



Planning

Getting Started with Planning

The goal of the planning process is to create a customized plan for deploying Cisco BLISS for Cable in your service provider telephony network. The plan will include identifying the components and technology that are needed to implement Cisco BLISS for Cable. Surveys capture information that is needed before your application is installed and configured.

Before You Begin

Work with your Cisco consultant to select an application or combination of applications.

- See [Cisco Cable-Ready Solutions for VoIP](#) for an introduction to VoIP systems for cable operators.
- See the [Cisco PacketCable™ Primer White Paper](#) for information about the architecture of PacketCable™ 1.1 and Cisco's implementation of this architecture.
- See the [Cisco BLISS for Cable Release 2.2 Overview](#) concept for a description of Cisco BLISS for Cable.

When You Are Done

You will understand [site preparation and network communications](#) requirements for the Cisco BTS 10200.



Note The Cisco BTS 10200 Softswitch User Documentation is password protected. See your Cisco representative for access information.

You will have completed the [Network Site Survey](#) and the [Building Environment and Power Site Survey](#) for the Cisco BTS 10200.

Go on to the [Installing](#) process.

Planning Tasks

Identifying the Components That You Need: Determine the components that are required to implement Cisco BLISS for Cable, including recommended hardware and software. Use the [Cisco BLISS for Cable Components](#) table to guide you.

Planning Redundancy: Read about and understand the requirements for a fault-tolerant network, understand the failover behavior of network components, and understand how to use this information to plan a system with optimum fault tolerance.

Planning Installation and Configuration: Be prepared with the information that you need to install and configure the Cisco BTS 10200 and other components.

Planning Concepts

Read these conceptual, overview topics for the background knowledge that you need to build an intelligent plan.

Cisco BLISS for Cable Solution Overview: An introduction to Cisco BLISS for Cable, in which individual Cisco hardware and software components are integrated for seamless interoperability.

Cisco BTS 10200 Softswitch Technical Overview: An introduction to the Cisco BTS 10200 Softswitch, a software-based, class-independent network switch that provides call-control intelligence for establishing, maintaining, routing, and terminating voice calls through the packet network via media gateways (MGWs), while seamlessly operating with legacy circuit-switched networks.



Note The Cisco BTS 10200 Softswitch User Documentation is password protected. See your Cisco representative for access information.

Other key concept topics:

Voice Services in Cable Networks

Cisco PacketCable™ Primer White Paper

Migration Paths for Voice-over-IP to PacketCable™

Cisco BTS 10200 in the PacketCable™ Network Overview

Cisco BTS 10200-Supported Signaling Protocols

Planning to Configure ITP

PacketCable™ Lawful Intercept Architecture



Note If you have already logged into www.cisco.com with the BTS guest username and password, you may receive an error message when attempting to access the *PacketCable™ Lawful Intercept Architecture* document. To access this document, close all open instances of your browser, restart your browser program, and log into www.cisco.com with your own registered username and password.

Identifying the Components That You Need

Use the following chart to identify the components you need for Cisco BLISS for Cable and the recommended hardware and software for each component.

Table 2-1 Cisco BLISS for Cable Components

Component	Role in the Solution	Hardware	Software and Release Level
Call Management Server (CMS)	<p>The CMS:</p> <ul style="list-style-type: none"> Provides the call-control intelligence for establishing, maintaining, routing, and terminating voice calls. Provides call-feature intelligence for telephony services. Serves as an interface to enhanced application platforms, such as voice mail and unified messaging. 	<p>The Cisco BTS 10200 Softswitch requires four application servers (two for the Call Agent/Feature Server and two for the Element Management System/Bulk Data Management System).</p> <ul style="list-style-type: none"> Small Platform Option—Requires four Sun Microsystems 240 hosts (Netra or Sunfire). Medium Platform Option—Requires four Sun Microsystems 440 hosts (Netra or Sunfire). Large Platform Option—Requires four Sun Microsystems 1280 hosts (Netra or Sunfire). <p>The Cisco BTS 10200 also requires two AC or two DC system switch routers (the Cisco Catalyst 2950, for example), two power distribution units (PDUs), and a terminal server (Cisco BTS 10200 Alarm Panel).</p> <p>See the Cisco BTS 10200 Softswitch Release Notes for Release 4.5 for more information about hardware requirements.</p>	<p>Cisco BTS 10200 Softswitch, Release 4.5</p> <p>Note The Cisco BTS 10200 Softswitch user documentation is password protected. See your Cisco representative for access information.</p>
Media Gateway Controller (MGC)	The MGC provides direct control over the media gateways that provide bearer interconnection to the PSTN.	—	Cisco BTS 10200 Softswitch, Release 4.5
Cisco IP Transfer Point (ITP) Signaling Gateway	<p>The Cisco ITP is required in order to provide SS7 interconnectivity for the Cisco BTS 10200 Softswitch in Release 4.5.</p> <p>For more information, see Cisco ITP as the Signaling Gateway for the Cisco BTS 10200 Softswitch.</p>	Cisco ITP 7301	12.2(25)SW3
		Cisco ITP 7507	12.2(25)SW3
			See also Cisco IP Transfer Point in IOS Software Release 12.2(25)SW3

Table 2-1 Cisco BLISS for Cable Components (continued)

Component	Role in the Solution	Hardware	Software and Release Level
Cable Modem Termination System (CMTS)	<p>The CMTS is a Cisco universal broadband router (uBR) with features that enable it to communicate with a hybrid fiber coaxial (HFC) cable network via a Cisco MCxx cable modem card. Cisco MCxx cable modem cards allow you to connect cable modems on the HFC network to a Cisco uBR in a Community Antenna Television (CATV) headend facility. The modem card provides the interface between the Cisco uBR protocol control information (PCI) bus and the radio frequency (RF) signal on the DOCSIS HFC network.</p> <p>For more information, see the <i>Cisco CMTS Feature Guide</i>.</p>	<p>Cisco uBR7246VXR</p> <ul style="list-style-type: none"> • Network Processing Engine: NPE-G1 • Broadband Processing Engine: <ul style="list-style-type: none"> – Cisco MC28U – Cisco MC28X – Cisco MC16U – Cisco MC16X 	12.3(9a)BC3
		<p>Cisco uBR10012</p> <ul style="list-style-type: none"> • Performance Routing Engine: <ul style="list-style-type: none"> – PRE-1 – PRE-2 • Broadband Processing Engine: <ul style="list-style-type: none"> – Cisco 5x20U – Cisco 5x20S 	12.3(9a)BC3
Media Gateway (MG)	The MG provides interconnection between IP networks and the PSTN to transmit bearer traffic.	<p>MGX8880, 8850:</p> <ul style="list-style-type: none"> • PXM-45 <ul style="list-style-type: none"> – VXSM – RPM-XF • PXM-1 <ul style="list-style-type: none"> – VISM 	<p>5.2(0.200)</p> <p>5.2(0.200)</p> <p>12.3(11)T7</p> <p>1.3.11</p> <p>3.3</p>
Embedded Multimedia Terminal Adapter (eMTA)	Residential gateways in the form of MTAs embedded in a cable modem (embedded MTA [eMTA]) provide access at the customer premises. By plugging a standard analog telephone into the MTA device, a user can make phone calls to another MSO's customer directly across the IP network or to anyone outside the network through a media gateway.	Arris Touchstone eMTA	4.1.34

Table 2-1 Cisco BLISS for Cable Components (continued)

Component	Role in the Solution	Hardware	Software and Release Level
Aggregation	<p>Cisco Catalyst 6509 Ethernet switches are used in Cisco BLISS for Cable to provide Layer 2 connectivity among the IP core, Cisco BTS 10200 Softswitch, and ancillary servers and element management components necessary to provision and maintain certain features in Cisco BLISS for Cable.</p> <p>The Cisco Catalyst 6509 also provides Layer 3 functionality for routing signaling packets to edge and trunking gateways, and to interconnect all servers within the SuperPOP.</p> <p>The Cisco Catalyst 6509 can also be used to aggregate the traffic from multiple CMTSs into a single interface on a Cisco 12000 series Internet router.</p>	Cisco Catalyst 6509	12.1(13)E12 or later
Core	Core routing functions.	Cisco 12000 Series Internet Router	12.0(13.3)S or later
Communications Assistance for Law Enforcement Act (CALEA)-Compliant Server	Lawful Intercept (LI) compliance in the United States is specified by the Communications Assistance for Law Enforcement Act (CALEA). For more information about PacketCable™ Lawful Intercept Architecture, see here .	SS8 Networks Xcipio	—
Media Server	The IP Unity Media Server can be used as an announcement server, voice-mail server, media server and/or application server in Cisco BLISS for Cable.	IP Unity Media Server	2.7
Record Keeping Server (RKS)	The RKS monitors and collects PacketCable™ event message data over LAN/WAN networks for Cable VoIP and content-based services, utilizing the PacketCable™ protocol standards. The application extracts all the relevant parts of a call and creates a call detail record (CDR) in the appropriate format for the billing and operations support systems.	See manufacturer's recommendations.	<p>Primal Solutions, Inc. RKS Software Access IM, 8.2.3 Rater 5.4.3 WPM 2.4.0</p> <p>Note Primal Solutions RKS Software has been tested only for integration.</p>

Table 2-1 Cisco BLISS for Cable Components (continued)

Component	Role in the Solution	Hardware	Software and Release Level
Network Management	Cisco Broadband Access Center (BAC) is a distributed, scalable, subscriber-device management application that enables automated flow-through provisioning of subscriber services. See the Cisco BACC Administrator's Guide for Release 2.6 for more information.	Sun 220 or 440 (large environment)	Release 2.6
	JacobsRimell's APS Softswitch Manager for Cisco BLISS Customers provides subscriber provisioning and infrastructure configuration for call management servers, signaling gateways, media gateways, softswitches, and BACC.	See manufacturer's recommendations.	JacobsRimell APS Softswitch Manager, Version 3.2 Note JacobsRimell software has been tested only for integration.
	Auspice's Cisco Cactus Correlation Solution provides service assurance.	See manufacturer's recommendations.	Auspice Cisco Cactus Correlation Solution: <ul style="list-style-type: none"> • TLX 4.2 • CCC 1.0 Note The Auspice products have been tested only for integration.

Planning Redundancy

Building redundancy into Cisco BLISS for Cable is recommended to maximize uninterrupted service if there is a component or network failure. Cisco BLISS for Cable has been designed to make optimum use of redundant components, providing automatic switchover and maintenance of call data during periods of critical hardware or software problems.

For more information about redundancy in Cisco BLISS for Cable, read the [Cisco Cable Voice Solutions High Availability White Paper](#).

Planning Installation and Configuration

Complete the following tasks before you begin installing or configuring Cisco BLISS for Cable.

Read [Site Preparation and Network Communications Requirements](#) for the Cisco BTS 10200. Verify that you have met all of the requirements listed in the document.



Note The Cisco BTS 10200 Softswitch User Documentation is password protected. See your Cisco representative for access information.

Complete the [Cisco BTS 10200 Softswitch Building Environment and Power Site Survey](#). Verify that your site meets the requirements listed in the survey.

Complete the [Network Site Survey For Software Installation](#) for the Cisco BTS 10200 Softswitch. The survey is used to collect information required by the Cisco BTS 10200 Softswitch application software to communicate with the service provider network. Your Cisco representative will use the information that you provide in this survey to create a customized Network Information Data Sheet (NIDS), which contains information used during the installation of the application software.

Cisco BLISS for Cable Release 2.2 Overview

Cisco Broadband Local Integrated Services Solutions (BLISS) is a service provider solution that delivers voice, video, and data services over a converged broadband access network. The bundled services can be delivered over the last mile through a variety of access mechanisms including T1/E1, cable, and Metro Ethernet. Cisco BLISS for Cable has been adapted specifically to the needs of the cable industry. Cisco has aggressively pursued component qualification against PacketCable™ specifications, the requirements for the cable industry. Cisco BLISS for Cable focuses on the North American Cable Operators/Multiple Systems Operators (MSOs) market and delivers the following incremental benefits to MSOs:

- Leverages investments made in upgrading the cable access plant
- Expands the set of services deliverable to end customer to include local voice services
- Delivers an integrated, tested solution to cable operators, which decreases risk and expedites time-to-market
- Enables operators to bundle services that increase revenue
- Adheres to cable industry standards to ensure interoperability and deliver important services

Cisco BLISS for Cable architecture builds upon the PacketCable™ standards and uses a Media Gateway Control Protocol (MGCP)-based centralized call control architecture.

Cisco BLISS for Cable Release 2.2 builds upon Cisco BLISS for Cable Releases 1.0, 1.5, and 2.0 and expands the framework to include new elements, features and cable access technology using packetized data transmission over the cable television hybrid fiber coaxial (HFC) network.

Cisco BLISS for Cable Release 2.2 features include

- New Solution Components and Protocols:
 - Cisco IP transfer point (ITP) signaling gateway (SG): A-links
 - Cisco MGX 8880 with VxSM
 - High availability cable modem termination system (CMTS)
 - Call admission control (CAC) for CMTS
 - Enhanced network management system (NMS) tools (JacobsRimell and Auspice)
 - External log server
 - T.38 fax relay call agent-controlled mode across SIP trunk interface
- Telephony Features:
 - Block toll free calls per subscriber

- Star code to access voice mail
- Single vertical service code (VSC) to activate or deactivate both call forwarding on no answer (CFNA) and call forwarding on busy (CFB)
- Stand-alone call redirection to voice-mail
- No solicitation announcement
- Incoming privacy indicator flag on call detail record (CDR)
- Operations, Architecture, and Security Features:
 - Call data block (CDB) filename based on PC filenaming conventions
 - .DONE indicator after successful transmission of call DB records to billing mediation server
 - Trace active call per directory number and trunk identification
 - Network continuity test and TDM test enhancements
 - Support for Communications Assistance for Law Enforcement Act (CALEA)
 - 30 originating point codes
- Scalability Features:
 - Subscriber database (DB) expansion to 125k subscriber lines
 - Large-hardware support: Sun 1280 (eight processors)

Architectural Overview

Cisco BLISS for Cable architecture is based on the CableLabs® PacketCable™ 1.5 architecture and utilizes the CableLabs® DOCSIS™ 1.1 HFC access network architecture, along with MSOC backbone architecture. Within Cisco BLISS for Cable, the Cisco BTS 10200 performs the functions of the call management server (CMS) and the media gateway controller (MGC) as defined in the PacketCable™ 1.5 specifications.

Cisco BLISS for Cable architecture consists of multiple functional planes:

- Customer premise equipment (CPE) layer and access gateways provide uplink technology.
- Aggregation layer provides aggregation of traffic from all of the CPE uplinks.
- Core switching layer provides the packet backbone.
- Trunking layer provides the interface between the public-switched telephone network (PSTN) and the Internet service provider (ISP).
- Call control and management provides the call control/signaling support, feature server interfaces, and support for network resource interfaces such as announcement servers and CALEA servers.
- Network management layer provides the EMS and network management components.

Solution Interoperability

Cisco BLISS for Cable relies on interoperability with various partner systems to provide particular functions. The partner systems may include multimedia terminal adapters (MTAs), announcement systems, interactive voice response (IVR) systems, voice-mail systems, billing mediation systems, and electronic surveillance systems.

QoS

Voice quality is primarily affected by three factors: delay, jitter, and loss. Cisco is a clear market leader with a superior quality of service (QoS) mechanism implemented in Cisco BLISS for Cable, which satisfies the ITU-T standard G.114 recommendations for delay.

IP Network QoS Design

With Cisco BLISS for Cable, the voice and data traffic generated from the cable modem is assigned the following IP precedence values:

- Bearer real-time traffic: IP precedence 5
- Voice signaling traffic: IP precedence 3
- Data traffic coming from the cable modem: IP precedence 0

To provide appropriate latency and jitter characteristics throughout the Cisco BLISS for Cable architecture, low-latency queuing (LLQ) is the primary queuing technique for all output service policies (queue structures for system backhaul links) on all platforms except the Cisco GSR 12000 Series routers, where the [modified deficit round robin \(MDRR\)](#) queuing strategy is used to provide a strict queue.

LLQ provides a combination of a priority queue (one that is completely serviced first, without deference to any other queues) for real-time traffic (namely RTP) and class-based weighted fair queuing (CBWFQ) for all other traffic types.

[Weighted random early detection \(WRED\)](#) is employed as the primary congestion avoidance technique. This QoS mechanism provides the ability to drop lower-priority traffic classes more aggressively than higher-priority traffic classes by looking at the average queue size.

Queue depth is analyzed against a minimum and maximum threshold. For an average queue depth below the minimum threshold, packets are queued. For an average queue depth above the maximum threshold, packets are dropped. When the average queue depth is between the minimum and maximum, a drop probability is used to determine the linear rate of drop. [DiffServ-compliant WRED uses differentiated services code point \(DSCP\)](#) to determine the drop probability.

Dynamic Quality of Service

DQoS Concept

A key feature of a PacketCable™ network is a dynamic quality of service (DQoS) capability that is similar to the dynamic services provided by DOCSIS 1.1. However, DOCSIS 1.1 DQoS authorizes and provisions services only in the cable network and does not reserve the resources needed to propagate a call from one endpoint to another across the network.

PacketCable™ DQoS extends the DOCSIS 1.1 services across the entire network so that resources can be dynamically authorized and provisioned from one endpoint to another. This prevents possible theft-of-service attacks and guarantees customers the services that they are authorized to use.

The PacketCable™ DQoS model uses a two-stage resource reservation process, in which resources are first reserved and then committed. This allows a bidirectional reservation process that ensures that resources are available at both endpoints of the connection before the call is actually placed.

When an MTA makes a call request, the local CMTS communicates with the gate controller to authorize the call's resources. After the resources are authorized, the CMTS reserves the local resources while it negotiates with the remote end for the resources required at that end.

The CMTS uses DOCSIS 1.1 dynamic service addition (DSA) messages to reserve the resources and then uses dynamic service change (DSC) messages to commit the resources.

When all required resources are available, the local CMTS and remote CMTS both commit the resources, allowing traffic to flow. Usage accounting and billing do not begin until the remote MTA picks up and the call is actually in progress.

The DQoS model ensures that both endpoints of a call, as well as the backbone network, have reserved the same bandwidth and that the bandwidth is reserved only while the call is in progress. When a call terminates, all portions of the network can release the call's resources and make them available for other users.

Making a Call Using DQoS

DOCSIS 1.1 networks use service flows to implement different QoS policies, but service flows exist only within the cable network. To control the service flows and to extend them across the entire network, a PacketCable™ network creates and maintains “gates.”

A gate is a logical entity created on the CMTS at each side of a connection that authorizes and establishes a particular DQoS traffic flow. The CMTS communicates with the gate controller to coordinate the creation of matching gates at each end of the connection.

Gates are unidirectional, so separate gates are required for the downstream and upstream traffic flows. The same gate ID, however, is usually used for both the downstream and upstream gates for a call. Each CMTS maintains its own set of gates, so a bidirectional traffic flow requires four gates to be created: two gates on the local CMTS and two gates on the remote CMTS.

For a typical call, gates progress through the following stages to create a DQoS traffic flow:

1. The local MTA makes a call request.
2. The gate controller sends a Gate-Allocation command to the CMTS, which creates a gate in response and sets its state to Allocated.
3. The call management server, which might be the same server as the gate controller, parses the call request to translate the destination phone number into the appropriate destination gateway.
4. The gate controller verifies that the MTA that is making the call request is authorized for the required resources.
5. The gate controller sends a Gate-Set command to the CMTS, which sets the gate state to Authorized.
6. The CMTS on each side of the connection reserves the local resources needed for the call, setting the gate state to Reserved.
7. As the remote CMTS and local CMTS perform gate coordination, their respective gates are set to the Local_Committed and Remote_Committed states.
8. When both sides have reserved all required resources, each CMTS sets its gate state to Committed, allowing traffic to flow.

Security

Within Cisco BLISS for Cable, the following PacketCable™ security measures are implemented:

- Signaling Security is based on IPsec encapsulating security payload (ESP) (3DES, HMAC-MD5) transport mode. Security association (SA) is unidirectional.
- IPsec Key management is either Kerberos (KDC) or IKE (pre-shared key):
 - NCS Signaling Security uses Kerberized IPsec
 - IPsec/IKE is used over the COPS and RADIUS interfaces

- Media Security uses AES (encrypted RTP and RTCP). This affects DQoS bandwidth/flows-spec calculation.
- Media Security Ciphersuite negotiation is in NCS Signaling (LCO and SDP). Null Ciphersuites are supported but still signaling in SDP.
- All PacketCable™ 1.0 Security requirements for CMS are implemented.

Information about Security Interface Features on the Cisco BTS 10200 Softswitch is available [here](#).

Other Planning Concepts

The following informational resources may help you in planning your Cisco BLISS for Cable system:

[Cisco BLISS for Cable Solution Overview](#)

[Cisco BTS 10200 Overview](#)



Note The Cisco BTS 10200 Softswitch User Documentation is password protected. See your Cisco representative for access information.

[Voice Services in Cable Networks](#))

[Cisco Packet Cable Primer](#)

[Migration Paths for Voice-over-IP to PacketCable™](#)

[Cisco BTS 10200 in the PacketCable™ Network Overview](#)

[Cisco BTS 10200-Supported Signaling Protocols](#)

[Planning to Configure ITP](#)

[PacketCable™ Lawful Intercept Architecture](#)



Note If you have already logged into www.cisco.com with the BTS guest username and password, you may receive an error message when attempting to access the *PacketCable™ Lawful Intercept Architecture* document. To access this document, close all open instances of your browser, restart your browser program, and log into www.cisco.com with your own registered username and password.

