway SIP end point	MGCP 1.0, SIP, H.323	3.1(0)
Cisco IAD 2421	Residential/Business Gateway	MGCP 1.0	12.3(9)
Cisco IAD 2431	Residential/Business Gateway	MGCP 1.0	12.3(7)T2
Cisco 2950	LAN Switch		12.1(22)EA2
Cisco 2970	LAN Switch		12.2(25)SE
Cisco 3640	Trunking Gateway	MGCP 1.0	12.3(7)T2
Cisco 3660/3660 Telco	Trunking Gateway	MGCP 1.0, TGCP, H.323	12.3(7)T2
Cisco 3725	Trunking Gateway	MGCP 1.0	12.3(7)T2
Cisco MGX 8850 VISM	Trunking Gateway	MGCP 1.0, TGCP	3.2
Cisco AS5300	Trunking Gateway ¹	MGCP 1.0, TGCP, H.323	12.3(7)T2
Cisco AS5350	Trunking Gateway ¹	MGCP 1.0, TGCP, H.323	12.3(7)T2
Cisco AS5400	Trunking Gateway	MGCP 1.0, TGCP, H.323	12.3(7)T2
Cisco AS5850	Trunking Gateway	MGCP 1.0, TGCP, H.323	12.3(7)T2
Cisco 2600	H.323 Gateway	H.323	12.2(13)T9
Cisco 2651 ITP	SS7 Signaling Gateway	SIGTRAN M3UA/SUA	12.2(21)SW
Cisco 7200 ITP	SS7 Signaling Gateway	SIGTRAN M3UA/SUA	12.2(21)SW
Cisco 7507 ITP	SS7 Signaling Gateway	SIGTRAN M3UA/SUA	12.2(21)SW

Table 5 *Component Interoperability Matrix (continued)*

Platform(s) Tested	Function(s) Tested	Protocol(s) Tested	Load(s) Tested
Cisco uBR7246VXR Router	CMTS	PacketCable EM 08	12.3(9)BC
Combined CALEA SII/PCCMTS ubr7246	CMTS	CALEA SII	12.3(9)BC
Cisco ESR10012 Router	CMTS	CALEA SII	12.0(25)S2
Embedded MTAs:			
Arris TTM220	eMTA	NCS 1.0, IPSEC	TS040122_071504.bin.telnet_on
Arris TTM420	eMTA	NCS 1.0, IPSEC	TS040122_071504_NA.TM402.TELNET_ON.img
Motorola SBV4200	eMTA	NCS 1.0, IPSEC	7.3.2
Toshiba	eMTA	NCS 1.0, IPSEC	6.2.13
Scientific Atlanta	eMTA	NCS 1.0, IPSEC	v1.1.1r1142-0716a-1
SIP Endpoints:			
Cisco ATA	SIP Endpoint	SIP	3.1(0)
Cisco 7905/7912	SIP Phone	SIP	1.0(1)
Cisco 7940/7960	SIP Phone	SIP	6.2

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

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 non-secure FTP; to FTP to any other system, your Cisco BTS 10200 Softswitch system must have secure FTP (SFTP) capabilities.

Installation Notes

For detailed installation procedures for installing the Release 4.4.1 software, refer to the CD Jumpstart Procedure and Application Installation for Duplex Systems links on the [Cisco BTS 10200 Softswitch Application Installation Guide](#) Web page.

Installing the Cisco BTS 10200 Softswitch consists of following two procedures, in this order:

1. The Jumpstart procedure
2. The Application Installation procedure

First, use the jumpstart procedure to have the system jumpstarted with the proper OS version and kernel patch level. Then, once the system is configured properly, you can begin the application installation.

**Note**

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

Outstanding Issues

There are some outstanding issues for Cisco BTS 10200 Release 4.5. Users should familiarize themselves with these issues and the features they affect, including:

- SIP ATA—The Cisco BTS 10200 implementation of SIP ATA requires the SIP ATA to collect digits based on specific feature logic. Currently, none of the SIP ATAs (either Linksys or Cisco) support digit collection for activation, invocation, and deactivation of Call Waiting Deluxe (CWD) and Three-way Call Deluxe (TWCD). However, these features are supported by other networks via sending hookflash indication over SIP.
- Calling Name not Blocked on SIP trunk using CNAB—For Calling Name not Blocked on SIP trunk, the Blocking toggle functionality is not supported over SIP trunk interface. The details are captured in CSCsa81305.
- One-Way voice path on Call Transfer via SIP trunks—Blind Transfer on ringback.
- Digit maps on MTAs are limited in the number of rules—There may be issues with the ITU dialplan encompassing the dialing patterns, depending on the country.

New Features for 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.

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 are operator configurable.
- OCB feature remains on a per subscriber basis feature.
- 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 none are 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 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 their 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.

H.323 Applications

H.323 applications are supported in Release 4.4.1, but not Release 4.4.0. For more information, refer to the [Cisco BTS 10200 Softswitch H.323 Protocol Guide for Release 4.4.1](#) for detailed descriptions and procedures for H.323.

Replaced Commands

The following two command 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 to resume 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 purpose, it can only 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 in 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=bfgl;
CLI>add termination prefix=ds/s-0/ds1-1/; port-start=1; port-end=23; type=trunk;
mgw-id=bfgl;
CLI>add termination prefix=ds/s-0/ds1-2/; port-start=1; port-end=24; type=trunk;
mgw-id=bfgl;

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

```

New Features for 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 describes 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 4.4:

- 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 user chooses another `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 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 is based on explicitly counting the number of retransmissions. In Release 4.4.0, which is based on RFC3261, 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 been 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 request transaction timers, which control the number of retransmissions that occur before a timeout.

**Note**

When 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 RFC3261) 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 RFC3261. 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**

This 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 (SPA)

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 setup 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 setup 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 message from Call Agent to MGCP Gateway from the Call Agent (CA) 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.

SCTP-ASSOC-PROFILE Parameters

Two parameters, HB_TIMEOUT and MAX_PATH_RETRANS, were available in prior releases of Cisco BTS 10200, but were not configurable. In Release 4.4.0 and going forward, the parameters are provisionable, but require a special sequence of CLI commands to take effect. The sequence of CLI commands to run are as follows.

Change the HB_TIMEOUT or MAX_PATH_RETRANS Parameters of an SCTP Association

Step 1 Add new sctp-assoc-profile with the desired values for HB_TIMEOUT and MAX_PATH_RETRANS. For example:

```
add sctp-assoc-profile id=newProfile; BUNDLE_TIMEOUT=100; MAX_ASSOC_RETRANS=4;
MAX_PATH_RETRANS=2; RETRIEVE_FLAG=Y; MAX_RTO=2000; MIN_RTO=300; SACK_TIMEOUT=200;
HB_TIMEOUT=1000;
```

Step 2 Control out-of-service the sctp-assoc to change in Step 1.

```
control sctp-assoc id=matedSGP_assoc1; mode=forced; target-state=OOS
```

Step 3 Change the sctp-assoc to use the new profile.

```
change sctp-assoc id=matedSGP_assoc1; SCTP_ASSOC_PROFILE_ID=newProfile
```

Step 4 Control in-service the sctp-assoc.

```
control sctp-assoc id=matedSGP_assoc1; mode=forced; target-state=INS;
```

The change takes affect.

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 supports 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 set up, 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 activate 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 active and standby side for both FSPTC and FSAIN. If and when both the signaling links go down, TSA brings down the platform.

Adjustable Timer for COS-Restrict Feature Confirmation Tone

In prior releases, select few 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 would be able to hear 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 will 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 loop back 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 loop-back test origination (MGW-PROFILE::SPARE2-SUPP=Y)
 - Configuring all test lines in the testing device as Subscriber terminations.

The feature assumes that the testing and tested devices are configured on same Call Agent. The loop-back feature does not provide for performing network loop-back 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.

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 FSAIN platform.

Each OPC has two subsystems (Toll-Free and LNP) on the FSAIN platform, and each OPC will have each subsystems (CNAM and 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, while 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 BTS10200 sent MGCP messages for active calls and idle terminations (not involved in the call). This occurred when 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 (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). The Cisco BTS 10200 shall:

1. If the endpoint is IDLE (in Cisco BTS 10200 resource state), Cisco BTS 10200 sends DeleteConnection to the endpoint (same as other gateways).
2. If the endpoint is ACTIVE (in Cisco BTS 10200 resource state), and if MGCP-SPARE1-SUPP= Y in MGW-PROFILE, Cisco BTS 10200 sends 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 values of min_dn_length and max_dn_length values 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 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 tables 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.

Support for Range of Channels for TGCP Endpoints

Release 4.4.x now supports a range of endpoints in an RSIP message. The supported formats with this release include:

- aaln/s1/[x-y]@mgw.ipclab.cisco.com

- aaln/s1/*@mgw.ipclab.cisco.com
- aaln/s1/x@mgw.ipclab.cisco.com
- *@mgw.ipclab.cisco.com
- ds1/ds-0/[x-y]@mgw.ipclab.cisco.com
- ds1/ds-0/x@mgw.ipclab.cisco.com
- ds1/ds-[0-2]/*@mgw.ipclab.cisco.com
- ds1/ds-0/[3,6-9,12-18]@mgw.ipclab.cisco.com

This is only necessary for gateways which might send a range of endpoints.

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 4.4.0.

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 document 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 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 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 to 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 s subscribers.

In Release 4.2, a new field was added to the SNMP Trap Signaling 68 event/trap. The new field contains a Subscriber's 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/line controlled using the MGCP protocol using '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 similar to a basic call line (and not like a Hotline, Warmline or HOTV call respectively). Only 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. 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 31](#)
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 31](#)
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 33](#)
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 34](#)
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 35](#)
New PacketCable-based features and functions have been introduced in the Cisco BTS 10200 Release 4.1 software.
- [H.323 Annex E Redundancy, page 35](#)
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 36](#)
IPManager is a UNIX shell script that manages a set of logical interfaces to provide another layer of redundancy.
- [SS7 CIC Audits, page 36](#)
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 36](#)
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 37](#)
Release 4.1 introduces Session Initiation Protocol (SIP) device support, and the changed trunk support.
- [OAMP Enhancements, page 37](#)

Several new commands are supported in Release 4.1.

- [Modified and New Subscriber Features, page 38](#)

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 an 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, SCCP, 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 statistic measurements for these signaling protocols:

- M3UA
- ISUP
- SCCP
- 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 the 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 of 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 6](#) identifies the new ISUP traffic measurements collected for China ISUP support.

Table 6 *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 not affect existing Cisco OSS applications that utilize the CORBA interface.



Note

Cisco OSS/NMS applications include EPOM and PTC. Partner applications include CEON IPS, all of 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, including:

- 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, “[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 vice-versa) 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. As compared 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, while 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 command 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 Provisioning Guide. If the service provider does not provision an announcement, and the feature calls it, the user hears a reorder tone.

New Documentation

New Documentation for Release 4.2

- *Application Installation Procedures (Release 4.2)*
- *Upgrade Procedures (Release 4.2)*
- *Continuous Computing Documentation (Release 4.2)*

New Feature Modules

- *H.323 Video, Routing, and Transparency Features for Release 4.2*
- *Calling Party Number Options for Outgoing SETUP Message*
- *Release 4.2 SIP-T Feature Module*

New Documentation for Release 4.4.0

Release 4.4.0 introduces a new set of user documentation specifically written for the Cisco BTS 10200 Softswitch Release 4.4.0 software and hardware. When used in conjunction with the following manuals, these Release Notes provide a comprehensive guide to the Release 4.4.0 features and operations:

- ***Cisco BTS 10200 Softswitch Release 4.4 System Description***—An updated and detailed technical overview of the Cisco BTS 10200 Softswitch system.
- ***Cisco BTS 10200 Softswitch Release 4.4 Provisioning Guide***—Contains procedures that show users how to provision the Cisco BTS 10200 and the specific features used by subscribers
- ***Cisco BTS 10200 Softswitch Release 4.4 Operations and Maintenance Guide***— Contains information on system management and maintenance.
- ***Cisco BTS 10200 Softswitch Release 4.4 Command Line Interface Reference Guide***—A comprehensive reference to provisioning Cisco BTS 10200 Softswitch system tables.

These Cisco BTS 10200 documents were also modified to reflect the new information for Release 4.4.0:

- *Release Notes (Release 4.4.0)*
- *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/univercd/cc/td/doc/product/voice/bts10200/index.htm>.

Cisco BTS 10200 Softswitch Release 4.4.0 user documentation is password protected. Consult your Cisco representative for access.

Caveats

Open and resolved caveats are no longer listed in the Release Notes. Instead, the latest information on caveats is available through a new online tool, **Bug Toolkit**, available for customers to query defects according to their own needs.

Bug Toolkit

To access Bug Toolkit, you must have an Internet connection and a Web browser as well as a Cisco.com username and password.

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** If you are looking for information about 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 typing 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 By version:

- Select **Major** for the major releases (i.e., 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 3 queries for Release 3.5.3 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.
-

Definition of Major, Point and Maintenance Releases

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

Major Release

A major release is a software release with 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 when delivering 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 non-sequential (skipped) when delivering to customers. This release is based on a previous Major/Minor release and receives defect fixes synced from previous Major/Minor releases throughout the life of this release.

Maintenance Release

A maintenance software release has defect fixes included to address specific problems. The Maintenance Release number increments as content is added and numbers may be non-sequential (skipped) when delivering to customers.

Release Naming Conventions

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

1. BTS 10200 uu.ww.xx.yzz (for example, in the Release Notes)
2. 900-uu.ww.xx.yzz (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—
 - D = Development load
 - I = Integration load
 - Q = System test load
 - F = Field verification Ready
 - V = Verified (specified for externally available)

Some naming convention examples are:

- 900-03.05.02V04
- 900-03.05.03V00
- 900-04.01.00V03

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 priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

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

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—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 priority level 1 (P1) or priority level 2 (P2) 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>

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.