



Home

Cisco BLISS for Cable

Welcome to the information site for Cisco Broadband Local Integrated Services Solution (BLISS) for Cable, the Cisco solution that enables service providers to deliver primary line voice services that comply with CableLabs® PacketCable™ specifications. This site contains the solution documentation that you need to plan, install, configure, provision, operate, maintain, and troubleshoot Cisco BLISS for Cable.

Supported Releases

This documentation covers Cisco BLISS for Cable through Release 2.2. If you are upgrading from a previous Cisco BLISS for Cable release, begin by reading the [Release Notes for Cisco BLISS for Cable Release 2.2](#) to familiarize yourself with functionality in this new release.

User Audiences and Processes

This documentation is written for customer staff who plan and implement Cisco BLISS applications. Information on each of the main processes is presented under its own tab.

Role	Objectives
Network Architect	Planning , so that you can tailor Cisco BLISS for Cable to your objectives.
Installer/Network Administrator	Installing , so that you can confidently install the right components, in the right order, for the system that you have selected.

Role	Objectives
Network Operator/Administrator	<p>Configuring, so that you can configure each component in your system. We provide overview information about the order in which components should be installed and configured, and links to detailed instructions for configuring and provisioning the Cisco BTS 10200 and other components.</p> <p>Provisioning, so that you can provision new features and subscribers.</p> <p>Operating, so that you can carry out day-to-day operations and maintenance tasks, including upgrading software and applying patches.</p> <p>Troubleshooting, so that you can optimize your application and find out what to do about specific Cisco BTS alarms and other network symptoms. This topic also includes links to basic troubleshooting documentation for other components.</p>
All	<p>Reference information, so that you can quickly look up topics such as Cisco BTS default settings or alarms. This information might be available elsewhere as needed for you to perform a particular task, but the Reference tab collects it in summary, reference form.</p>

Related Topics

[Using This Information System](#)—Basic instructions and tips on using this system.

[Obtaining Documentation](#) and [Obtaining Technical Assistance](#)—Standard Cisco information.

[Release Notes](#)—Cisco BTS 10200 and other major component release notes.

[Cisco BLISS for Cable Release 2.2 Overview](#)—Start here to get an overview of Cisco BLISS for Cable and the various components and features it comprises.

Using This Information System

This information system is designed to give you an easily-navigable portal to all documentation related to Cisco BLISS for Cable. The system is organized according to the processes and tasks that you use in deploying and operating your solution.

[About the Information System Window](#)

[Types of Topics](#)

[Tips for Using This System](#)

About the Information System Window

The information system window is laid out so that you can easily navigate between topic areas, select more detailed information, and directly access product and platform documentation, without ever losing your place or having to cope with a complex hierarchy of windows.

Types of Topics

You can tell what type of topic a link is from its name:

- “Doing” topics, such as “Installing the Cisco BTS 10200,” are task topics and provide instructions for doing something.
- “Overview” topics, such as “Planning to Configure ITP,” are concepts to help you understand and plan your deployment and carry out tasks knowledgeably.

Where Information Is Located

Cisco BLISS for Cable encompasses a range of products and technologies, and the documentation encompasses information that may reside in several locations:

- Solution overviews and high-level process and procedure information specific to Cisco BLISS for Cable is located within this information system.
- Product and technology overviews, detailed requirements, task details, and other more generic topics are located outside this information system. These topics have the appearance of standard Cisco documentation with which you may already be familiar. Links to these topics appear with an icon that indicates that clicking the link opens the topic in a new, secondary browser window offset from the current window, rather than replacing the current topic in the content area of the current window.

About the Secondary Browser Window

When a topic like “Installing the Cisco BTS 10200” opens in a new, secondary browser window, that window stays open until you close it. (Click the **Close** button or choose **File > Close**.) If the window is open when you click another link that opens in a secondary browser window, the new topic replaces the current one.

Tips for Using This System

- Use the tabs to navigate between major process areas.
- Use the left navigation menu to navigate to major topics within a process.
- In a secondary popup window:
 - When you are done with the window, click the **Close** button to close it. (It does not close automatically.)
 - You can go back to a previous topic by right-clicking and choosing **Back** or **Forward**.
 - You can view normal browser toolbars, the address bar, and similar items using commands on the **View** menu.

Obtaining Documentation

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

Cisco.com

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

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

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

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

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

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

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

Documentation Feedback

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

You can send comments about Cisco documentation to bug-doc@cisco.com.

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

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

We appreciate your comments.

Cisco Product Security Overview

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

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

From this site, you can perform these tasks:

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

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

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

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

Reporting Security Problems in Cisco Products

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

- Emergencies—security-alert@cisco.com

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

- Nonemergencies—psirt@cisco.com

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

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

**Tip**

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

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

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

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

Obtaining Technical Assistance

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

Cisco Technical Support & Documentation Website

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

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

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

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

**Note**

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

Submitting a Service Request

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

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

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

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

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

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

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

Release Notes

Release Notes for Cisco BLISS for Cable

[Release Notes for Cisco BLISS for Cable Release 2.2](#)

When the release notes open (in a new window), you can download the PDF version by right-clicking the PDF icon.

Release Notes for Cisco BLISS for Cable Components

Cisco BTS 10200 Softswitch:

Cisco BTS 10200 Softswitch Release Notes for Release 4.5

Cisco IP Transfer Point (ITP):

Release Notes for Cisco 7000 Series Routers for Cisco IOS Release 12.2 SW

Cable Modem Termination System (CMTS):

Release Notes for Cisco uBR7200 Series for Cisco IOS Release 12.3 BC

Cross-Platform Release Notes for Cisco IOS Release 12.3

Media Gateway:

5.0.10 Release Notes for MGX 8880 Media Gateway

5.2.00 Release Notes for Cisco MGX 8850, Cisco MGX 8950, and Cisco MGX 8830

Release Notes for Cisco MGX Route Processor Module (RPM-XF) Cisco IOS Release 12.3(11)T7 for PXM45-based Switches, Release 5.2.00

Release Notes for Cisco Voice Interworking Service Module Release 3.3.20

Network Management:

Broadband Access Center for Cable Release Notes for Release 2.6

Acronyms

Common Acronyms Used in Cisco BLISS for Cable Documentation

A B C D E F G H I J K L M N O P Q R S T U V W X

Acronym	Definition
A	
AAA	authentication, authorization, and accounting
AC	automatic callback
AC_ACT	automatic callback activation
AC_DEACT	automatic callback deactivation
ACR	anonymous call rejection
ACR_ACT (ACRA)	anonymous call rejection activation
ACR_DEACT (ACRD)	anonymous call rejection deactivation
ACRA (ACR_ACT)	anonymous call rejection activation
ACRD (ACR_DEACT)	anonymous call rejection deactivation
AGW	access gateway
AIN	Advanced Intelligent Network
AIOD	automatic identified outward dialing
ALI	automatic location identification
AMA	automated message accounting
ANC	announcements module
ANI	automatic number identification

Acronym	Definition
ANS	announcement server
ANSI	American National Standards Institute
API	application programming interface
AR	automatic recall
AR_ACT	automatic recall activation
AR_DEACT	automatic recall deactivation
AT	access tandem
ATA	analog telephone adaptor
ATIS	Alliance for Telecommunications Industry Solutions
ATM	Asynchronous Transfer Mode
B	
B-number	DN that a user enters as the forward-to number (also referred to as MN)
BCM	basic call module
BDMS	Bulk Data Management System
BEM	billing event message
BGDP	basic group dialing plan
BGL	business group line
BLA	billing adapter
BLISS	Broadband Local Integrated Services Solution
BLV	Busy Line Verification
BP	block pair
BRIDS	Bellcore rating input database system
BS	billing server
BTA	basic trading area
C	
CA	call agent
CAC	carrier access code
CALEA	Communications Assistance for Law Enforcement Act
CAMA	centralized automatic message accounting
CAS	channel-associated signaling
CAT	customer access treatment
CATV	Community Antenna Television
CBLK	call block (reject caller)
CBR	constant bit rate
CBWFQ	class-based weighted fair queuing
CCS	common channel signaling
CCW	cancel call waiting

Acronym	Definition
CDB	call data block
CDP	custom dial plan
CDR	call detail record
CE	computing element
CFB	call forwarding on busy
CFBVA	call forwarding on busy variable activation
CFBVD	call forwarding on busy variable deactivation
CFNA	call forwarding on no answer
CFNAVA	call forwarding on no answer variable activation
CFNAVD	call forwarding on no answer variable deactivation
CFU	call forwarding unconditional
CFUA	call forwarding unconditional activation
CFUD	call forwarding unconditional deactivation
CFVBBG	call forwarding variable for basic business group
CFVABBG	CFVBBG activation
CFx	A general reference to all of the forwarding features (CFB, CFNA, and CFU)
CHD	call hold
CIC	circuit identification code, carrier identification code
CID	calling identity delivery, also caller ID (<i>see also</i> CND)
CIDB	calling identity delivery blocking
CIDCW	calling identity delivery on call waiting
CIDS	calling identity delivery and suppression (per call)
CIDSD	calling identity delivery and suppression (per call)—delivery part
CIDSS	calling identity delivery and suppression (per call)—suppression part
CIP	carrier identification parameter
CLASS	custom local area signaling services
CLC	Carrier Liaison Committee
CLEC	competitive local exchange carrier
CLEI	common language equipment identifier
CLI	command-line interface
CLIP	calling line ID presentation
CLIR	calling line ID restriction
CLLI	Common Language Location Identifier
CMIP	Common Management Information Protocol
CMS	call management system, call management server

Acronym	Definition
CMTS	cable modem termination system
CNAB	calling name delivery blocking
CNAM	calling name delivery
CND	calling number delivery, calling number display
CNDB	calling number delivery blocking
CNM	connection module, customer network management
CO	central office
COCUS	central office code utilization survey
CODEC	coder/decoder, compression/decompression
COPS	Common Open Policy Service Protocol
CORBA	Common Object Request Broker Architecture
COS	class of service
COT	customer-originated trace, continuity testing, central office termination
CPCN	certificate of public convenience and necessity
CPE	customer premises equipment
CPRK	call park
CPRK_RET	call park retrieve
CPSG	call park subscriber group
CPU	call pickup, central processing unit
CS	capability set (for example, CS-2)
CSA	callpath services architecture
CSN	circuit switched network
CSR	carrier sensitive routing
CT	call transfer, call type
CW	call waiting
CWI	call waiting indication
D	
DA	directory assistance, distinctive alerting
DACWI	distinctive alerting call waiting indication
DF	delivery function (CALEA)
DID	direct inward dialing
DLEC	data local exchange carrier
DN	directory number
DND	do not disturb
DNIS	dialed number identification service
DNS	Domain Name System
DOCSIS	Data Over Cable Service Interface Specification

Acronym	Definition
DOD	direct outward dialing
DOW	day of week
DOY	day of year
DP	dial plan, dial pulse, demarcation point
DPC	destination point code
DPN	directed call pickup without barge-in
DPN_O	directed call pickup without barge-in (originate)
DPN_T	directed call pickup without barge-in (terminate)
DPU	directed call pickup with barge-in
DPU_O	directed call pickup with barge-in (originate)
DPU_T	directed call pickup with barge-in (terminate)
DQoS	dynamic quality of service
DRCW	distinctive ringing/call waiting
DRCW_ACT	distinctive ringing/call waiting activation
DSA	dynamic service addition
DSC	dynamic service change
DSCP	differentiated services code point
DSL	digital subscriber line
DSP	digital signal processing
DSX	digital system cross-connect frame
DTMF	dual tone multifrequency
E	
E1	Wide-area digital transmission scheme used predominantly in Europe that carries data at a rate of 2.048 Mbps. European equivalent of T1.
E3	Wide-area digital transmission scheme used predominantly in Europe that carries data at a rate of 34.368 Mbps. European equivalent of T3.
E-911	Enhanced 911
E & M	“Ear and Mouth.” Switch-to-switch signaling on PSTN
EA	equal access
EC	echo cancellation
ECSA	Exchange Carriers Standards Association
EDP	event detection point
EM	event message
EMS	Element Management System, Event Messages Specification (PacketCable™)
eMTA	embedded multimedia terminal adapter
ERC	easily recognizable codes

Acronym	Definition
ERQNT	Embedded Request for Notification
ESB	Emergency Service Bureau
ESL	emergency service line
ESP	encapsulating security payload
ETSI	European Telecommunications Standards Institute
F	
FCAPS	fault, configuration, accounting, performance, security
FCI	furnish charging information
FCP	Feature Control Protocol
FGB	Feature Group B
FGD	Feature Group D
FIM	feature interaction manager
FS	Feature Server
FSAIN	Feature Server for Advanced Intelligent Network services
FSPTC	Feature Server for POTS, Tandem, and Centrex services
FTP	File Transfer Protocol
FXO	Foreign Exchange Office
FXS	Foreign Exchange Station
G	
GAP	generic address parameter
GSM	global system for mobile communications
GUI	graphical user interface
H	
HFC	hybrid fiber coaxial
HLR	home location register
HNPA	home numbering plan area
HSI	H.323 signaling interface
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
I	
IAD	integrated access device
IANA	Internet Assigned Numbers Authority
IAP	intercept access point
ICAP	Inter-call Agent Protocol
ICMP	Internet Control Message Protocol
IDDD	international direct distance dialing
IE	information element

Acronym	Definition
IETF	Internet Engineering Task Force
IKE	Internet key exchange
ILEC	incumbent local exchange carrier
IMT	intermachine trunk
IN	intelligent network
INC	Industry Numbering Committee
IP	Internet Protocol
IPM	impulses per minute
IPsec	Internet Protocol security
IPT	IP-based telephony
IRDP	ICMP Router Discovery Protocol
ISA	ISDN adapter
ISDN	Integrated Services Digital Network
ISFG	incoming simulated facility group
ISO	International Organization for Standardization
ISP	Internet service provider
ISS	ISDN stack
ISUP	ISDN user part
ITP	IP transfer point
ITU	International Telecommunications Union
IVR	interactive voice response
IXC	interexchange carrier
J	
JCA	Java cryptography architecture, Java console agent
JCM	Java console module
JDBC	Java database connectivity
JMS	Java message service
K	
KAM	keepalive module
kbps	kilobits per second
L	
LAN	local-area network
LATA	local access and transport area
LCR	least cost routing
LDAP	Lightweight Directory Access Protocol
LEC	local exchange carrier
LERG	local exchange routing guide

Acronym	Definition
LI	lawful intercept
LIDB	line information database
LLQ	low-latency queuing
LNP	local number portability
LPC	local point code
LRN	local routing number
LRQ	location request (H.323 signaling)
LRU	least recently used
LSA	local serving area
LSSGR	LATA Switching Systems Generic Requirements
M	
Mbps	megabits per second
MCF	multiple call forwarding
MCS	media gateway control stack
MDC	midcall
MDN	multiple directory numbers
MDRR	modified deficit round robin. A queuing strategy in which nonempty queues are served one after another, in round-robin fashion.
MF	multifrequency
MG (MGW)	media gateway
MGA	media gateway adapter
MGC	media gateway controller
MGCP	Media Gateway Control Protocol
MGW (MG)	media gateway
MIB	Management Information Base
MIME	Multipurpose Internet Mail Extensions
MLHG	multiline hunt group
MN	<i>See</i> B-number
MNM	maintenance module
ms	millisecond
MSA	Metropolitan Statistical Area
MSO	Multiple Systems Operator
MSOC	multiservice over cable
MSU	message signal unit
MTA	multimedia terminal adapter
MTP	Message Transfer Part
MTU	maximum transmission unit

Acronym	Definition
MWI	message waiting indicator
N	
NANP	North American Numbering Plan
NAS	network access server
NCS	network-based call signaling
NE	network element
NEBS	Network Equipment Building Standards
NFAS	Non-Facility Associated Signaling
NIS	Network Information Service
NMS	network management system
NO	network operator
NOC	network operations center
NOD	nature of dial
NPA	Numbering Plan Area
NSE	name signaling event
NTP	Network Time Protocol
NU	network unit
nxx	NANP digits: n=2, 3, ...9 and x=0, 1, ...9
O	
OAM	Operation, Administration, and Maintenance, Operations, Administration module
OAM&P	Operations, Administration, Maintenance, and Provisioning
OBCSM	originating basic call state machine
OCB	outgoing call barring
OCN	operating company number
OI	operator interrupt
OLI	originating line information
OPC	originating point code
OPT	Open Packet Telephony
OS	operating system
OSA	open service adapter
OSFG	outgoing simulated facility group
OSI	Open Systems Interconnection
OSS	operations support system
OSSGR	Operator Services Systems Generic Requirements
P	
PBX	private branch exchange
PCI	protocol control information

Acronym	Definition
PCM	pulse code modulation
PCMA	pulse code modulation a-law
PCMU	pulse code modulation mu-law
PCPS	per-call presentation status
PCS	personal communications services
PCSNDB	personal communications services numbering database
PDU	power distribution unit
PIC	presubscribed interexchange carrier, point in call
PLT	platform
POI	point of interface, point of interconnection
POP	point of presence
POPD	public office dialing plan
POSIX	Portable Operating System Interface UNIX
POTS	plain old telephone service
PPP	Point to Point Protocol
PPQ	point to point queuing
PPS	permanent presentation status
PRI	primary rate interface
PS	presentation status
PSAP	public safety answering point
PSTN	public switched telephone network
PVC	permanent virtual circuit
Q	
QoS	quality of service
QSIG	Q (point of the ISDN model) Signaling. Signaling standard. Common channel signaling protocol based on ISDN Q.931 standards and used by many digital PBXs.
R	
RACF	remote activation of call forwarding
RACF-PIN	remote activation of call forwarding personal ID number
RADIUS	Remote Authentication Dial-In User Service
RAID	redundant array of inexpensive disks
RAS	Registration, Admission, and Status protocol. A protocol that is used between endpoints and the gatekeeper to perform management functions. The RAS signaling function performs registration, admissions, bandwidth changes, status, and disengage procedures between the VoIP gateway and the gatekeeper.
RCF	remote call forwarding

Acronym	Definition
RDBS	routing database system
RDM	redundancy module
RDT	recall dial tone
RF	radio frequency
RFC	Request for Comment (IETF)
RGW	residential gateway
RIP	Routing Information Protocol
ROH	receiver off hook
RPC	remote point code, remote procedure call
RQNT	request for notification
RR	resource record
RSA	rural service area
RSIP	restart in progress
RSM	resource module
RSVP	Resource Reservation Protocol
RTM	routing module
RTP	Real-Time Transport Protocol
R-UDP	Reliable User Datagram Protocol (Cisco Systems proprietary signaling backhaul protocol)
S	
S7A	SS7 adapter
S7S	SS7 stack (DGM&S)
SA	security association
SAC	service access call
SAI	signaling adapter interface
SC1D	speed call 1-digit
SC1D_ACT	speed call 1-digit activation
SC2D_ACT	speed call 2-digit activation
SCA	selective call acceptance
SCA_ACT	selective call acceptance activation
SCF	selective call forwarding
SCF_ACT	selective call forwarding activation
SCP	service control point, signal control point
SCR	selective call rejection
SCR_ACT	selective call rejection activation
SCTP	Stream Control Transmission Protocol
SDK	Software Development Kit
SDP	Session Description Protocol

Acronym	Definition
SFG	simulated facility group
SFTP	Secure File Transfer Protocol (FTP)
SG	signaling gateway
SGCP	Simple Gateway Control Protocol
SIA	SIP adapter
SID	system identification number
SIM	service interaction manager
SIP	Session Initiation Protocol
SLE	screening list editing
SLTA	Signaling Link Test Acknowledgment (an SS7 signaling link test message type)
SLTM	Signaling Link Test Message (an SS7 signaling link test message type)
SM	Session Manager
SMA	SNMP adapter
SMDS	Switched Multimegabit Data Service
SMTP	Simple Mail Transfer Protocol. Internet protocol providing e-mail services
SNMP	Simple Network Management Protocol. A network management protocol used in TCP/IP networks.
SOHO	small office home office
SP	service provider
SPCS	stored program control system
SQL	Structured Query Language
SRST	Survivable Remote Site Telephony
SS7	Signaling System 7
SSF	service switching function
SSH	secure shell
SSL	secure sockets layer
SSP	service switching point, signal switching point
STP	signal transfer point
SVC	switched virtual circuit
T	
T1	trunk level 1. Digital WAN carrier facility. T1 transmits DS-1-formatted data at 1.544 Mbps through the telephone-switching network.
T3	trunk level 3. Digital WAN carrier facility. T3 transmits DS-3-formatted data at 44.736 Mbps through the telephone-switching network. Compare with E3.

Acronym	Definition
TAC	Cisco Technical Assistance Center
TAP	Telocator Alphanumeric Paging Protocol
TBCSM	terminating basic call state machine
TCAP	Transaction Capabilities Application Part
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDD	telecommunications device for the deaf
TDM	time-division multiplexing
TDP	trigger detection point
TF	toll free
TG	trunk group
TGW	trunking gateway
TMN	Telecommunications Management Network
TNS	transit network selection
TOD	time of day
TOPS	traffic operator position system
TOS	type of service
TPM	terminating point master
TRS	telecommunications relay services
TSAP	transport service access point
TTY	text typewriter
TWC	three-way calling
U	
UAA	user authentication adapter
UAC	user agent client
UAS	user agent server
uBR	universal broadband router (Cisco)
UCD	uniform call distribution
UDP	User Datagram Protocol
URI	uniform resource identifier
URL	universal resource locator
USTWC	usage-sensitive three-way calling
V	
VBR	variable bit rate
VLAN	virtual LAN
VMWI	visual message waiting indicator
VoATM	Voice over ATM

Acronym	Definition
VoIP	Voice over IP
VSC	vertical service code
W	
WAN	wide-area network
WFI	waiting for instruction
WRED	weighted random early detection
X	
xDSL	(generic) digital subscriber line



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	<p>12.2(25)SW3</p> <p>See also Cisco IP Transfer Point in IOS Software Release 12.2(25)SW3</p>

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.





Installing

Getting Started with Installing

The goal of this process is to successfully install the required components for Cisco BLISS for Cable.

Before You Begin

Complete the [Planning](#) process, including identifying needed components and familiarizing yourself with all detailed product requirements and important concepts for the application that you are implementing. Have copies of the completed [Network Site Survey](#) and Network Information Data Sheet (NIDS) provided by Cisco for your specific system. If you would like to enter any parameters different from the values on these data sheets, contact Cisco TAC for an evaluation of the potential impact of the changes. Obtain Cisco TAC concurrence on any changes.

When You Are Done

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

Installation Tasks

Installation Concepts

Installation Tasks

Complete the following tasks to install and initially configure Cisco BLISS for Cable components.

Task	Details
Install and configure Broadband Access Center for Cable (BACC).	<p>The Cisco BACC Installation Guide for Release 2.5 provides instructions for installing and configuring BACC.</p> <p>The BACC Administrator's Guide for Release 2.6 provides information on configuring BACC and on PacketCable™ DHCP options to BACC properties mapping.</p> <p>Note DNS and DHCP must be configured before other solution components are installed, because those components will use DNS.</p>
Install the Cisco BTS 10200 Softswitch server hardware according to manufacturer recommendations.	<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>For more information about hardware requirements, see the Cisco BTS 10200 Softswitch Release Notes for Release 4.5.</p>
Install the power distribution unit (PDU) for AC or DC systems.	<p>The PDU and power strips can be ordered through Cisco.</p> <ul style="list-style-type: none"> • DC-powered systems require two (redundant) feeds of 40 A. The Cisco part number is BTS10200-DCPDU=. • AC-powered systems require two (redundant) circuits of 20 A. The Cisco part number is BTS10200-ACPDU=.
Install the terminal server according to manufacturer recommendations.	<p>You need one alarm panel or your own terminal server that allows for console login. The Cisco BTS 10200 Alarm Panel serves as a terminal server. For more information about hardware requirements, see the Cisco BTS 10200 Softswitch Release Notes for Release 4.5.</p>
Install the Cisco Catalyst 2950 switches.	<p>The Catalyst 2950 Switch Hardware Installation Guide provides instructions for installing the Catalyst 2950.</p>
Cable the Cisco BTS 10200 hardware to the Cisco Catalyst 2950 switches.	<p>The Cisco BTS 10200 Softswitch Cabling, VLAN, and IRDP Procedures document provides instructions for cabling the Cisco BTS 10200 hardware to the Cisco Catalyst 2950 hardware.</p>

Task	Details
Configure VLANs on the Catalyst 2950.	The <i>Cisco BTS 10200 Softswitch Cabling, VLAN, and IRDP Procedures</i> document provides instructions for setting up VLANs on Catalyst 2950 switches.
Enable Internet Control Message Protocol (ICMP) Router Discovery Protocol (IRDP) on the Cisco BTS 10200 Softswitch and on adjacent routers.	The <i>Cisco BTS 10200 Softswitch Cabling, VLAN, and IRDP Procedures</i> document provides instructions for enabling IRDP.
Jumpstart the Cisco BTS 10200 hardware to install the Sun operating system, file systems, and necessary patches to the Sun servers.	<i>Cisco BTS 10200 Softswitch CD Jumpstart Procedure for Solaris 10 Based Duplex Systems, Release 4.5</i> , provides instructions for jumpstarting Solaris 10 on the Cisco BTS 10200 Softswitch host machines using the jumpstart CD.
Install the Cisco BTS 10200 Softswitch software.	<i>Cisco BTS 10200 Softswitch Application Installation, Release 4.5</i> , provides instructions for installing release 4.5 of the Cisco BTS 10200 Call Agent/Feature Server and Element Management System software on the servers.
Install the MGX.	The <i>Cisco MGX 8800/8900 Hardware Installation Guide, Releases 2-5.2</i> , provides instructions for installing the MGX components.
Install the Cisco IP Transfer Point (ITP) hardware.	Select from the following guides, depending on the component that you are using for ITP: <ul style="list-style-type: none"> • <i>Cisco7301 Installation and Configuration Guide</i> • <i>Cisco 7500 Series Installation and Configuration Guide</i>
Install Cisco ITP.	The <i>ITP Installation and Operations Manual</i> provides instructions for installing ITP.
Install the CMTS.	Select from the following guides, depending on the CMTS component you are using: <ul style="list-style-type: none"> • <i>Cisco uBR7246VXR Universal Broadband Router Hardware Installation Guide</i> • <i>Cisco uBR10012 Universal Broadband Router Hardware Installation Guide</i>
Install the embedded multimedia terminal adapter (eMTA).	See the appropriate manufacturer recommendations.

Installation Concepts

Read these conceptual, overview topics for the background knowledge that you need to install Cisco BLISS for Cable components.

BTS 10200 Site Preparation and Network Communications Requirements

Cisco MGX 8800/8900 Hardware Installation Guide, Releases 2 - 5.2:

- *Product Overviews*

- *Preparing for Installation*

Broadband Access Center for Cable Release 2.5: Preparing to Install Components



Configuring

Getting Started with Configuring

The goal of this process is for you to do the following:

- Understand the tasks required to configure Cisco BLISS for Cable components.
- Configure all required Cisco BLISS for Cable components.
- Verify that the network is successfully configured.

Before You Begin: Complete the [Installing](#) process for all components required in your application.

When You Are Done: After you verify communication among components, your network is ready to place in service. Go on to the [Provisioning](#) process to provision features and subscribers or on to the [Operating](#) process for information on ongoing management of your network.

[Configuration Tasks by Component](#)

[Configuration Tasks by Feature](#)

[Configuration Concepts](#)

Configuration Tasks by Component

Complete the tasks in the following table to configure components that are part of Cisco BLISS for Cable.

You will find additional configuration information in the [Configuration Tasks by Feature](#) section.

Task	Details
Configure the Cisco BTS 10200.	<p>Configuring the Cisco BTS 10200 consists of provisioning a series of data tables on the Call Agent and Feature Servers. A complete Cisco BTS 10200 implementation is very complex and will vary by customer.</p> <p>More detailed information about the Cisco BTS 10200 data tables and fields can be found in the Cisco BTS 10200 Command Line Interface Reference Guide.</p> <p>An overview of PacketCable™ specific features can be found in the Cisco BTS 10200 Softswitch PacketCable™ and Event Message Provisioning and Operations Guide.</p> <p>Note The Cisco BTS 10200 Softswitch user documentation is password protected. See your Cisco representative for access information.</p>
Configure the Cisco IP Transfer Point (ITP).	<p>The Cisco IP Transfer Point (ITP) in IOS Software Release 12.2(25)SW3 document provides configuration tasks and procedures.</p>
Configure the cable modem termination system (CMTS).	<p>Select from the following guides, depending on the CMTS component you are using:</p> <ul style="list-style-type: none"> • Cisco uBR7200 Series Software Configuration Guide • Cisco uBR10012 Universal Broadband Router Software Configuration Guide <p>In addition, the Cisco CMTS Feature Guide provides information about specific features.</p> <p>The Cisco Broadband Cable Command Reference Guide contains the cable-specific commands for the Cisco uBR7100 series, Cisco uBR7200 series, and Cisco uBR10012 universal broadband routers.</p> <p>The CMTS Configuration FAQ provides answers to frequently-asked questions about configuring CMTS.</p>

Task	Details
Configure the Cisco MGX components.	<p>The <i>Cisco MGX 8850 (PXM1E/PXM45), MGX 8950, MGX 8830, and MGX 8880 Configuration Guide, Release 5</i>, provides instructions for configuring the MGX 8880 and MGX 8850.</p> <p>The <i>Cisco MGX 8850 (PXM1E/PXM45), MGX 8950, MGX 8830, and MGX 8880 Command Reference, Release 5</i>, provides a detailed description of the PXM commands required for configuration at the shelf and PXM card level.</p> <p>The <i>Voice Switch Services (VXSM) Configuration and Command Reference Guide, Release 5</i>, provides instructions for configuring the VXSM.</p> <p>The <i>Cisco Voice Interworking Services (VISM) Configuration Guide & Command Reference, Release 3.3</i>, provides instructions for configuring the VISM.</p> <p>In particular, see <i>Configuration for VoIP Switching Applications</i> for configuring VoIP switching applications on a Cisco MGX 8850 or MGX 8880 equipped with VXSMs.</p>
Configure the embedded multimedia terminal adapter (eMTA).	Although there are standard PacketCable™ parameters defined for MTAs, the actual configuration is vendor-specific. For specific configuration procedures, see the appropriate vendor documentation
Configure Broadband Access Center for Cable (BACC).	<p>The BACC <i>Administrator's Guide for Release 2.6</i> provides BACC configuration checklists and task information for the following:</p> <ul style="list-style-type: none"> • Configuring BACC • Configuring and using the sample user interface • BACC support tools and advanced concepts • Device provisioning engine CLI
Configure Cisco SIP devices.	The <i>Cisco BTS 10200 SIP Provisioning Guide</i> provides instructions for configuring SIP devices.

Configuration Tasks by Feature

Complete the tasks in the following table to configure particular features of Cisco BLISS for Cable. You will find additional configuration information in the [Configuration Tasks by Component](#) section.

Task	Details
Configuring Lawful Intercept (LI) for CALEA Compliance.	<p>The PacketCable™ Lawful Intercept Architecture document provides configuration files for the following devices:</p> <ul style="list-style-type: none"> • Cisco uBR 7246 VXR CMTS • VISM Trunking Gateway • Cisco BTS 10200 Call Agent • SS8 Xcipio Mediation Device <p>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.</p>
Configure T.38 fax relay.	<p>The T.38 Fax Relay Feature Module provides instructions for configuring T.38 fax relay on the Cisco BTS 10200 Softswitch.</p> <p>Note The Cisco BTS 10200 Softswitch user documentation is password protected. See your Cisco representative for access information.</p>

Configuration Concepts

Read these conceptual overview topics to better understand configuration concepts related to Cisco BLISS for Cable:

Cisco ITP as the Signaling Gateway for the BTS 10200 Softswitch

Planning to Configure ITP

Broadband Access Center for Cable DOCSIS and PacketCable™ Options

Cisco MGX 8850 (PXM1E/PXM45), MGX 8950, MGX 8830, and MGX 8880 Configuration Guide, Release 5: Preparing for Configuration



Provisioning

Getting Started with Provisioning

The goal of this process is for you to provision Cisco BLISS for Cable features and subscribers.

Before You Begin: Complete the [Configuring](#) process for all components that are required in your application.

When You Are Done: Go on to the [Operating](#) process for information on ongoing management of your network.

Provisioning Tasks

Provisioning Concepts

Provisioning Tasks

Complete the following tasks to provision Cisco BLISS for Cable features and subscribers.

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

Task	Reference
Provision the Cisco BTS 10200 features and subscribers.	Cisco BTS 10200 Provisioning Guide
Provision PacketCable™ features on the Cisco BTS 10200.	Cisco BTS 10200 Softswitch PacketCable™ and Event Message Provisioning and Operations Guide (Release 4.5)
Provision the dial plan.	Cisco BTS 10200 Softswitch Dial Plan Guide
Provision SIP subscribers.	Cisco BTS 10200 SIP Provisioning Guide
Provision devices on the Broadband Access Center for Cable (BACC).	Device Provisioning Engine CLI

Provisioning Concepts

Read these conceptual, overview topics for the background knowledge that you need to provision Cisco BLISS for Cable features and subscribers.

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

[Cisco BTS 10200 Softswitch Provisioning Overview](#)

[Cisco BTS 10200 Network and Subscriber Feature Descriptions](#)

[Cisco BTS 10200 Dial Plan Guide: Preparing for Dial Plan Provisioning](#)



Operating

Getting Started with Operating

The goal of this process is to help you successfully operate your network day-to-day.

Before You Begin: Complete the [Installing](#), [Configuring](#), and [Provisioning](#) processes for all components and features required in your application.

Operating Tasks by Component

Operating Concepts

Upgrade Information

Operating Tasks by Component

This section provides references to resources for operating the components within Cisco BLISS for Cable.

Component	Resource
Call Management Server (CMS) or Media Gateway Controller (MGC): <ul style="list-style-type: none">• Cisco BTS 10200 Softswitch	Cisco BTS 10200 Operations and Maintenance Guide Note The Cisco BTS 10200 Softswitch user documentation is password protected. See your Cisco representative for access information.
Cisco IP Transfer Point (ITP) signaling gateway (SG): <ul style="list-style-type: none">• Cisco ITP 7301• Cisco ITP 7507	Cisco IP Transfer Point (ITP) in IOS Software Release 12.2(25)SW3

Component	Resource
CMTS: <ul style="list-style-type: none"> • Cisco uBR7246 • Cisco uBR10012 	The <i>Cisco CMTS Feature Guide</i> provides overview information and configuration tasks and examples. The <i>Cisco Broadband Cable Command Reference Guide</i> contains cable-specific commands for the Cisco uBR7100 series, Cisco uBR7200 series, and Cisco uBR10012 universal broadband routers.
Media Gateway (MG): <ul style="list-style-type: none"> • MGX8880 <ul style="list-style-type: none"> – PXM-45 – RPM-XF – VXSM • MGX 8850 <ul style="list-style-type: none"> – PXM-1 – VISM 	The <i>Cisco MGX 8850 (PXM1E/PXM45), MGX 8950, MGX 8830, and MGX 8880 Configuration Guide, Release 5</i> , provides switch operating procedures .
Broadband Access Center for Cable (BACC)	The <i>BACC Administrator's Guide for Release 2.6</i> provides information about the following operational tasks: <ul style="list-style-type: none"> • database management • log files • alerts and alert messages
Embedded multimedia terminal adapter (eMTA)	See the appropriate manufacturer documentation.

Operating Concepts

Read these conceptual, overview topics for the background knowledge that you need to operate Cisco BLISS for Cable.

Cisco MGX 8850 (PXM1E/PXM45), MGX 8950, MGX 8830, and MGX 8880 Configuration Guide, Release 5: Switch Operating Procedures

Upgrade Information

Upgrade guides for the Cisco BTS 10200 Softswitch are located [here](#).

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





Troubleshooting

Getting Started with Troubleshooting

This topic provides links to detailed troubleshooting information for the Cisco BTS 10200 and other solution components.

The [Troubleshooting Resources](#) section provides links to documentation to help you troubleshoot Cisco BLISS for Cable at the component level.

The [Troubleshooting Concepts](#) section contains an overview of troubleshooting concepts for Cisco BLISS for Cable. It provides guidelines for troubleshooting problems on the network, including guidelines for preventing problems before they occur.

Troubleshooting Resources

This section provides resources for troubleshooting Cisco BLISS for Cable at the component level. See the [Troubleshooting Concepts](#) section for generic troubleshooting information.

1

If You Are Troubleshooting . . .	Use This Document
Call Management Server (CMS) or Media Gateway Controller (MGC): <ul style="list-style-type: none"> • Cisco BTS 10200 Softswitch 	<ul style="list-style-type: none"> • Cisco BTS 10200 Troubleshooting Guide Release 4.5 <p>Note The Cisco BTS 10200 Softswitch user documentation is password protected. See your Cisco representative for access information.</p>
Cisco IP Transfer Point (ITP) signaling gateway (SG): <ul style="list-style-type: none"> • Cisco ITP 7301 • Cisco ITP 7507 	<ul style="list-style-type: none"> • Cisco BTS 10200 Softswitch SS7 SIGTRAN Solution Guide • Cisco 7500 Series Routers Troubleshooting Documentation Roadmap

If You Are Troubleshooting . . .	Use This Document
CMTS: <ul style="list-style-type: none"> • Cisco uBR7246 	<ul style="list-style-type: none"> • Hardware Troubleshooting the Cisco uBR72xx / uBR7246 VXR Universal Broadband Router • Cisco uBR7200 Series Universal Broadband Routers Field Notices
<ul style="list-style-type: none"> • Cisco uBR10012 	<ul style="list-style-type: none"> • Cisco uBR10012 Universal Broadband Router Troubleshooting Guide • Cisco uBR10012 Universal Broadband Router Field Notices
Media Gateway (MG): <ul style="list-style-type: none"> • MGX8880 <ul style="list-style-type: none"> – PXM-45 – RPM-XF – VXSM • MGX8850 <ul style="list-style-type: none"> – PXM-1 – VISM 	<ul style="list-style-type: none"> • Cisco MGX 8800 Series Switch System Error Messages • MGX Error Messages, Release 5 • VXSM Troubleshooting
Embedded Multimedia Terminal Adapter (eMTA)	See the appropriate manufacturer's documentation.
Cisco Broadband Access Center for Cable (BACC)	Cisco BACC CLI Reference Guide, Support and Troubleshooting Commands Cisco Broadband Access Center Troubleshooting Tech Notes

Troubleshooting Concepts

Troubleshooting consists of determining the nature of a problem and then isolating the problem to a particular device or component of a device. When a problem has been isolated and identified, troubleshooting also consists of fixing the problem, usually by replacing the device, some component of the device, or changing a setting or variable in the software.

Cisco telephony solutions include connections to external switches and to internal components such as call agents, signal processors, and trunking gateways. This complex environment involves many connections, links, and signaling protocols. Connectivity and performance problems are very difficult to resolve. The goal of this section is to provide you with a general troubleshooting strategy for isolating and resolving connectivity and performance problems.

The general idea of a troubleshooting model is to systematically reduce a large set of possible causes of trouble to a small set of causes or to a single cause. You can then fix the problem and restore network function. After the problem is resolved, a systematic method of documenting the case helps to capture, preserve, and communicate the troubleshooting experience gained while solving the problem.

As more advanced technologies and services are introduced into communication networks, the tasks of designing, managing, and maintaining the resulting networks are also becoming increasingly complex. The use of a systematic troubleshooting model increases the expertise of the organization and reduces the time to solve similar problems in the future. This evolution of improving expertise and collaboration can help mitigate the pressures of supporting crucial, complex networks.

Interoperability

Cisco BLISS for Cable uses a wide range of network elements (NEs), but there are certain limitations. Some features involve the use of other NEs deployed in the service provider network: for example, gateways, media servers, announcement servers, MTAs, and Session Initiation Protocol (SIP) phones. See [Cisco BLISS for Cable Components](#) for a complete list of hardware and software tested for compatibility in Cisco BLISS for Cable. In addition, see the [Component Interoperability](#) section of the *Cisco BTS 10200 Softswitch Release Notes for Release 4.5* for a complete list of the specific peripheral platforms, functions, and software loads that have been used in system testing for interoperability with the Cisco BTS 10200 Softswitch Release 4.5 software.

Earlier or later releases of platform software might be interoperable, and it might be possible to use other functions on these platforms. The list certifies only that the required interoperation of these platforms, the functions listed, and the protocols listed have been successfully tested with the Cisco BTS 10200 Softswitch.

Symptoms, Problems, and Solutions

The symptoms of a problem can be general (such as being unable to access the SS7 network) or specific (routes are not in a routing table). First, you need to determine the cause of a symptom by using troubleshooting tools and techniques. After identifying the cause, you can correct the problem.

Attempt to reproduce the reported symptoms, if possible. If you cannot reproduce the symptoms, it will be extremely difficult to analyze and solve the problem. If you cannot narrow the troubleshooting scope to a particular subsystem or component, you may not be able to determine how to fix the problem.

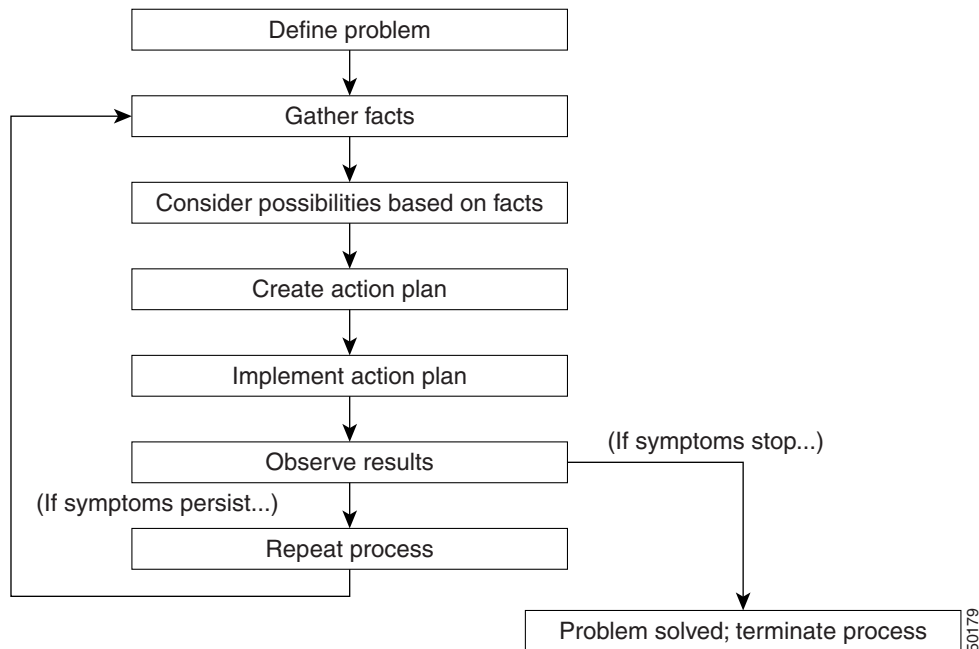
General Problem-Solving Model

When you are troubleshooting in a telephony environment, a systematic approach always works best. An unsystematic approach to troubleshooting can result in a “quick fix,” but it is usually a waste of valuable time and resources and often makes the situation worse.

A systematic approach employs the following steps:

- Define the specific symptoms
- Identify all potential problems that could be causing the symptoms
- Systematically eliminate each potential problem (from the most likely to the least likely) until the symptoms disappear

The following figure illustrates the process flow for the general problem-solving model. This process flow is not a rigid outline for troubleshooting a network; it is simply a foundation from which you can build a problem-solving process to suit your particular environment.



The following steps detail the problem-solving process outlined in the problem-solving model illustration:

-
- Step 1** When analyzing a network problem, make a clear problem statement. You should define the problem in terms of a set of symptoms and potential causes.
To properly analyze the problem, identify the general symptoms and then ascertain what kinds of problems could cause these symptoms. For example, hosts might not be responding to service requests from clients (a symptom). Possible causes might include a misconfigured host, bad interface cards, or missing router configuration commands.
- Step 2** Gather the facts that you need to help isolate possible causes.
Ask questions of affected users, network administrators, system managers, and other key people. Collect information from sources such as network management systems, protocol analyzer traces, output from diagnostic commands, or the software release notes.
- Step 3** Consider possible problems based on the facts that you gathered. Using the facts, you can eliminate some of the potential problems from your list.
Depending on the data, for example, you might be able to eliminate hardware as a problem so that you can focus on software problems. At every opportunity, try to narrow the number of potential problems so that you can create an efficient plan of action.
- Step 4** Create an action plan based on the remaining potential problems. Begin with the most likely problem, and devise a plan in which only one variable is manipulated.
Changing only one variable at a time enables you to reproduce a given solution to a specific problem. If you alter more than one variable simultaneously, you might solve the problem, but identifying the specific change that eliminated the symptom becomes far more difficult and will not help you solve the same problem if it occurs in the future.
If a variable change does not resolve the network problem, change the variable back to its initial setting before proceeding. This allows the resolution of the network problem to be traced to a single variable change instead of a combination of variable changes.

- Step 5** Implement the action plan, performing each step carefully while testing to see whether the symptom disappears. Whenever you change a variable, be sure to gather results. Generally, you should use the same method of gathering facts that you used in [Step 2](#) (that is, working with the key people affected, in conjunction with utilizing your diagnostic tools).
- Step 6** Analyze the results to determine whether the problem has been resolved. If it has, then the process is complete.
- Step 7** If the problem has not been resolved, create an action plan based on the next most likely problem in your list. Return to [Step 4](#), change one variable at a time, and repeat the process until the problem is solved.
-

**Note**

If you exhaust all the common causes and actions—either those outlined in this section or ones that you have identified for your environment—you should contact your Cisco technical support representative.

Resolving Network Problems

It is always easier to recover from a network failure if you are prepared for it ahead of time. Possibly the most important requirement in any network environment is to have current and accurate information about that network available to the network support personnel. Intelligent decisions can be made about network change only with complete information.

To determine whether you are prepared for a network failure, answer the following questions:

- Do you have an accurate physical and logical map of your network?
- Does your organization or department have an up-to-date network map that outlines the physical location of all the devices on the network and how they are connected, as well as a logical map of network addresses, network numbers, subnetworks, and so forth?
- Do you have a list of all network protocols implemented in your network?
- For each of the protocols implemented, do you have a list of the network numbers, subnetworks, zones, areas, and so on that are associated with them?
- Do you know which protocols are being used to route calls?
- For each protocol, do you have correct, up-to-date configuration information?
- Do you know all the points of contact to external networks, including any connections to the Internet, the public switched telephone network (PSTN), or the Signaling System 7 (SS7) network?
- For each external network connection, do you know what protocols are being used?
- Do you have an established baseline for your network?
- Has your organization documented normal network behavior and performance at different times of the day so that you can compare the current problems with a baseline?

If you can answer yes to all of these questions, you will be able to recover from a failure more quickly and easily than if you are not prepared. Lastly, for every problem solved, be sure to document the problems with solutions provided. This way, you will create a problem/answer database that others in your organization can refer to in case similar problems occur later. This will invariably reduce the time to troubleshoot your networks and, consequently, minimize your business impact.

Resolving System Problems

If the troubleshooting procedures that you follow do not solve the problems, contact your technical support group. If additional support is needed, contact Cisco Technical Assistance Center (TAC) for assistance. See the [Obtaining Technical Assistance](#) section for more information.

When possible, have the following information on hand before calling Cisco TAC for technical support:

- Alarms currently active on the system
- Summary of events that may be related to this problem
- Current status of internal and external components (administrative and operational states)
- Hardware documentation and cabling diagrams, if applicable



Reference

Reference Information

This section provides quick lookup of reference topics for the Cisco BLISS for Cable components. Portions of this material are available elsewhere under different headings, but the Reference tab collects it in summary, reference form.

Subject	Reference
Cisco BTS 10200 Softswitch: Call Management Server; Media Gateway Controller	<p>Cisco BTS 10200 Softswitch Release 4.5 Documentation:</p> <ul style="list-style-type: none"> • Release Notes • System Description • Site Preparation and Network Communications Requirements <p>Note The Cisco BTS 10200 Softswitch user documentation is password protected. See your Cisco representative for access information.</p>
Cisco IP Transfer Point (ITP) Signaling Gateway: ITP 7301, ITP 7507	<p>Cisco ITP as the Signaling Gateway for the Cisco BTS 10200 Softswitch</p> <p>Cisco IP Transfer Point (ITP) in IOS Software Release 12.2(25)SW3</p>
Cable Modem Termination System (CMTS): Cisco uBR7216, Cisco uBR10012	<p>CMTS Overview</p> <p>Cisco CMTS Feature Guide</p> <p>Cisco IOS Release 12.3</p>
Media Gateway	<p>Guide to MGX 8880 Media Gateway User Documentation</p> <p>Guide to Multiservice Switch and Media Gateway Documentation</p>
Aggregation; Cisco Catalyst 6509	<p>Introduction to the Cisco Catalyst 6509 Switch</p> <p>Release Notes for Cisco IOS Release 12.1E on the Catalyst 6500 and Cisco 7600 Supervisor Engine and MSFC</p>

Subject	Reference
Core; Cisco GSR 12000 Series Router	Cisco IOS 12.0(13.3)S
Communications Assistance for Law Enforcement Act (CALEA)-Compliant Server; SS8 Networks Xcipio	<p data-bbox="902 308 1385 338">PacketCable™ Lawful Intercept Architecture</p> <p data-bbox="902 354 1474 667">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.</p> <p data-bbox="902 699 1141 728">SS8 Networks Xcipio</p>
Network Management; Broadband Access Center for Cable (BACC)	<p data-bbox="902 747 1414 777">Introduction to Cisco Broadband Access Center</p> <p data-bbox="902 793 1474 848">Release Notes for Broadband Access Center for Cable Release 2.6</p> <p data-bbox="902 865 1308 894">Administrator's Guide for Release 2.6</p>



About

Cisco BLISS for Cable Release 2.2

Cisco BLISS for Cable Release 2.2 Documentation: First edition 10/31/2005

Legal Notices

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

Cisco Systems, Inc. Copyright 2005



Help

Using This Information System

This information system is designed to give you an easily-navigable portal to all documentation related to Cisco BLISS for Cable. The system is organized according to the processes and tasks that you use in deploying and operating your solution.

[About the Information System Window](#)

[Types of Topics](#)

[Tips for Using This System](#)

About the Information System Window

The information system window is laid out so that you can easily navigate between topic areas, select more detailed information, and directly access product and platform documentation, without ever losing your place or having to cope with a complex hierarchy of windows.

Types of Topics

You can tell what type of topic a link is from its name:

- “Doing” topics, such as “Installing the Cisco BTS 10200,” are task topics and provide instructions for doing something.
- “Overview” topics, such as “Planning to Configure ITP,” are concepts to help you understand and plan your deployment and carry out tasks knowledgeably.

Where Information Is Located

Cisco BLISS for Cable encompasses a range of products and technologies, and the documentation encompasses information that may reside in several locations:

- Solution overviews and high-level process and procedure information specific to Cisco BLISS for Cable is located within this information system.
- Product and technology overviews, detailed requirements, task details, and other more generic topics are located outside this information system. These topics have the appearance of standard Cisco documentation with which you may already be familiar. Links to these topics appear with an icon that indicates that clicking the link opens the topic in a new, secondary browser window offset from the current window, rather than replacing the current topic in the content area of the current window.

About the Secondary Browser Window

When a topic like “Installing the Cisco BTS 10200” opens in a new, secondary browser window, that window stays open until you close it. (Click the **Close** button or choose **File > Close**.) If the window is open when you click another link, the new topic replaces the current one.

Tips for Using This System

- Use the tabs to navigate between major process areas.
- Use the left navigation menu to navigate to major topics within a process.
- In a secondary popup window:
 - When you are done with the window, click the **Close** button to close it. (It does not close automatically.)
 - You can go back to a previous topic by right-clicking and choosing **Back** or **Forward**.
 - You can view normal browser toolbars, the address bar, and similar items using commands on the **View** menu.



A

access gateway [30](#)
aggregation [27](#)
alarm panel [36](#)
announcement server [27, 30](#)
application server [27, 36](#)
architecture
 DOCSIS [30](#)
 lawful intercept [27](#)
 PacketCable [23, 30](#)

B

billing mediation systems [30](#)

C

cable modem termination system [26](#)
CALEA [27](#)
call control [30](#)
call control intelligence [25](#)
call detail record [30](#)
call feature intelligence [25](#)
call management server [25, 30](#)
CBWF queuing [31](#)
Cisco ITP Signaling Gateway [25](#)
CMTS [26](#)
Communications Assistance for Law Enforcement Act [27](#)
component interoperability [53](#)

components

 hardware [25](#)
 identifying [23, 24](#)
 role in the solution [25](#)
 software and release levels [25](#)
congestion avoidance [31](#)
core routing [27](#)
core switching layer [30](#)
CPE layer [30](#)

D

data tables [40](#)
DHCP [36](#)
DiffServ-compliant WRED [31](#)
DNS [36](#)
DOCSIS
 architecture [30](#)
 DQoS [31](#)
 DSA messages [31](#)
 DSC messages [31](#)
 HFC network [26](#)
 service flows [32](#)
documentation
 DVD [4](#)
 obtaining [4](#)
DQoS
 DOCSIS [31](#)
 PacketCable [31](#)
 PacketCable gates [32](#)

E

embedded multimedia terminal adapter [26](#)

H

HFC network [29](#)

I

ICMP [37](#)

Information System

 About [3, 61](#)

 secondary browser window [3, 62](#)

 Tips [3, 62](#)

 Types of Topics [3, 61](#)

intelligence

 call control [25](#)

 call feature [25](#)

interactive voice response [30](#)

interoperability

 billing mediation [30](#)

 IVR [30](#)

 voice-mail [30](#)

IP precedence value

 bearer traffic [31](#)

 data traffic [31](#)

 signaling traffic [31](#)

J

jitter [31](#)

L

latency [31](#)

lawful intercept [27](#)

layer

 aggregation [30](#)

 core switching [30](#)

 CPE [30](#)

 network management [30](#)

 trunking [30](#)

low-latency queuing [31](#)

M

MDRR queuing [31](#)

media

 gateway [26](#)

 controller [25, 30](#)

 server [27](#)

MGCP [29](#)

N

Network Information Data Sheet [29](#)

network management [28, 30](#)

NIDS [29, 35](#)

O

obtaining

 additional publications and information [7](#)

 documentation [4](#)

 technical assistance [6](#)

P

PacketCable

- architecture [23, 30](#)
- DQoS [31](#)
- event message data [27](#)
- gates for DQoS [32](#)
- lawful intercept architecture [27](#)
- parameters, MTAs [41](#)
- protocol standards [27](#)
- security measures [32](#)
- specifications [29, 30](#)
- standards [29](#)

PDU [36](#)

protocols

- DHCP [36](#)
- ICMP [37](#)
- MGCP [29](#)

Q

QoS

- design [31](#)
- G.114 Standard [31](#)

queue depth [31](#)

queuing

- CBWF [31](#)
- depth [31](#)
- low-latency [31](#)
- MDRR [31](#)

Rrecord keeping server [27](#)redundancy [23, 28](#)RKS [27](#)

Roles

- All [2](#)
- Installer [1](#)
- Network Administrator [1, 2](#)
- Network Architect [1](#)
- Network Operator [2](#)

Ssecondary browser window [3, 62](#)

security

- association [32](#)
- ciphersuite negotiation [33](#)
- Cisco BTS 10200 features [33](#)
- IPsec ESP [32](#)
- media [33](#)
- PacketCable measures [32](#)
- signaling [32](#)

servers

- announcement [27, 30](#)
- application [27](#)
- application, Cisco BTS Softswitch [36](#)
- CALEA-compliant [27](#)
- call management [25, 30](#)
- media [27](#)
- record keeping [27](#)
- terminal [36](#)
- voice-mail [27](#)

signaling gateway [25](#)

site

- preparation [23, 28](#)
- survey [23, 29, 35](#)

SS7 interconnectivity [25](#)

T

terminal server [36](#)

Topics

Doing [3, 61](#)

Overview [3, 61](#)

troubleshooting

model [53](#)

network problems [55](#)

symptoms [53](#)

system problems [56](#)

V

VLANs [37](#)

voice-mail

server [27](#)

systems [30](#)

VoIP systems [23](#)

W

WRED [31](#)

DiffServ-compliant [31](#)