Cisco Systems

Cisco Broadband
Local Integrated Services Solution for T1/E1
Design and Implementation Guide

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Cisco BLISS for T1/E1 Design and Implementation Guide

Preface

This preface describes the objectives, audience, organization, and conventions of the *Cisco Broadband Local Integrated Services Solution for T1/E1 Design and Implementation Guide*. It also refers you to related publications and describes online sources of information.

Document Objective

This guide is designed to help you plan, install, configure, and provision the Cisco Broadband Local Integrated Services Solution (BLISS) Release 4.0 for T1/E1. It describes the methods and procedures for initial planning, site preparation, hardware installation, and software configuration with the focus on the Cisco equipment used in the solution.

Audience

This guide is intended for the following audience:

- Network designers who have experience with telecommunications networks, protocols, and equipment, as well as experience with data communications networks, protocols, and equipment.
- Network operators and administrators who have experience in telecommunications networks, protocols, and equipment, as well as a familiarity with data communications networks, protocols, and equipment.
- Component installers who have experience installing telecommunications equipment and cables, as well as experience installing data communications equipment and cabling.

Document Organization

Table 1 describes the chapters in this guide.

Table 1 Chapters in This Guide

Chapter	Title	Contents
Chapter 1	Solution Overview	Overview of the Cisco BLISS for T1/E1 solution.
Chapter 2	Planning and Design	This chapter discusses elements of the Cisco BLISS for T1/E1 design that should be considered before the solution is deployed.
Chapter 3	Security Recommendations	This chapter describes significant threats to service that can occur from the untrusted portion of the Cisco BLISS for T1/E1 network. It also describes the solutions to manage those security threats.
Chapter 4	Voice Traffic Engineering	This chapter describes the traffic engineering needed to support the voice application, including a section covering Internet data traffic engineering.
Chapter 5	Configuring the Solution	This chapter covers provisioning of the individual components of the Cisco BLISS for T1/E1 architecture where those configurations are unique to the Cisco BLISS for T1/E1 solution.

Document Conventions

Command descriptions use the following conventions:

boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A string is a nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Screen examples use the following conventions:

`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.
italic screen font	Arguments for which you supply values are in *italic screen* font.
⟶	This pointer highlights an important line of text in an example.

^	The symbol ^ represents the key labeled Control. For example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Documentation Suite

The documents that make up the Cisco Broadband Local Integrated Services Solution for T1 documentation set are listed in Table 2.

Table 2 Cisco Broadband Local Integrated Services Solution for T1 Documentation

Functional Area	Publication	Description and Audience
Troubleshooting	*Cisco Broadband Local Integrated Services Solution for T1/E1 Troubleshooting Guide*	Helps you troubleshoot the Cisco Broadband Local Integrated Services Solution for T1/E1. This guide is intended for the following audience: • Component installers who have experience installing telecommunications equipment and cables, as well as data communications equipment and cabling. • Network operators and administrators who have experience in telecommunications networks, protocols, and equipment, as well as a familiarity with data communications networks, protocols, and equipment.

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/univercd/home/home.htm

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

Documentation DVD

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

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/

Cisco Marketplace:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical 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
- Nonemergencies—psirt@cisco.com

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 that has the most recent creation date in this public key server list:

http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on

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

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

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support 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, 365 days a year, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support 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 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 TAC 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 TAC 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.

- 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

- Cisco Marketplace provides a variety of Cisco books, reference guides, 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

- *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

- 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

Solution Overview

Note The product name of this solution is the "Cisco Broadband Local Integrated Services Solution (BLISS) for T1/E1." In the interest of brevity, in this document it is referred to as the "Cisco BLISS for T1 solution." All references to T1 apply equally to E1 configurations except where otherwise stated.

The Cisco Broadband Local Integrated Services Solution (BLISS) framework enables service providers primarily focused on serving their subscriber base via traditional high-speed access to deliver complete integrated services. The Cisco BLISS for T1 solution delivers packet voice and data services over a traditional T1 infrastructure. Using existing access lines, the Cisco BLISS for T1 solution allows service providers to offer a bundle of packet-based services including local and long-distance voice services and high-speed data. By providing multiple services over a common infrastructure, carriers can increase their revenue and profits, while simultaneously offering small and medium-sized business customers a better telecommunications value.

The Cisco BLISS for T1 solution uses MGCP-based centralized call-control architecture and uses an IP core for packet transport to team the Cisco BTS 10200 Softswitch with Cisco gateways to create a virtual switch network. The Cisco BTS 10200 has SIP and H.323 signaling interfaces for interconnection with SIP and H.323 voice networks. In addition, support for SIP endpoints is provided on the Cisco 7960, 7940, 7912, and 7905 IP phones.

This chapter includes the following sections:

Cisco BLISS Solution Architecture

There are currently three architectures for the Cisco BLISS solutions: Cable, Metro Ethernet, and T1. All three architectures are similar in terms of the backend components such as the Cisco BTS 10200, media gateways, and the core routing and switching components. Where they differ is in the access delivery method.

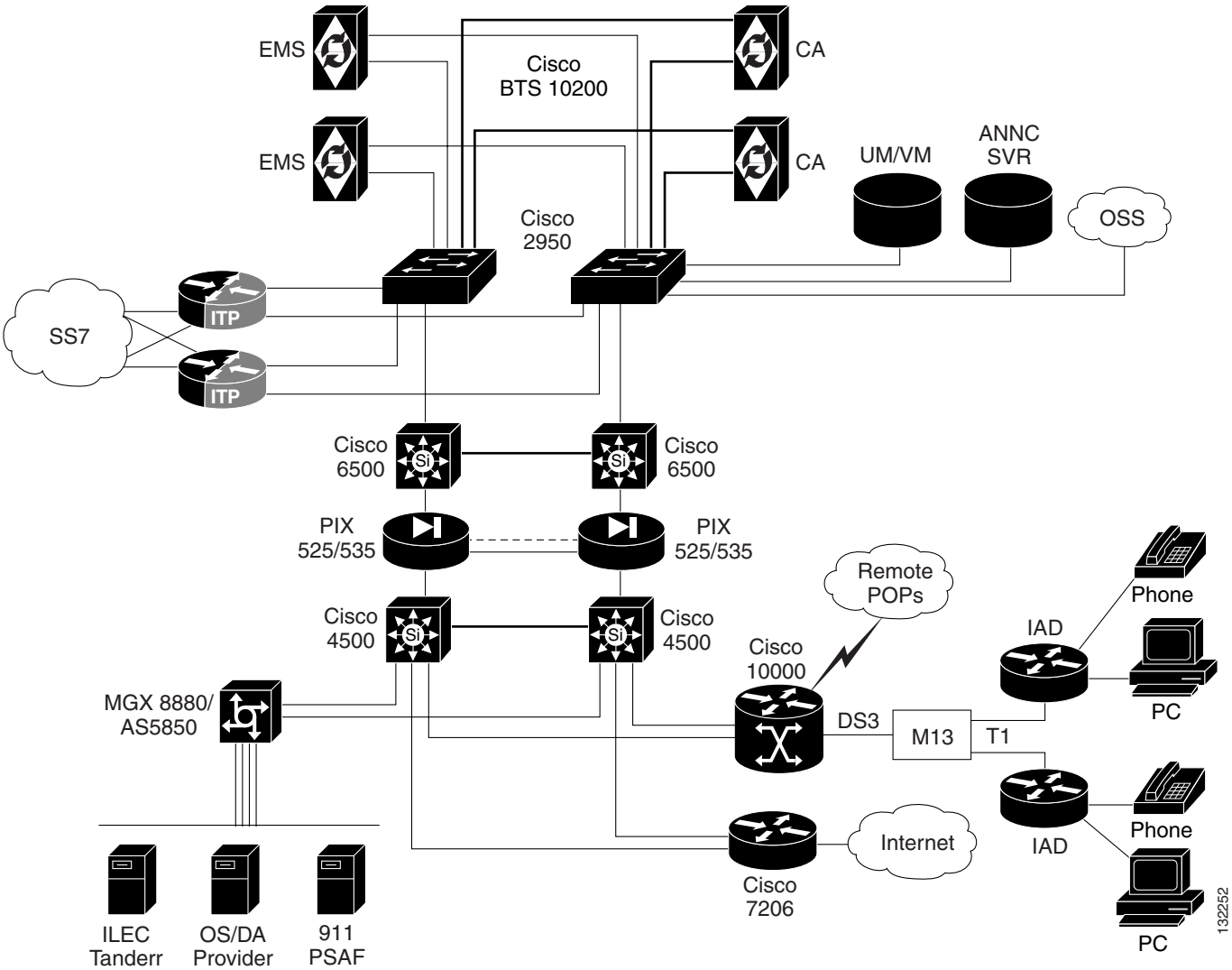
- The Cisco BLISS for Cable version of the solution provides voice access via an embedded Media Termination Adapter (eMTA) at the customer premises with Cable Modem Termination Systems (CMTSs) used in the POP for customer traffic aggregation.
- The Cisco BLISS for Metro Ethernet solution extends Ethernet to the customer premise where a Cisco Integrated Access Device (IAD) is used to provide the interfaces to the voice network. Aggregation is provided by a switching platform such as the Catalyst 6500/7600.

- The Cisco BLISS for T1 solution provides a T1 connection from the service provider POP to the customer premises where an IAD2420/2430 is used to provide the voice interfaces to the service provider's network. In the POP the Cisco 10000 router is used to aggregate T1s from customer locations as well as provide QoS, routing, and packet replication services for CALEA.

This document focuses on the Cisco BISS for T1 solution. The Cisco BLISS for Cable and Cisco BLISS for Metro Ethernet solutions are beyond the scope of this document and are covered in documentation dedicated to those technologies.

Figure 1-1 illustrates the Cisco BLISS for T1 solution architecture.

Figure 1-1 Cisco BLISS for T1 Solution Architecture



Cisco BLISS for T1 Solution Components

This section describes the following components of the Cisco BLISS for T1 solution:

Cisco BTS 10200 Softswitch

The Cisco BLISS for T1 solution uses the Cisco BTS 10200 Softswitch as a Call Agent (CA). Call Agent hosts used in this version of the solution are Sun-based platforms consisting of the Sun 240, Sun 440, and Sun 1280 platforms. The Call Agent application is active on only one Call Agent host platform at a time, and switches to the standby Call Agent host platform under failure conditions. The result is that Call Agent host failure and switchover events are invisible for established calls. Calls in the process of being set up during the switchover event cannot be preserved and must be reattempted. The Call Agent includes a scalable, open host that provides SIGTRAN interfaces, alarms, and a reliable IP link between the Call Agent and media gateways. The following sections provide detailed Call Agent specifications for Sun-based systems.

Logical Components

The Cisco BTS 10200 Softswitch consists of five independent logical components in a distributed architecture:

- **Call Agent (CA)**—Serves as a call management system (CMS) and media gateway controller (MGC). It handles the establishment, processing, and teardown of telephone calls.
- **Feature Servers (FSs)**—Provide POTS, Tandem, Centrex, and Advanced Intelligent Network (AIN) services to the calls controlled by the CAs. The FSs also provide processing for service features such as call forwarding, call waiting, local number portability, and so forth.

  There are two types of FSs in the Cisco BTS 10200 Softswitch:

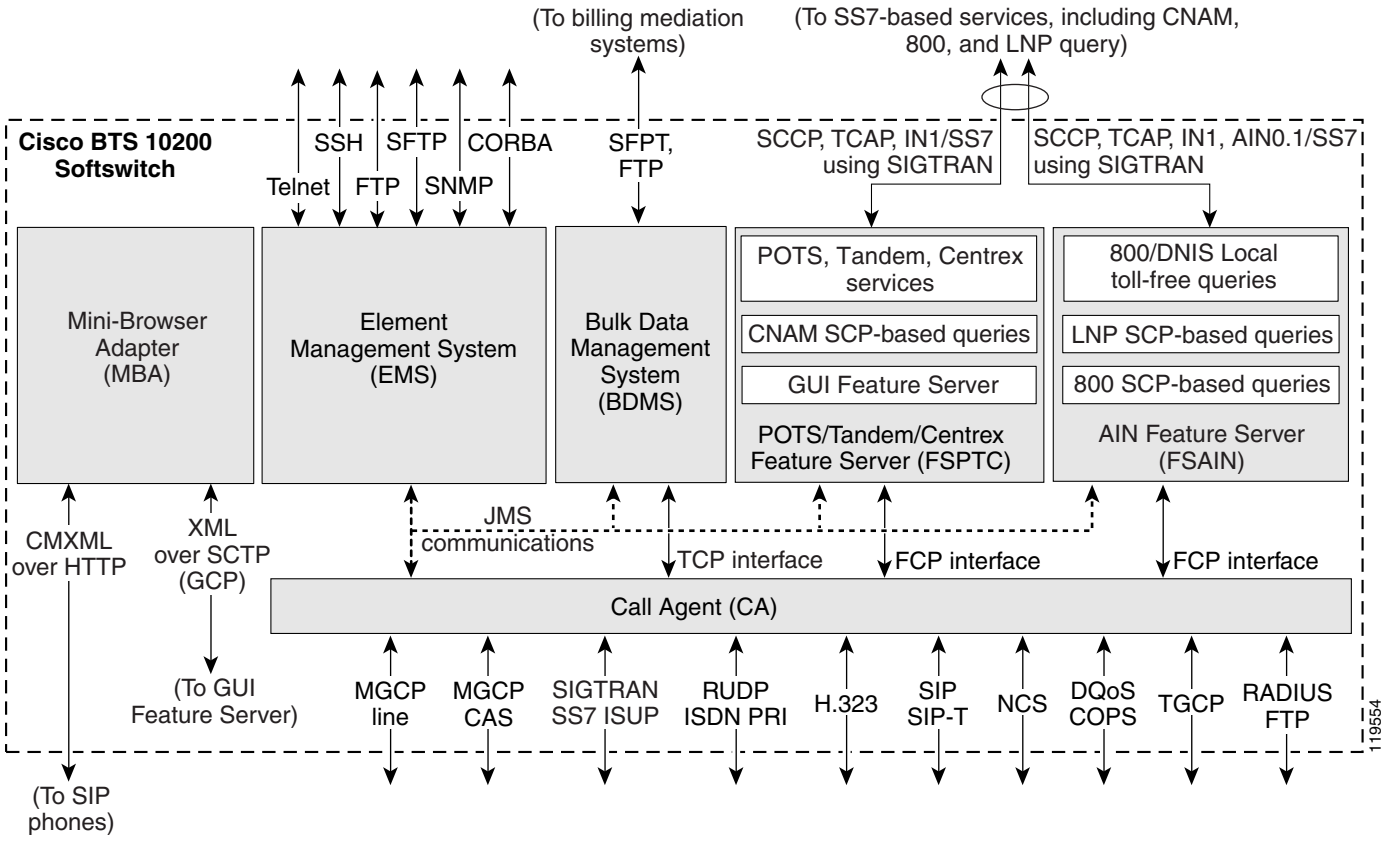
  - FSPTC—FS for POTS, Tandem, and Centrex features
  - FSAIN—FS for AIN services

- **Element Management System (EMS)**—Controls the entire Cisco BTS 10200 Softswitch and acts as a mediation device between a network management system (NMS) and one or more CAs. It is also the interface for the provisioning, administration, and reporting features of the Cisco BTS 10200 Softswitch.
- **Bulk Data Management System (BDMS)**—Coordinates the collection of billing data from the CA, and the forwarding of billing records to the service provider billing mediation device.
- **Mini-Browser Adapter (MBA)**—Performs GUI management for GUI-enabled SIP phone handsets; this GUI allows SIP phone users to self-provision certain features. The MBA runs on a separate Sun host machine that is not part of the standard Cisco BTS 10200 Softswitch hardware set.

This section describes the functions provided by each of the logical components of the Cisco BTS 10200 Softswitch. The information is organized as follows:

The architecture and interworking of the logical components (CA, FS, EMS, BDMS, and MBA) are shown in Figure 1-2.

Figure 1-2 Cisco BTS 10200 Softswitch Architecture, Showing Logical Components



CA Functions

The Call Agent (CA) provides monitoring and control of external network elements (NEs). It connects to multiple networks through the signaling adapter interface (see Figure 1-2). This interface converts incoming and outgoing signaling to and from the standard internal messaging format of the CA. This interface allows the CA to connect to multiple networks and exchange signaling messages for setup, teardown, and transfer of calls.

Signaling Adapter Interface

The signaling adapter interface performs the following functions:

- Uniform primitives (signaling indications) for all interactions between different protocol stacks and the CA modules.
- Uniform data structures containing common information elements from different signaling protocols.
- Call control primitives for exchanging call signaling messages between CA and the signaling network.
- Maintenance primitives for signaling link hardware maintenance and signaling protocol stack provisioning.

Billing Data Generation and Interfaces

The CA supports the following billing data generation methods:

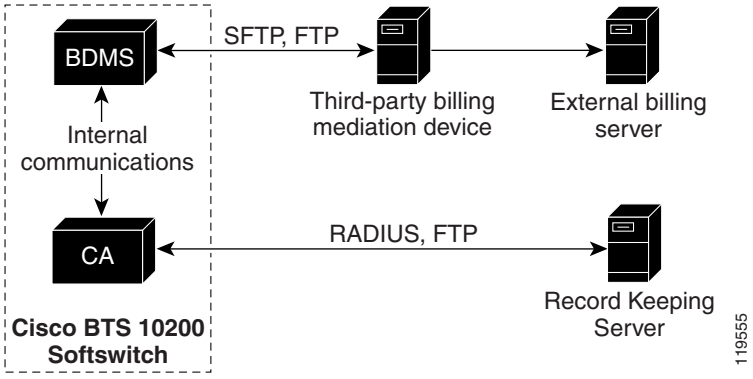
- Call detail blocks (CDBs)—Traditional post-call billing data, which the CA sends via internal communications to the BDMS (see Figure 1-3). The BDMS forwards this data via FTP or SFTP (a provisionable option) to a third-party billing mediation device. For additional information on the BDMS, see the "BDMS Functions" section on page 1-8.
- PacketCable event messages (EMs)—Real-time call data flow, which is transferred directly from the CA to a Record Keeping Server (RKS) that assembles call detail records (CDRs) from the EMs.

  The following billing interfaces are provided for EMs on the CA (see Figure 1-3):

  - RADIUS—Used by the CA to transmit EMs automatically to an external RKS
  - SFTP—Used for manual transfer of EMs from the CA to the RKS

Note PacketCable EMs are used for billing only in the Cisco BLISS for Cable solution.

Figure 1-3 CA Billing Interfaces



FS Functions

There are two different types of Feature Servers (FSs) in the Cisco BTS 10200 Softswitch.

- FSPTC—FS for POTS, Tandem, and Centrex features
- FSAIN—FS for Advanced Intelligent Network services

Each FS communicates internally with the CA, and externally (via a signaling gateway) with signal transfer points (STPs) that are part of the SS7 signaling system. Note that although it is technically possible to place the Feature Servers and Call Agent on physically separate servers, we recommend they be installed on the same physical server.

The FSs provide access to features through a well-defined interface. The Cisco BTS 10200 Softswitch architecture logically separates the FSs (which provide feature control) from the CA (which provides call control) with a clear interface—Feature Control Protocol (FCP)—defined between them. The FSs provide support for POTS, Centrex, AIN, 8XX service, and other enhanced services. The FSs are colocated on the same machine as the CA.

An FS is invoked from a call detection point (DP) in the CA. For each DP, the CA checks if any triggers are armed. If a trigger is armed, the CA checks if the trigger applies to the subscriber, group, or office (in that order). If the trigger is applicable, the CA invokes the FS associated with that trigger. The Cisco BTS 10200 Softswitch call processing mechanisms are based on the ITU CS-2 call model.

The FSAIN supports the automatic call gap (ACG) function for communications with a service control point (SCP). When an SCP sends a message to the FSAIN regarding the allowed query rate, the Cisco BTS 10200 Softswitch adjusts its query rate accordingly.

EMS Functions

The Element Management System (EMS) manages all of the Cisco BTS 10200 Softswitch components and provides operations, administration, maintenance, and provisioning (OAM&P) interfaces for monitoring and control. It provides the following user OAM&P capabilities:

- Access the system via a secure interface.
- Perform system administration and security functions.
- Show, add, change, or delete the database information through a local or remote interface.
- Display reports of events, alarms, and faults.
- Monitor and manage hardware.
- Monitor and manage traffic measurements.
- Monitor and manage queuing and audit functions.
- Display and control the status of a component.

The internal database contains the provisioned data for basic call processing, billing, and special call features. Key data structures are stored in shared memory and are accessible to any process in the system. A library of read/write locks controls access to shared memory. The data structures are implemented using Oracle in the EMS/BDMS, and an indexed database (IDX) in the CA/FS.

The EMS provides a flexible mechanism to transport information over any protocol to any external device. The EMS interface design takes into account that each carrier has its own unique set of Operations Support Systems (OSSs). The EMS provides a decoupling layer between the external protocols used within the service provider network and the internal protocols of the Cisco BTS 10200 Softswitch. The core system does not need to interpret the specific data formats used by the other carrier network elements.

EMS Communications

Operators, network administrators, and end users can communicate with the EMS from their workstations or PCs over the interfaces shown in Figure 1-4.

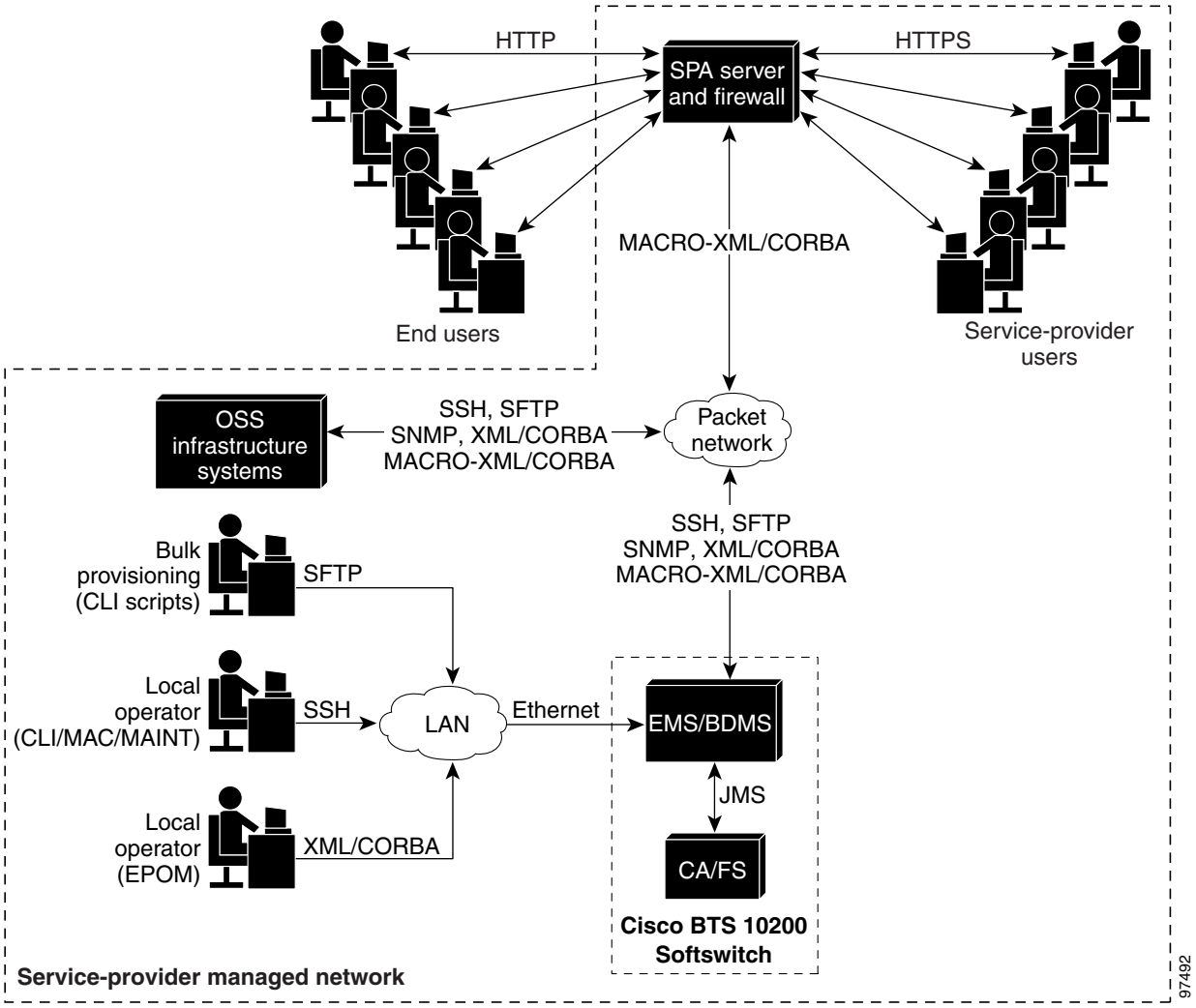
The user interfaces include the following:

- Secure shell (SSH)—For provisioning via CLI and Maintenance (MAINT) shells.
  - CLI shell—Used for entering entire commands and their parameters from the command line.
  - MAINT shell—Provides a maintenance interface for CLI commands that does not time out or disconnect on switchover. It supplies a prompt based on the username.
- Secure File Transfer Protocol (SFTP)—for bulk provisioning sessions. SSH and SFTP are always available on the Cisco BTS 10200 Softswitch, and there is no command to turn them off.
- XML/CORBA and MACRO-XML/CORBA support the following:
  - CORBA provisioning and monitoring interface
  - Provisioning via the Cisco Extensible Provisioning and Operations Manager (EPOM) and the Cisco Self-Service Phone Administration (SPA)
  - CORBA over SSL for communications with the Cisco BTS 10200 Softswitch
- Simple Network Management Protocol (SNMP)—Provides traps, status, control, and measurement functions, and provisionable community strings.

  The Cisco BTS 10200 Softswitch SNMP agent provides the following functions:
  - Collection of statistics and traffic management data
  - Status and control
  - SNMP trap reports
  - Bulk status and control

  The SNMP agent supports SNMPv2c operations defined by the opticall.mib Management Information Base (MIB). The MIB is located in the directory /opt/BTSsnmp/etc on the EMS. The NMS needs to load the main MIB (opticall.mib) that will in turn import three other MIBs—IPCELL-TC, SNMPv2-TC, and SNMPv2-SMI. The main MIB uses variables from these MIBs.
- Hypertext Transfer Protocol (HTTP) and Secure Hypertext Transfer Protocol (HTTPS)—Permits end users and service providers to perform many of the feature provisioning processes via the web-based Cisco SPA system. Access from the user's web browser to the SPA server is via HTTP. Access from the service provider's web browser is via HTTPS.

Figure 1-4 Preferred EMS Management Interfaces for Service Provider and End Users



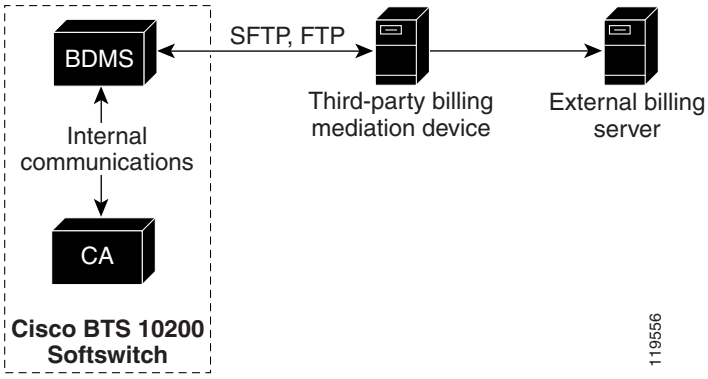
BDMS Functions

The Bulk Data Management System (BDMS) stores billing data in the form of call detail blocks (CDBs). CDBs are assembled from billing messages generated in the CA when billing-related call events occur during call processing. The BDMS formats the CDBs into a flat ASCII-file format, and transmits them to an external billing collection and mediation device that is part of the service provider billing system (see Figure 1-5). Finally, the BDMS forwards this data to an external billing mediation system or billing server, where it is assembled into CDRs.

The BDMS provides the following billing functions:

- Supports batch record transmission via FTP and SFTP.
- Issues events as appropriate including potential billing data overwrites.
- Saves billing data records in persistent store—the allocated storage space is provisionable using CLI commands and can range from 10 MB to 5 GB (default 1 GB).
- Supports user-provisionable billing subsystem parameters.
- Supports on-demand CDB queries based on file name, time interval, call type, service type, termination cause, terminating number, originating number, or last record(s) written.

Figure 1-5 Billing Interface to the BDMS



MBA Functions

SIP phones interface via the IP network with the Mini-Browser Adapter (MBA) for services. The user accesses service functions via the "services" key on the SIP phone. A GUI on the SIP phone allows users to self-provision certain features. The MBA supports these services and performs GUI management for the GUI-enabled SIP-phone handsets.

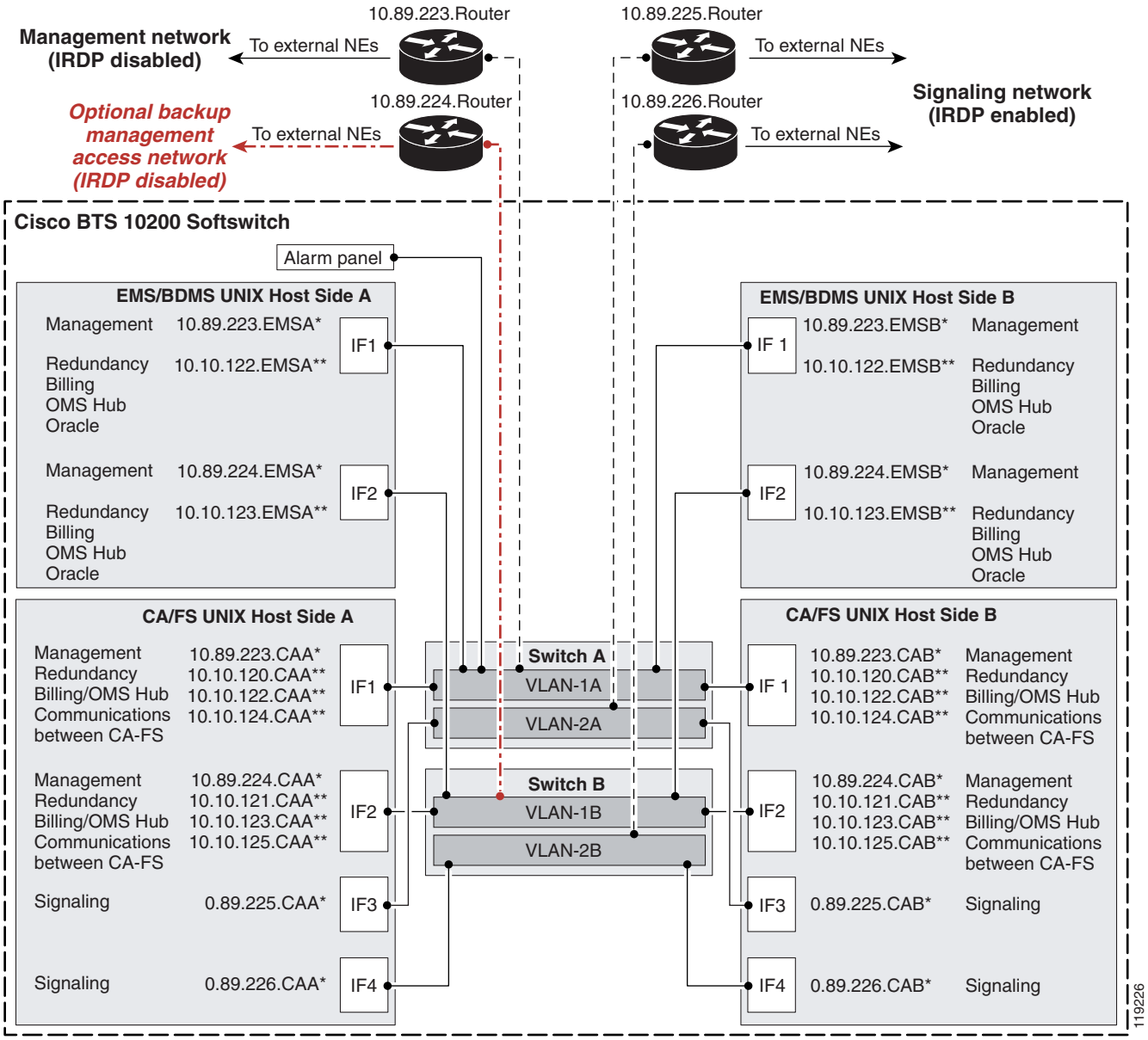
The Cisco BTS 10200 Softswitch architecture illustrated in Figure 1-2 on page 1-4 shows the MBA and its interfaces:

- The MBA interfaces with the GUI feature server (GFS) in the FSPTC. The GFS is the feature server data access component for GUI management, and is responsible for subscriber data access and northbound updates into the EMS. Internal signaling between the MBA and the GFS is via GUI Control Protocol (GCP), which is an XML-based protocol over SCTP links.
- Signaling between the MBA and SIP phones uses Cisco CMXML protocol over HTTP.

Reliability and Availability of Components

The Cisco BTS 10200 Softswitch network configuration is shown in Figure 1-6. This configuration provides redundant host machines for the EMS/BDMS and CA/FS components, redundant management local area networks (LANs), and six interfaces to the external routers. The configuration enhances security by separating management traffic from signaling traffic. As shown in the drawing, the service provider has the option of installing a backup management access network.

Figure 1-6 Cisco BTS 10200 Softswitch Network Configuration



Notes for Figure 1-6:

1. The following labels represent specific components and functions:
   - IF = Interface
   - A* and B* represent physical IP addresses; A** and B** represent logical IP addresses
   - Signaling: MGCP, SIP, and H323 use dynamically assigned logical IP addresses associated with this interface
   - OMS Hub carries internal communications

2. “To external NEs" refers to the following links in the service provider network:
   - Uplinks for external access to hosts, used for management services (via SSH, SFTP, and so forth), DNS services, and outbound billing data (via FTP or SFTP).
   - Uplinks for external communications, used for connection to external NEs via an IRDP-enabled network.
3. To support full system redundancy, you must connect the external uplinks from the Catalyst switches to separate routers (6500s) as shown in Figure 1-6:
   - There must be dual (redundant) signaling uplinks from each Catalyst switch, so that each Catalyst switch is connected to each router (6500) providing connectivity for the signaling network.
   - There must be a single management uplink from Catalyst Switch A to one of the management routers. A second management uplink, from Catalyst B to the other management router, is optional. A consequence of the second “optional” management network is that BTS installation still creates this interface and puts it into the hosts table with a 10.89.x.x address, and that has to be there. In DNS, however, you only have to put one entry for the management network “broker”
   - The routers must be connected to separate networks with diverse routing paths to the applicable external NEs and services (such as OSS, DNS, media gateways, and announcement servers).
   - IRDP must be disabled on the primary and secondary EMS server interfaces.
4. It is important to ensure redundancy of the DNS lookup function, so that this function is not completely lost in the event of a network outage. We recommend that two (redundant) DNS units be deployed in the service provider network, and that the two DNS units be reachable via separate networks with diverse routing paths. We also recommend that you place the DNSs behind a load balancer so that a single IP address is exported to clients such as the Cisco BTS 10200 Softswitch.
5. The alarm panel refers to a terminal server (which could be a terminal server built into an alarm panel). It could be customer supplied or Cisco supplied, depending on the hardware options selected. The alarm panel supplied with some Cisco BTS 10200 Softswitch systems is not used for alarms or for aggregation or reporting of machine alarms, but rather is used as a form of terminal concentrator. The Cisco BTS 10200 Softswitch software does not transmit machine alarms through this port. Instead, machine alarms are sent via alarm reports, as described in the *Cisco BTS 10200 Softswitch Operations and Maintenance Guide*.

Dual Active/Standby Configuration

Note This section is applicable to the EMS, BDMS, CA, and FS components, but not the MBA component. The MBA is not deployed in a dual configuration.

Each logical component (EMS, BDMS, CA, and FS) is deployed in a dual active/standby configuration, with the two sides running on separate computers (hosts). The active side of each component is backed up by a standby side on the other host. The communication paths among the components are also redundant. The redundant architecture supports the reliability and availability of the entire system. The active and standby sides of each logical component pair operate as follows:

- There is no traffic load sharing between the active and standby sides; the active side performs all of the call processing, and the standby does none.
- Call and feature data from the active side are replicated to the standby side at specific checkpoints of a call (when a call is answered, released, and so forth).

- An automatic internal audit function runs on the standby side of each component—EMS, BDMS, CA, and FS. It checks all the shared memory tables in the components to verify consistency and to check for any corruption. The audit reports any data structure inconsistencies or corruption via alarms and trace messages.
- Each side maintains a keepalive channel with the corresponding mate side. The keepalive process on each side determines if the mate is faulty. If there is a failure on the active side (or if the operator intentionally brings down the active side), the other side becomes active and takes over the traffic load. All stable calls continue to be processed without any loss of calls. There is no service outage, but during a switchover, transient calls can be impacted.
- IP Manager, a built-in IP management function, provides logical interfaces to several signaling protocol components (such as MGCP, H.323, SIP) for remote devices on the currently active CA/FS. If IP Manager detects a CA/FS platform failover (from primary to secondary or vice-versa), it migrates the IP addresses of the logical interfaces over to the newly active CA/FS side.
- The operator can manually switch (force) either side to become active, which automatically forces the other side into standby mode.

Process Restartability

When a Cisco BTS 10200 Softswitch process exits due to an internal error (such as SIGSEGV on UNIX) or is terminated by the platform, the system automatically restarts the process that shut down. Restarting the process is a preferred alternative to switching over to the mate, because the restart preserves stable calls and also attempts to preserve transient calls. When a process is restarted, the process audits information such as resource states and attempts to repair inconsistencies. If a process experiences a high failure rate (even after repeated restarts), the system will switch over to the mate.

Additional information regarding the Cisco BTS 10200 Softswitch can be found at http://www.cisco.com/en/US/products/hw/vcallcon/ps531/index.html

Cisco ITP Signaling Gateway

Prior to the Cisco BTS 10200 Softswitch Release 4.x, the interface to the SS7 network was via a pair of SS7 termination cards inserted in the Cisco BTS 10200 chassis. Although serviceable, these SS7 cards had limitations that have now been addressed with the addition of the Cisco IP Transfer Point (ITP) as the Signaling Gateway for the Cisco BTS 10200. These limitations included scalability, flexibility, redundancy, serviceability, and support for open standards. The ITP addresses all of these issues with proven technology and a carrier class system.

The ITP was introduced to the Service Provider market in 2001 and is deployed globally with great success. As currently deployed, the ITP supports functionalities that include STP, Signaling Transport over IP and ATM, and Signaling Gateway for Next Generation end nodes like SSP and SCP. The ITP is certified by Telcordia as an ANSI STP, is completely open-standards based, and provides STP-class availability. The ITP is offered on multiple platforms and can scale from 4 links up to 800 links. e Table 1-1 highlights the ITP models and capacities.

Table 1-1 Cisco ITP Models and Capacities

Cisco ITP Model	Dual Power	Dual Processor	Hot-Swap Line Cards	Max SS7 Low Speed Links	Max SCTP Link Associations	Max T1/E1 Ports
2651XM	Yes	No	No	4	100	4
7200VXR (NPE 400)	Yes	No	Yes	24	1000	48
7301	Yes	No	Yes	48	1000	8
7507	Yes	Yes	Yes	240	1000	80
7513	Yes	Yes	Yes	800	1000	176

Additional information regarding the Cisco ITP can be found at http://www.cisco.com/en/US/products/sw/wirelssw/ps1862/index.html.

Cisco Catalyst 6509

The Catalyst 6509 is a multilayer switching component. It provides high port density Ethernet/Fast Ethernet, Gigabit switching functions, and Layer 3 routing. In the Cisco BLISS for T1 solution, it is used to provide Layer 2 connectivity to the Cisco BTS 10200 and to provide Layer 3 functionality for routing signaling packets to the edge and trunking gateways. Figure 1-7 shows the Catalyst 6509 core router.

Note that the Catalyst 6509 is purely a data switch and that there are no features specific to this platform required to support Cisco BLISS for T1. Therefore other platforms such as the Catalyst 4500 that support IRDP and L2/L3 functionality could be used. In addition other configurations of the Catalyst 6500 could be used, such as the Catalyst 6506 with the appropriate supervisor module and line cards to meet density and traffic requirements.

Cisco Catalyst 4506

The Catalyst 4506 is also multilayer switching component. It provides high port density Ethernet/Fast Ethernet, Gigabit switching functions, and Layer 3 routing. In the Cisco BLISS for T1 solution, it can be used to provide L2/L3 connectivity to the Cisco BTS 10200 as well as remote POPs that do not have a BTS. Figure 1-8 shows the Catalyst 4506 router.

Note that as with the Catalyst 6509, this switch is purely a data switch and that there are no features specific to this platform required to support the Cisco BLISS for T1 solution. Therefore, other platforms could be used in a mated pair to provide redundancy.

Cisco Catalyst 2950-24

The Catalyst 2950-24 (Figure 1-9) is a Layer 2 switch that is deployed in a mated pair to provide redundant connectivity between the servers that comprise the Cisco BTS 10200. In addition, these switches provide the management and signaling interfaces to the Cisco BTS 10200. When the server hardware is purchased through Cisco, the 2950-24 switches are included. If the customer purchases the Cisco BTS 10200 server hardware through another vendor, they must purchase these switches separately.

Figure 1-7 Cisco Catalyst 6509

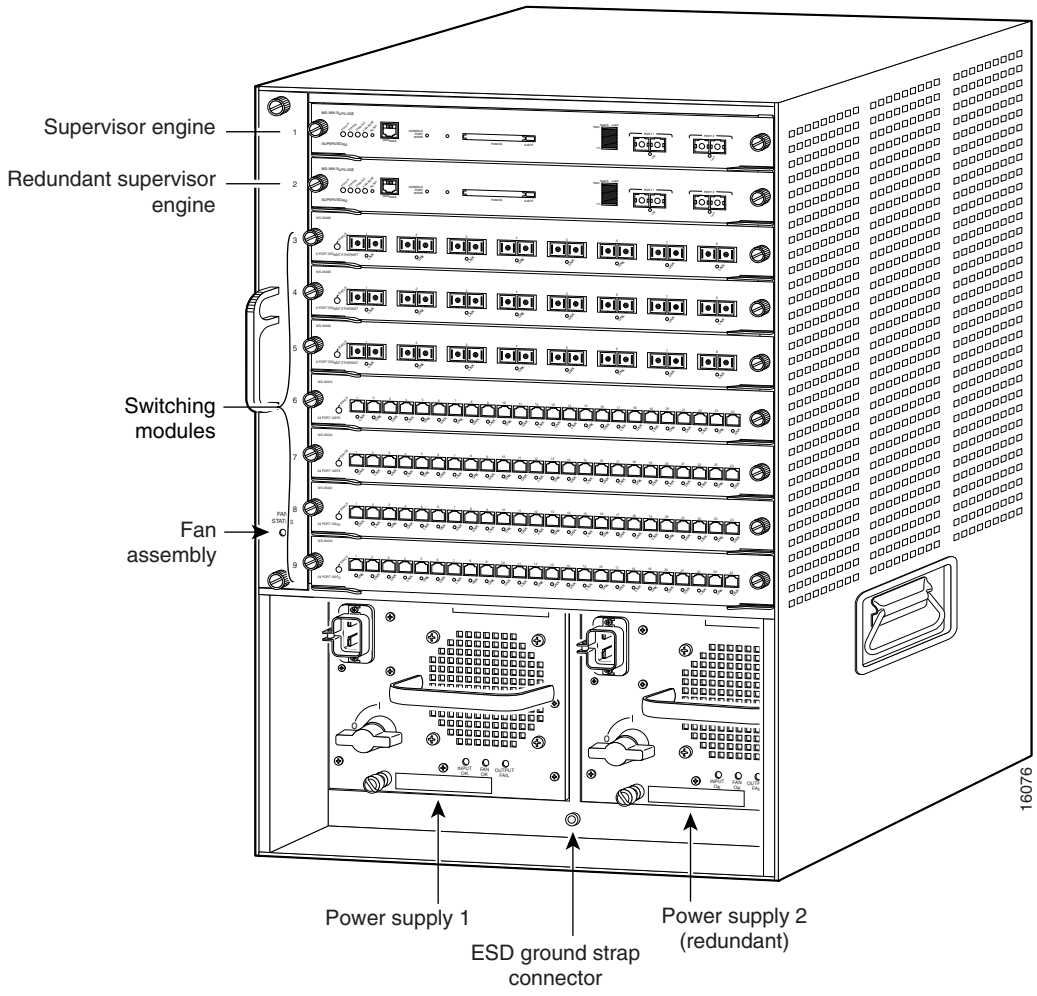


Figure 1-8 Cisco Catalyst 4506

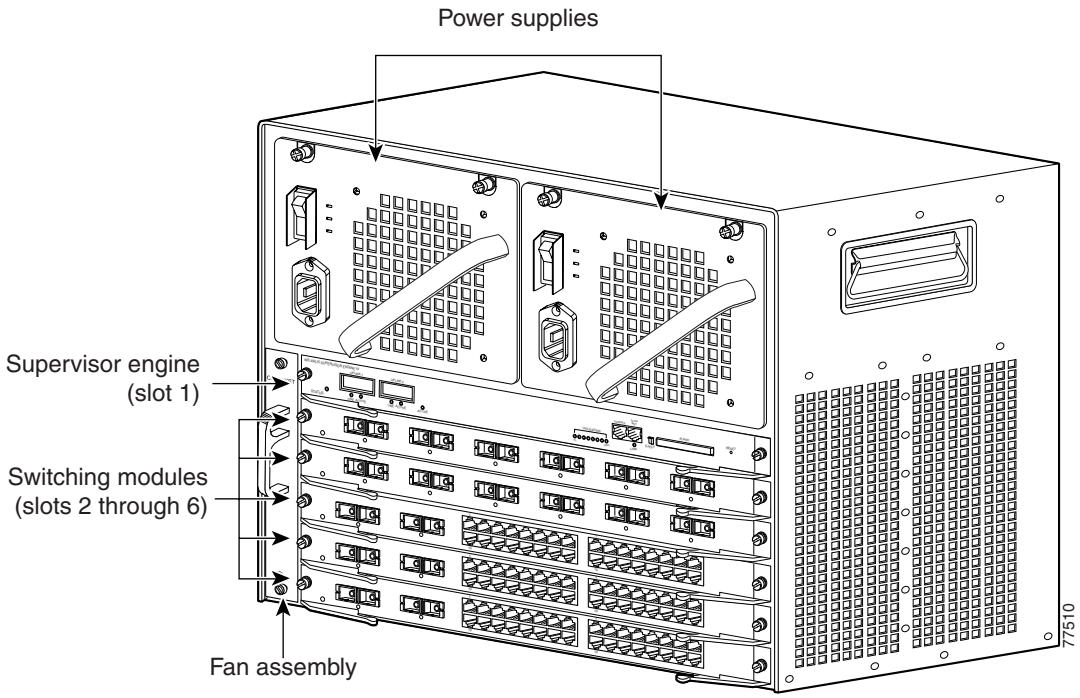
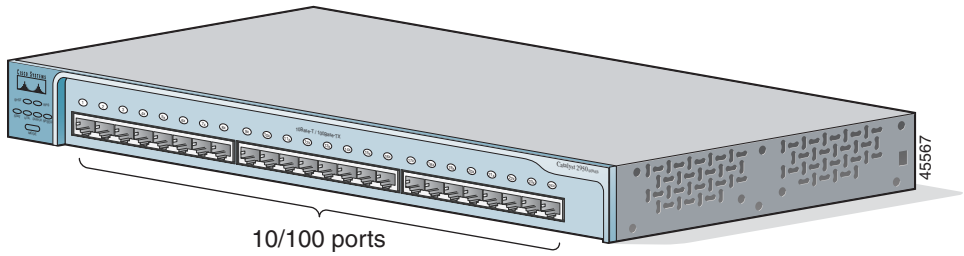


Figure 1-9 Cisco Catalyst 2950-24 Router



Cisco 10000 Edge Services Router

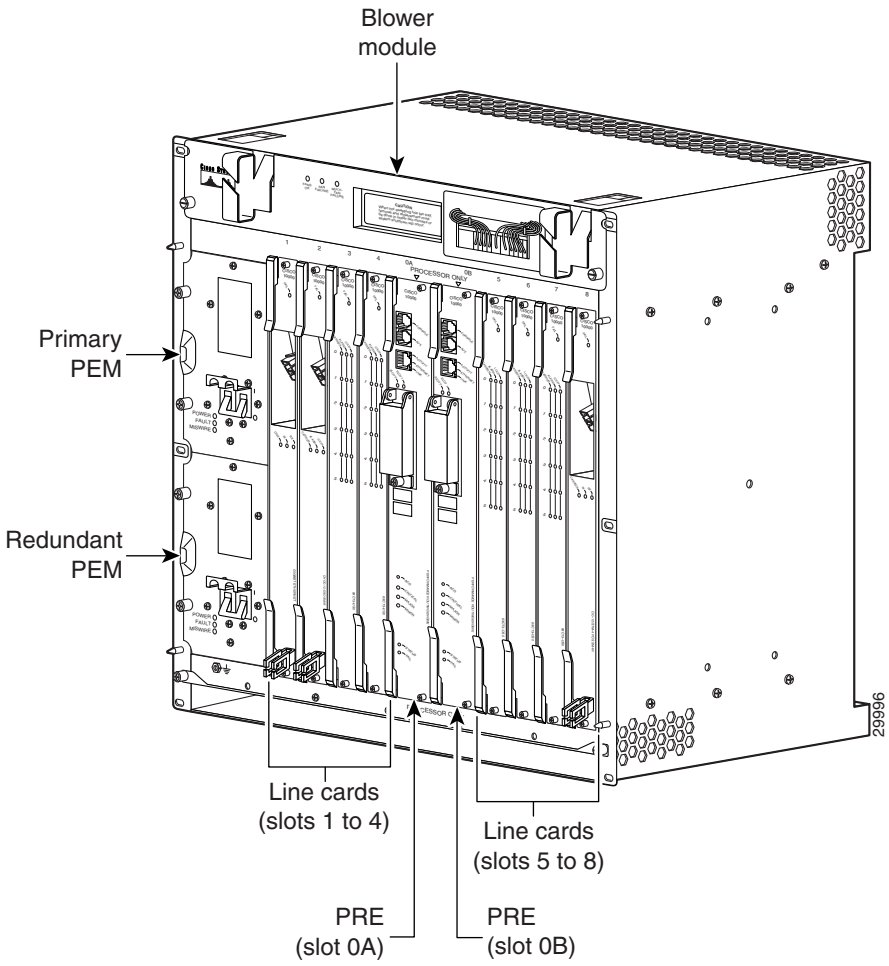
In the Cisco BLISS for T1 solution single or multiple T1 uplinks from customer premises equipment (CPE) are multiplexed into T3s and are aggregated at the Cisco 10000 Edge Services Router (ESR). The Cisco 10000 ESR is a Layer 3 platform that enables provisioning of IP QoS services, critical to maintaining voice quality, across thousands of leased-line and private line connections without performance degradation. The Cisco 10000 ESR accomplishes this by performing the application of QoS using Parallel Express Forwarding (PXF) hardware.

The Cisco IOS release used on the Cisco 10000 ESR is optimized for edge routing functions in the service providers networks. The software release includes a comprehensive set of standard features, including IP routing protocols, security services, and various commands to help configure and administer the router. In addition, this release supports advanced features, including quality of service (QoS), Multilink Point-to-Point Protocol (MLPPP), automatic protection switching (APS), and Communications Assistance for Law Enforcement Act (CALEA).

Cisco 10000 ESR Hardware

Figure 1-10 shows the layout of components in the Cisco 10000 ESR chassis.

Figure 1-10 Cisco 10000 ESR Chassis Layout



Deployment of the Cisco 10000 in the Cisco BLISS for T1 environment typically requires a combination of the following types of cards depending on the service provider environment.

Router Control

- Performance Routing Engine 1 (PRE1) line card providing centralized processing and up to 2.6 million packets per second performance.

CPE Aggregation

- Channelized T3 line card providing six T3 connections, each of which can be configured as full rate DS3, channelized DS3, DS1, and fractional DS1.
- Channelized OC-3 line card providing four OC-3 interfaces that can be configured as full rate DS3, channelized DS3, DS1, and fractional DS1.
- Channelized OC-12 line card providing one OC-12 interface that can be configured as full rate DS3, channelized DS3, DS1, and fractional DS1.

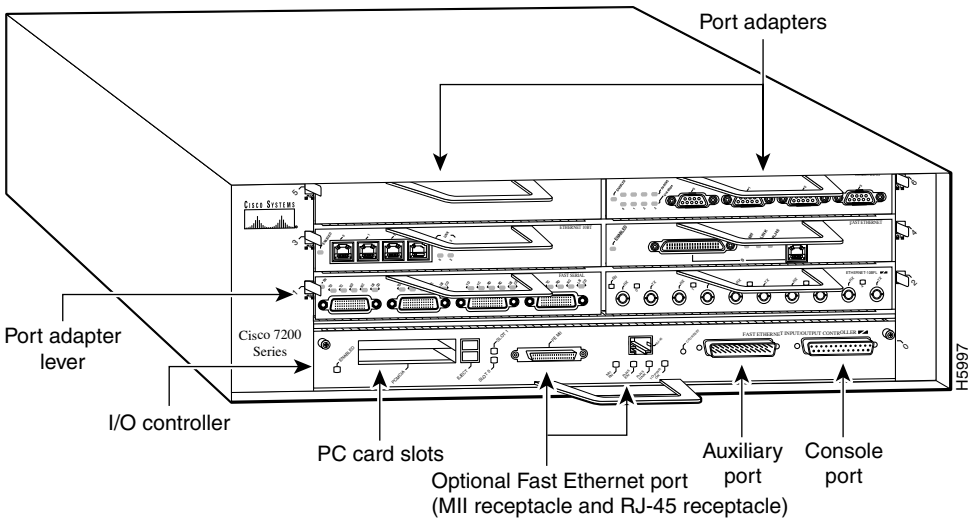
IP Backhaul

- Gigabit Ethernet line card providing one or two Gigabit Ethernet connections per slot.
- OC-12 Packet-over-SONET line card providing a single OC-12 connection.

Cisco 7200 ISP Connection Gateway

The Cisco 7200 ISP Connection Gateway (Figure 1-11) acts as the border router between the service provider network and the Internet. This router can deployed as a mated pair connected to two different Internet providers to provide redundancy or a single router if redundancy is not required or another POP's Internet connection will be used as a backup. Configuration of the router will vary depending on the interfaces required to connect to the Internet provider's network.

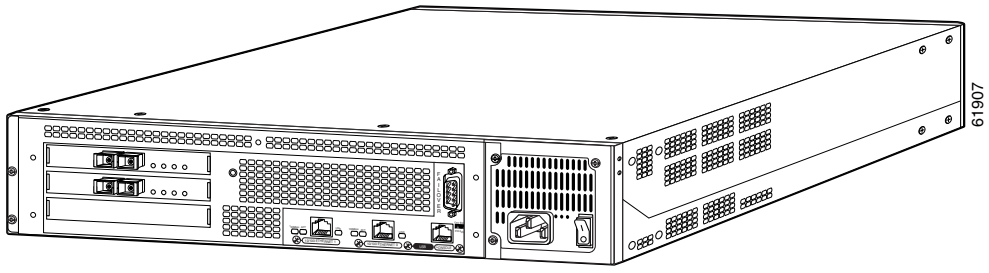
Figure 1-11 Cisco 7200 ISP Connection Gateway



Cisco PIX Firewall

Cisco PIX Firewalls (Figure 1-12) provide advanced security services for multimedia and voice standards, including H.323 Version 4, SIP, Cisco Skinny Client Control Protocol, RTSP, and MGCP. The Cisco PIX Firewall protects the Cisco BTS 10200 from various IP attacks, such as denial of service (DOS), unauthorized access, and so on. The most appropriate Cisco PIX Firewall models for the Cisco BLISS for T1 solution are the 525 or 535 models. Selection of the firewall is based on throughput capacity as well as capacity of the VoIP signaling Application Layer Gateway (ALG). The ALG allows for the dynamic creation of holes in the firewall by examining IP port information in the signaling traffic.

Figure 1-12 Cisco PIX Firewall

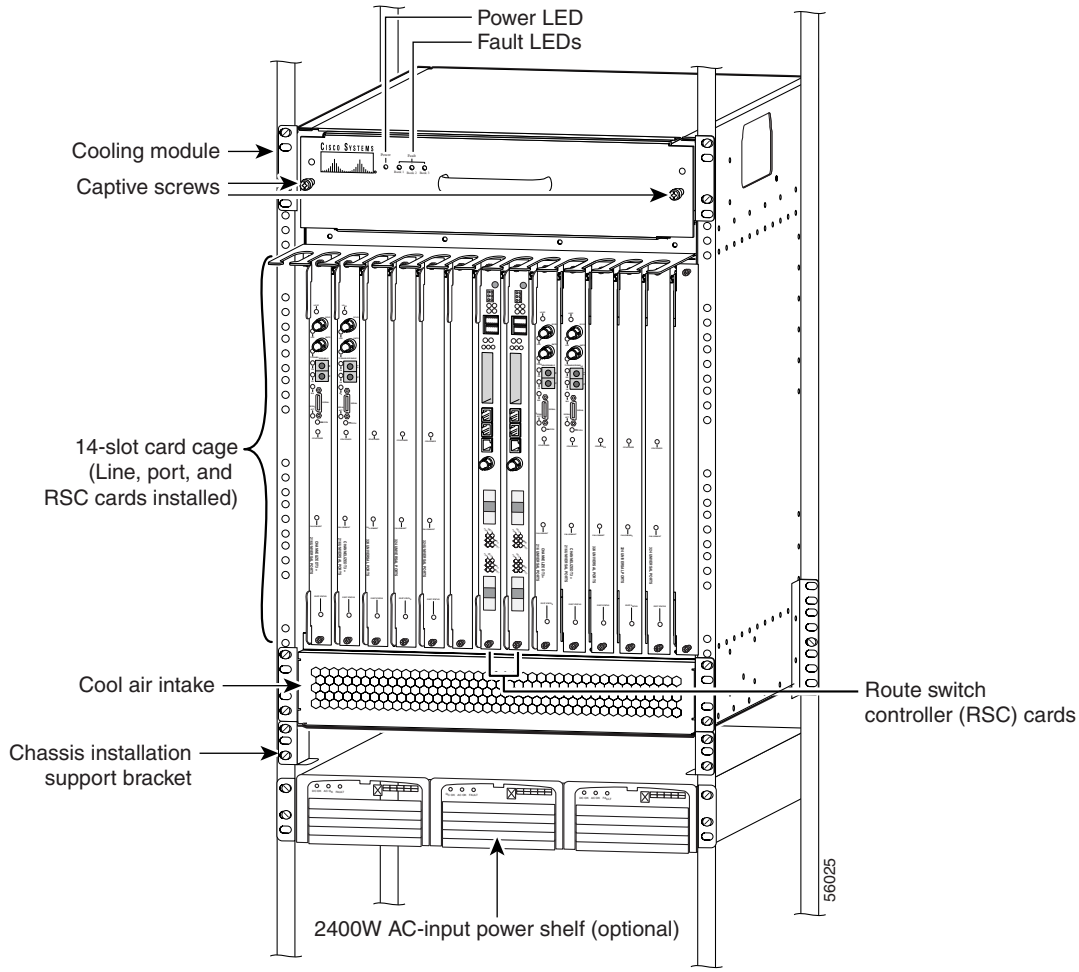


Cisco AS5850 Universal Gateway

The Cisco AS5850 Universal Gateway (Figure 1-13) is a high-density universal gateway, with carrier-class attributes, offering highest capacity and high availability in its class. This gateway is designed to meet the demands of large, innovative service providers, supporting up to 5 Channelized T3s (CT3s), 96 T1s, 86 E1s, or 2 STM-1 (108 E1s) of data, voice, and fax services, on any port at any time. It offers high-availability features such as hot-swap on all cards, load-sharing and redundant hot-swappable power supplies, redundant fans and fan banks, redundant route switch controller (RSC) cards, and Call Admission Control (CAC), all part of the carrier-class attributes required to provide a highly available system.

The Cisco AS5850 can be used to terminate all trunks types associated with the Cisco BLISS for T1 solution. One consideration of deploying the Cisco AS5850 is the impact to voice calls in the event of an eRSC card failure. If the eRSC fails, then all transient and stable calls are lost. Upon failover to the standby eRSC, calls can be re-established. The advantage of the Cisco AS5850 gateway is that it runs Cisco IOS and provides the common IOS interface for configuration and troubleshooting.

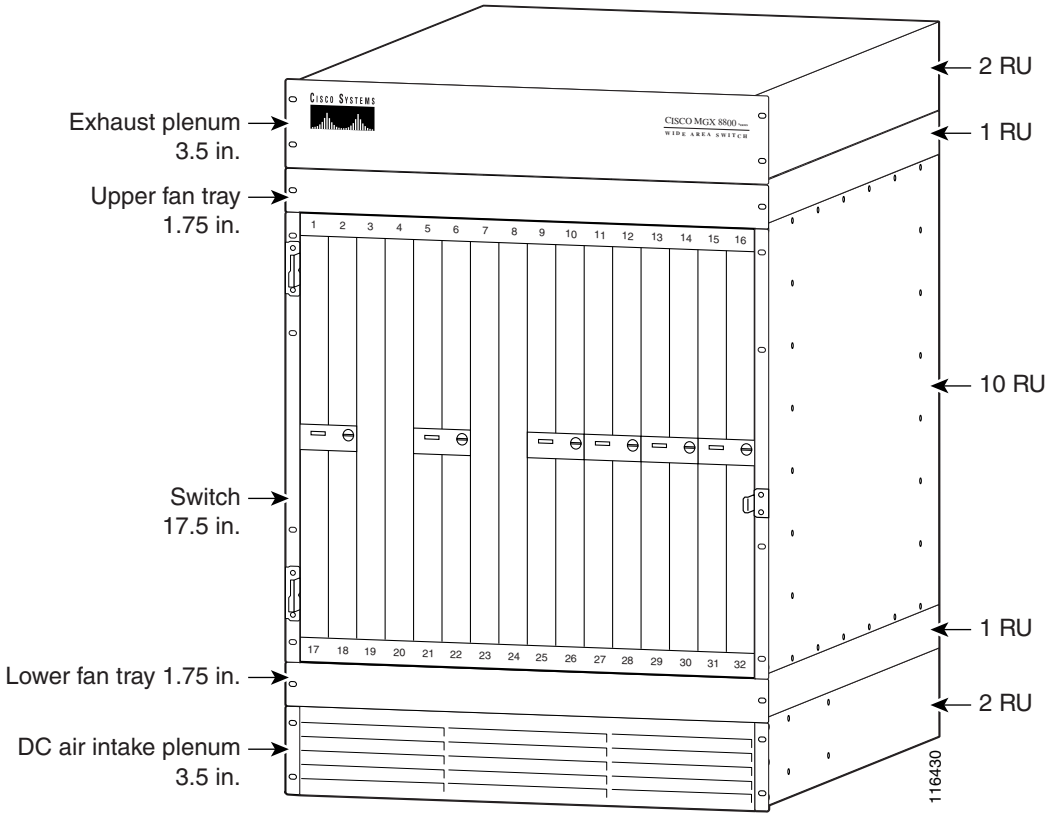
Figure 1-13 Cisco AS5850 Universal Gateway



Cisco MGX 8880 Media Gateway

The Cisco MGX 8880 Media Gateway (Figure 1-14) enables a range of packet voice applications for wireline, wireless and cable. With its comprehensive suite of quality of service (QoS) features and high-availability hardware and software, the Cisco MGX 8880 Media Gateway allows service providers to optimize their existing network infrastructure and lay the foundation for the delivery of advanced services and applications.

Figure 1-14 Cisco MGX 8880 Media Gateway

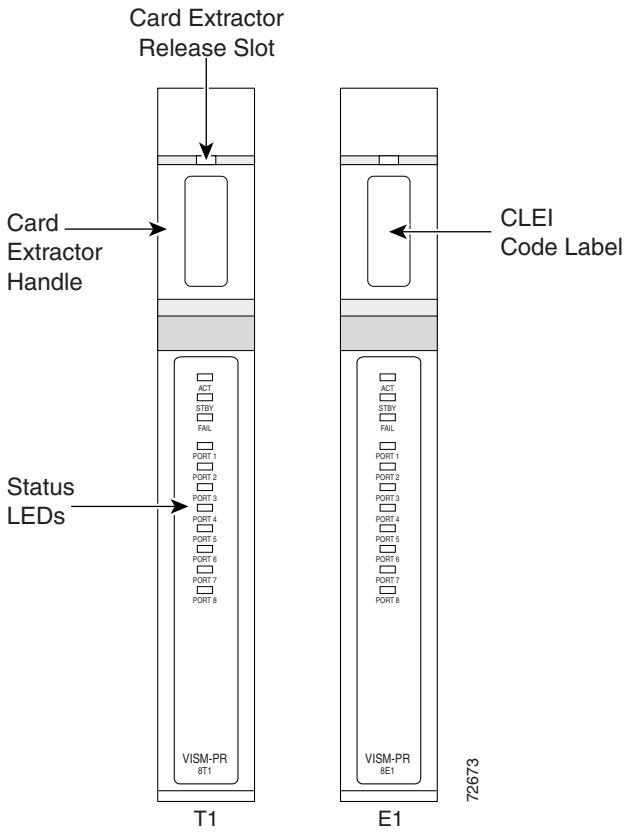


The advantage of using the Cisco MGX 8880 over the 8850 is improved pricing, three units fit into a 7-foot rack, and it provides a non-forklift upgrade to higher capacity using the VXSM.

Cisco VISM-PR

The Cisco VISM-PR cards (Figure 1-15) offer a field-proven full set of voice over IP (VoIP) and voice over ATM (VoATM) features, including toll-quality voice, fax, and modem. The Cisco VISM-PR cards can be deployed in standalone configurations or with softswitches to enable a variety of packet voice services in network architectures using the Media Gateway Control Protocol (MGCP), PacketCable Trunking Gateway Control Protocol (TGCP), H.323, and the Session Initiation Protocol (SIP).

Figure 1-15 Cisco VISM-PR Cards



Termination of the T1s to the VISM card can be done in a couple of ways. One is to use the 8-port T1 back card which provides the physical interfaces for the eight T1s supported on the card. There is a 1-to-1 relationship between back card and VISM. The second way is to use the SRM module with either the channelized OC-3 back card or the T3 back card. This card provides muxing functionality and provides connectivity to the VISMs via the Cisco MGX 8880 integrated TDM bus. In this scenario there is no back card used for the VISM.

All components in the VISM are capable of full redundancy. With the exception of the VISM, when a failure occurs, voice calls are not affected. When a failure occurs in the VISM, all voice calls active on that VISM are dropped and can be reestablished when the standby VISM becomes active. VISMs can be configured for 1:1 or 1:N redundancy.

Cisco MGX 8850 Series

The Cisco MGX 8850 is a high-density trunking gateway that is superseded by the Cisco MGX 8880, which was covered in the previous section. Applications which require a full-featured ATM switch will still require the Cisco MGX 8850, as the Cisco MGX 8880 only supports voice gateway functions. Note that both platforms are functionally equivalent in terms of voice capability using the VISM, but when using the VXSM (currently not part of the BLISS for T1 solution) the Cisco MGX 8880 provides greater feature depth. For more information on the VXSM, refer to http://www.cisco.com/univercd/cc/td/doc/product/wanbu/8850px45/vxsm/rel5/index.htm.

Cisco IAD2430 Series

Located at the customer site, the Cisco IAD2430 series provides support for analog phones (FXS and FXO ports). The uplink WAN connection is through T1 lines using PPP for Layer 2 link control. The Cisco IAD provides management MIBs and supports SNMP messages and northbound interfaces for network management. The Cisco IAD also provides remote access for element management and element configuration.

The Cisco IAD integrates user-side data, voice and fax signals and connects them to the wide area network (WAN) for transport by Voice over IP (VoIP).

Interfaces supported will depend on the model of the IAD and are as follows.

Voice

- Digital: One T1-PBX (channel-associated signaling [CAS], Primary Rate Interface [PRI]) port
- Analog: 8 FXS/16 FXS/24 FXS ports (RJ-21 connector)
- Bearer: TDM voice, VoIP (Real-Time Transport Protocol [RFC1889] [RTP], cRTP)
- VoIP properties: RTP, cRTP, echo cancellation, silence suppression/comfort noise, modem passthrough, Cisco fax relay, T.38 fax relay
- Call control: MGCP 0.1, MGCP 1.0, H.323, SIP
- DSPs: CELP (G.729a), ADPCM (G.726 (32), G.726(16)), PCM (G.711uLaw, G.711aLaw)
- Interface type: Loop start, ground start
- RENs: 5 REN per port, 12 REN per system
- Simultaneous voice calls (digital/analog): 24/24

WAN

- One or two T1/E1 (Point-to-Point Protocol [PPP], High-Level Data Link Control [HDLC], or Frame Relay) with integrated channel service unit/digital service unit (CSU/DSU) (RJ-48 connector)
- One or two Fast Ethernet (10/100BASE-T) ports for Ethernet access
- One voice WAN interface card (VWIC) slot for:
  - Broadband interfaces

    ADSL (WIC1-ADSL) or G.SHDSL (WIC1-SHDSL) for DSL uplink

    WAN: WIC-1DSU-T1, VWIC-2MFT-T1, VWIC-2MFT-E1
  - Voice interfaces—VIC2-4FXO, VIC2-2FXO, VIC2-2FXS, VIC-4FXS/DID, VIC2-2BRI-NT/TE
  - Serial interfaces—WIC-2T, WIC-1T

The Cisco IAD can be placed on a desktop, or mounted on a wall or in a 19-inch rack.

Figure 1-16 through Figure 1-19 show the Cisco IADs supported in the Cisco BLISS for T1 solution.

Figure 1-16 Cisco IAD2431-8FXS Chassis

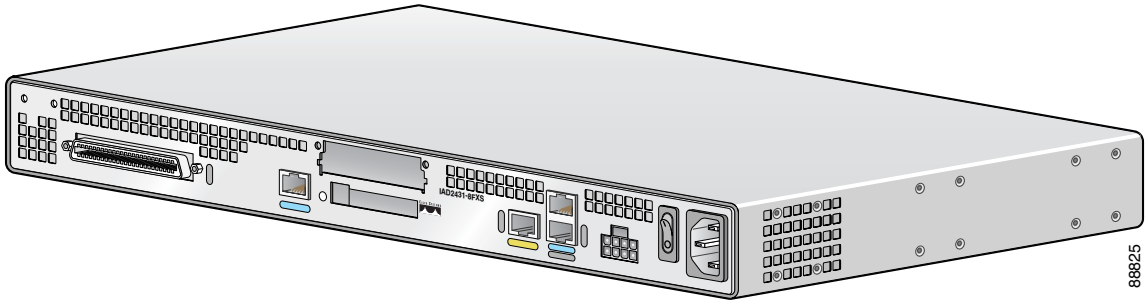


Figure 1-17 Cisco IAD2431-16FXS Chassis

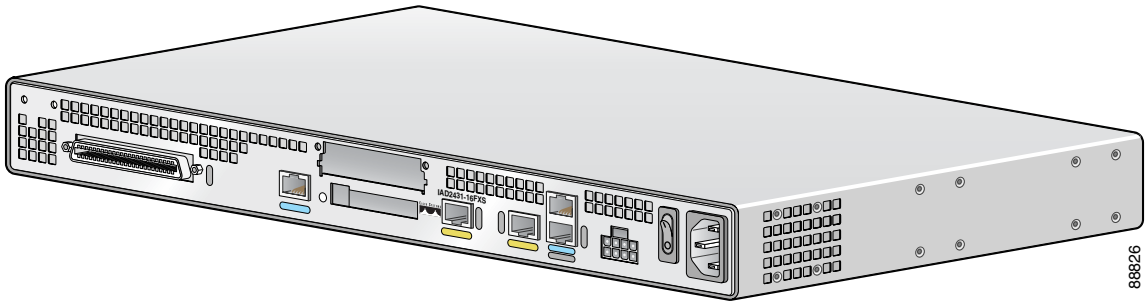


Figure 1-18 Cisco IAD2431-1T1E1 Chassis

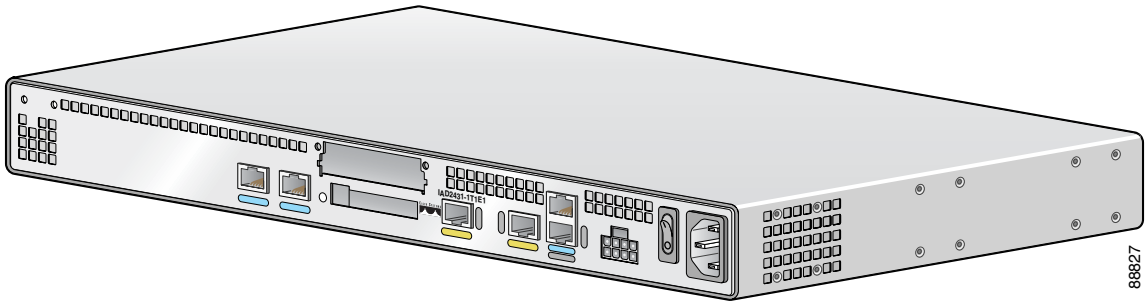
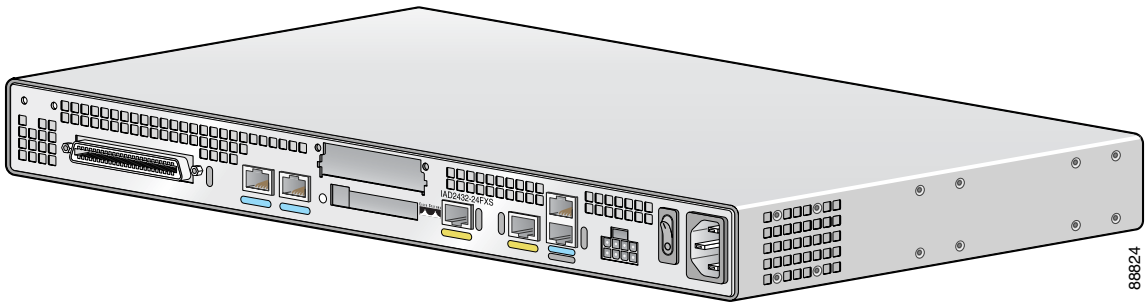


Figure 1-19 Cisco IAD2432-24FXS Chassis



Cisco SIP IP Phones

The Cisco SIP IP phones supported are the Cisco 7960, 7940, 7912, and 7905. The notable phone features are shown in Table 1-2.

Table 1-2 Cisco SIP Phone Features

Phone	Features
7960	• XML Browser • Pixel Based Display • PC Ethernet Port • Headset Jack • 6 Lines
7940	• XML Browser • Pixel Based Display • PC Ethernet Port • Headset Jack • 2 Lines
7912	• Pixel Based Display • PC Ethernet Port • 1 Line
7905	• Pixel Based Display • 1 Line

IP Unity Announcement Server

The Harmony6000 Media Server is used as an announcement server in the Cisco BLISS for T1 solution; however, this server is built for high-speed, high-volume media processing. The carrier-grade hardware platform is specifically designed to overcome the challenges of delivering services such as interactive voice response (IVR), conferencing, announcements, automated speech recognition, text-to-speech and others, on a single platform (see http://www.ip-unity.com/solutions/harmony6000/)

This platform is provided by a third-party vendor and not directly through Cisco. Customers wishing to use this product should work directly with IP Unity to acquire the unit and obtain support. For additional information on IP Unity and its use in the Cisco BLISS for T1 solution, contact the Cisco Account Team.

Figure 1-20 IP Unity Harmony 6000 Announcement Server

Planning and Design

Network designs will vary slightly from customer to customer due to differing sets of requirements and general technology and deployment preferences and methodologies. This chapter discusses elements of the Cisco BLISS for T1 design that should be considered before the solution is deployed.

Network Design

The initial step in planning and design is to collect the customer requirements to ensure that what the customer is looking for is something Cisco can deliver. The internal Network Commit Process validates and assures the fit between a Cisco Systems solution and a set of customer requirements to ensure that Cisco can deliver, deploy, and support the solution. The benefits of the process are as follows:

- Align customer requirements with Cisco capabilities
- Assure deployment success
- Manage customer expectations
- Ensure customer satisfaction

This chapter includes the following sections:

Redundancy

This section identifies the key redundancy features of the design and points out portions of the design which lack redundancy and are single points of failure.

Table 2-1 summarizes the physical redundancy recommendations for the Cisco BLISS for T1 solution.

Table 2-1 Physical Redundancy Recommendations

Node	Redundancy	Comment
Cisco BTS 10200 Softswitch	Dual CA and EMS	Fully redundant
Cisco ITPs	Deployed as mated pairs	Fully redundant
Cisco MGX 8880	2 PXM45, 2 RPM-XF, dual power supplies, 2 SRM3T3 cards, 1:N VISM Redundancy	Fully redundant
Cisco 10000 ESR	2 PRE-1, dual power supplies, 2 GE uplinks, DS3 WAN and VPN tunnel provide alternate paths for POP interconnect	Partially redundant 6-port DS3 line cards are not redundant
Catalyst 6509	Deployed as mated pair	Fully redundant
Catalyst 4506	Deployed as mated pair	Fully redundant
Catalyst 3550	Deployed as mated pair	Fully redundant
Cisco 7206	Single point of failure for internet connectivity	Partially redundant Power supplies are redundant
Cisco 2811 Terminal Server	Used as out-of-band backup system for device management	Not redundant
Cisco PIX Firewalls	Deployed as active/standby mated pair	Fully redundant
Cisco IAD2430	None	Not redundant
DNS Server	Dual DNS servers with dual load balancers	Fully redundant

Cisco BTS 10200 Softswitch

The Cisco BTS 10200 Softswitch is comprised of two discrete, redundant components including the Call Agent (CA) and the Element Management System (EMS.) At any given time during operation, there is one pair of system components—CA and EMS—in an active state and the other pair is in a standby state. Also, the primary CA is in regular communication with the primary EMS and the secondary CA. This ensures that the CA's indexed databases (IDXs) are in sync with each other. Similarly, the primary EMS and secondary EMS use replication to sync their respective Oracle databases to each other.

Cisco ITPs

Cisco ITPs are deployed as a mated pair, which provides a fully redundant configuration. How traffic flows though the Cisco ITPs during a failure situation will be dependent on the method used for deployment. More detail on the two methods and the pros and cons of both will be covered in more detail in the "Configuring the Cisco ITP" section on page 5-6.

Cisco MGX 8880

In the Cisco BLISS for T1 solution, the Cisco MGX 8880 acts as the trunking gateway, providing connectivity to the PSTN. With respect to redundancy, the advantage of using the Cisco MGX 8880 in the solution is that the only active call impacting failure is a failure of a VISM. A VISM failure results in the loss of up to eight T1s. This is much better when compared to the Cisco AS5850 where an eRSC failure can result in the loss of up to 112 T1s or a line card failure can result in a loss of up to 28 T1s.

The Cisco MGX 8880 contains four main cards:

- VISM
- PXM45
- RPM
- SRM3T3

Each card is discussed in more detail in the following subsections.

VISM

The voice interworking service module (VISM) card has eight T1s. The total number of cards that can be put in each shelf of the Cisco MGX 8880 is 12 for a total of 24 cards across the upper and lower shelves. We recommend that the VISMs be deployed with 1:N redundancy to maximize the capacity of the MGX and provide a redundant VISM if one of the active VISMs fails.

PXM45

The PXM45 provides the control function for the MGX and interconnects the various line cards in the chassis. For example, the PXM45 interconnects the VISM and the RPM via a point-to-point ATM permanent virtual circuit (PVC). Redundancy for the PXM45 is provided through an active/standby configuration. The active card will process traffic while the standby card is idle. The active and standby cards communicate for synchronization and to determine if a switchover is necessary. In case of a PXM failure, the standby card becomes the active PXM and the MGX continues to process traffic normally. A PXM failure does not impact active calls.

RPM

The Route Processor Module (RPM) is a router on a blade that terminates the ATM PVC from the VISM and routes VoIP traffic between the Cisco BLISS for T1 core network and the VISM. RPM redundancy is provided through an active-active mechanism. Two RPMs are installed in the MGX chassis and a PVC from each is created to each VISM card in the chassis. One of the PVCs is designated active and the other standby. If an RPM fails, operations, administration, and maintenance (OAM) messages will be lost on the active PVC and the VISM will switch to the standby PVC and voice calls will continue to flow.

SRM3T3 (Optional)

The SRM Card multiplexes the T1s from VISM cards and aggregates them on the T3s on the SRM3T3 card. Redundancy for the SRM3T3 cards is provided through an active/standby configuration. If the PXM switches over to the secondary, the SRM card also switches to the secondary card. The PXM and SRM card are locked to each other from a redundancy perspective. For example, if PXM A and SRM A are locked together, and either of them fails, the MGX will failover to PXM B and SRM B. There are four SRM cards in the MGX, two for each shelf. T3 connectivity redundancy is provided with Y-cables.

Cisco 10000 ESR

The Cisco 10000 Edge Services Router (ESR) provides edge aggregation services in the Cisco BLISS for T1 architecture. It provides aggregation for T1s connecting customer premises equipment (CPE) to the T1 network as well as backhaul of customer traffic to the Cisco BLISS for T1 core. Redundancy in the Cisco 10000 ESR is provided through the use of dual power supplies and active/standby Performance Routing Engines (PRE-1). The Cisco 10000 ESR also supports Non Stop Forwarding and Stateful Switchover (NSF/SSO), which are mechanisms to prevent the disruption of IP traffic flow during a PRE switchover.

Catalyst 6509

We recommend deploying two identical Catalyst 6509 switches as a mated pair in the Cisco BLISS for T1 core network to provide full switch redundancy.

Catalyst 4506

We recommend deploying two identical Catalyst 4506 switches as a mated pair in the Cisco BLISS for T1 remote point of presence (POP) core networks to provide full switch redundancy.

Catalyst 3550

We recommend deploying two identical Catalyst 3550 switches as a mated pair in the Cisco BLISS for T1 remote POP core networks to provide full switch redundancy.

Cisco 7206

The Cisco 7206 provides routing services between the Internet and the Cisco BLISS for T1 network. The only redundancy on this platform is dual power supplies. If redundant connections to the Internet are a customer requirement, dual Cisco 7206 switches can be deployed with redundant connections to the Internet.

Cisco 2811 Terminal Server

This device is not redundant. Its only purpose is to provide out-of-band management for devices if in-band management is unavailable.

Cisco PIX Firewalls

Cisco PIX Firewalls are deployed in an active/standby mated pair configuration, hence there is no single point of failure.

Cisco IAD2430

The Cisco IAD2430 Series Integrated Access Device does not support any redundancy mechanisms. If the box fails, the entire unit has to be replaced.

DNS Server

DNS services are deployed on separate primary and secondary servers which provide full redundancy. In addition, active/standby load balancers are deployed to provide a single virtual IP address to all Cisco BLISS for T1 devices.

IP Addressing Recommendations

It is important that the IP addressing for the Cisco BTS 10200 Softswitch, as defined in the Network Site Survey document, be understood before designing the addressing scheme for the network.

In addition, actual public and private IP address assignments for the network should be done in conjunction with customer personnel. In general, the addressing of the Cisco BLISS for T1 network follows the same guidelines as IP addressing for any data communications network, keeping the following guidelines in mind.

- Determine if the customer will obtain a block of addresses from the American Registry for Internet Numbers (ARIN) or if the addresses will be provided by the Internet service providers to which the customer is connecting. If POP Internet connections are going to be used as backups for other POP Internet connections, determine if one service providers IP addresses are routable through another service providers network. In general, it is more advantageous for customers to get their own block of addresses as it allows them more flexibility in connecting and routing to the Internet.
- Consider summarizing when addressing the individual POPs. Summarizing allows the addresses from one POP to be propagated to another POP in the form of a summary route. This reduces routing overhead by minimizing the number of routes in routing tables as well as reducing network convergence operations caused by networks transitioning states within POPs. For large POPs, intra-POP summarization may be required and must be considered when assigning addresses.
- Assign addresses in such a way to identify device attributes such as location and device type. This will aid in troubleshooting network problems. End customers should understand that moving from one location to another could result in a change to their IP addressing if the move results in a change to their summarization area.

Routing Protocol Recommendations

This section describes the routing and related redundancy aspects of the MGCP signaling path to and from the Cisco BTS 10200 for the Cisco BLISS for T1 solution.

Signaling redundancy is provided by:

- ICMP Router Discovery Protocol (IRDP) between the Call Agent and the Catalyst 6509 Multilayer Switch Feature Cards (MSFCs)
- Open Shortest Path First (OSPF) between the Catalyst 6509/MSFCs and other network devices.

When selecting a routing protocol for the Cisco BLISS for T1 solution things to consider are:

- Scalability
- Route convergence time
- High availability features like NSF/SSO
- Ability to support migration to technologies like MPLS
- Industry familiarity

Considering the above requirements, OSPF was selected for the Cisco BLISS for T1 solution.

ICMP Router Discovery Protocol

ICMP Router Discovery Protocol (IRDP) is defined by RFC 1256 and is an extension to ICMP that allows routers to notify hosts of their presence. This is the mechanism used by the Call Agent to converge its default route if a default route fails. For any failure between the Call Agents and the Catalyst 6509 switches, the host should adjust its default route within 10 seconds. This only impacts the MGCP signaling traffic from the Call Agent to MGCP endpoints. RTP traffic does not traverse the Call Agent and therefore is not affected.

IRDP defines Router Advertisement and Router Solicitation messages. Router Advertisements are sent in the period between the values configured for ‘ip irdp minadvertinterval x’ and ‘ip irdp maxadvertinterval y.’ For the Cisco BLISS for T1 solution, these will be set to their lowest possible values (between 3 and 4 seconds). These advertisements can be sent to the multicast address 224.0.0.1 or to the all 1’s broadcast address, 255.255.255.255. The IRDP message includes a lifetime field and a preference level that will be important to the convergence times. The lifetime field (configured by ‘ip irdp holdtime x’) is used to tell the host how long the advertisement should remain valid. This would allow for 2 to 3 advertisement losses before invalidating the advertisement.

Router Solicitations are used by the host during initialization time to request an early advertisement. An early advertisement is useful in environments where the advertisement interval is very long. Because the Cisco BLISS for T1 solution will use an update interval of 3 to 4 seconds, the solicitation is not that important. The host, however, will still send it when its process starts.

Open Shortest Path First Protocol

Open Shortest Path First (OSPF) is a link state routing protocol that quickly converges around failures in a manner that does not produce routing loops. Items that should be considered that affect OSPF convergence times are as follows:

- OSPF Designated Router Selection, page 2-7
- Neighbor Adjacency, page 2-7
- OSPF Cost, page 2-7
- OSPF Area, page 2-7
- OSPF and PIX, page 2-8

OSPF Designated Router Selection

For broadcast media, OSPF defines a Designated Router Selection process that determines the Designated Router and Backup Designated Router. The Designated Router is responsible for keeping the databases of all other routers on the subnet synchronized. When the Designated Router fails, the Backup Designated Router takes over, but can take additional time to synchronize all of the routers on the subnet. The time required to synchronize depends on the number of routes in the routing table. The Cisco BLISS for T1 design should not allow any of the trunking gateways or announcement servers to become the Designated Router or Backup Designated Router. This can be accomplished by setting the 'ip ospf priority 0' in those devices.

Neighbor Adjacency

OSPF routers send hello multicast packets to maintain the neighbor adjacency. The OSPF hello interval and dead time are key factors in determining network convergence time. If necessary, OSPF endpoint hello intervals can be adjusted downward to improve the update time of the link state database if a neighbor router fails.

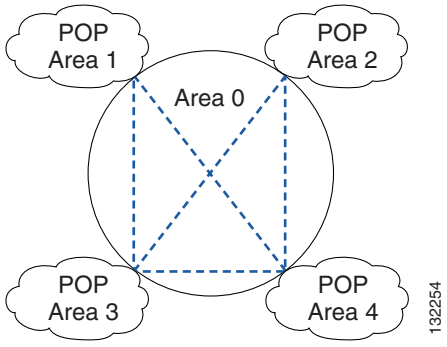
OSPF Cost

OSPF cost provides a mechanism to prefer one path over another through the network when multiple paths exist. It allows the path that traffic takes through the network to be determined beforehand for both normal and failure scenarios, which provides the necessary level of control to ensure continued operation of voice services.

OSPF Area

It is important to consider not only the current BLISS network design but also future network growth when designing OSPF areas. The purpose of OSPF areas is to reduce routing table size and prevent network events such as link failures or device outages in one area from affecting devices in other areas. In general, each POP should be defined as its own area with the core network connecting the POPs designated as area 0. See Figure 2-1.

Figure 2-1 OSPF Area



OSPF and PIX

The recommended release for the Cisco PIX Firewall is Version 6.3. This version includes support for the OSPF routing protocol which allows the Cisco PIX Firewall full routing functionality within the OSPF area. Note that when enabling OSPF on the Cisco PIX Firewall while using MD5 authentication, the Cisco PIX Firewall does not accept spaces within OSPF authentication keys or message digests, but Cisco IOS does. This may create compatibility issues when a Cisco PIX Firewall tries to exchange OSPF messages in an adjacent Cisco IOS device. Up to two OSPF process can be defined in the Cisco PIX Firewall and only broadcast networks are supported. OSPF features not supported by the Cisco PIX Firewall Version 6.3 include:

- Point-to-point link/serial interface/nonbroadcast multiaccess (NBMA)
- OSPF on demand circuit
- Flood reduction
- Redistribution of routes between non-OSPF routing protocols
- Policy routing

SS7 ITP Considerations

The following items should be considered in the deployment of the Cisco ITPs for SS7 connectivity:

- ITP Hardware Redundancy, page 2-8
- Platform Redundancy, page 2-8

ITP Hardware Redundancy

The Cisco 7507 platform is an internally hardware-redundant solution. The Cisco BLISS for T1 solution will not include internal hardware redundancy as a possible fully redundant solution. The reasons are:

- Customers do not view a single node with redundant cards as a viable alternative to having redundant nodes.
- In integration testing, many issues were found when hot-swapping cards on the Cisco 7507 ITP.

Also note that some customers felt that the Cisco 7507 with full internal redundancy configured did not have sufficient density and preferred the Cisco 7513 platform. Note however that the Cisco 7507 or Cisco 7513 may be part of a fully redundant SG Mated Pair.

Platform Redundancy

ITP redundancy can also be accomplished by connecting two ITP nodes together. This can be done in one of two ways. The ITPs can be connected as an *SG Mated Pair* or as an *ITP-Group*.

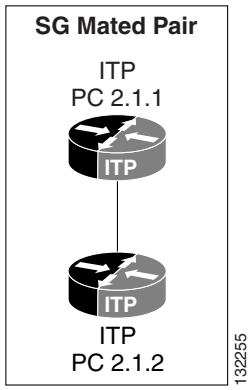
An SG Mated Pair is utilized whenever the customer wants to connect to the Service Provider SS7 Network via D-links. The ITP-Group is used whenever the customer wants to connect to the Service Provider SS7 Network via A-, E-, or F-links.

When provisioning the Cisco BTS 10200, these two forms of redundancy cannot be combined. If there are two Signaling Gateway Processes (SGPs) defined for one signaling gateway (SG), then that SG will be the only SG in the associated SG Group. Likewise, if there are two SGs in an SG Group, then a second SGP cannot be added to either of the associated SGs.

SG Mated Pair

As an SG Mated Pair connection, each Cisco ITP has its own point code and acts as a signalling termination point (STP) that connects to other STPs in the SS7 network via D-links. Any Cisco ITP can be used in this form of redundancy.

Figure 2-2 SG Mated Pair



Pros:

- The solution is fully hardwareredundant and IP network redundant.
- Each Cisco ITP acts as an STP and can have full STP functionality.
- Global Title Translation (GTT) can be supported on the Cisco ITP through the use of a capability point code.
- Geographical separation between the Cisco ITPs is allowed.

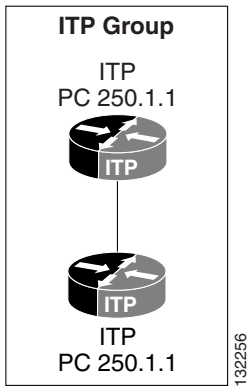
Cons:

- Each Cisco ITP requires its own point code.

ITP-Group

In an ITP group (the SIGTRAN Distributed MTP feature) configuration, each Cisco ITP acts as a *physical* SGP. Two of these physical SGP processes are connected together to form one logical SG. In this configuration, both Cisco ITPs share the same point code value. Note that this form of redundancy is not available for the Cisco 7500 because it has internal hardware redundancy. It is available for the Cisco 2651 and Cisco 7300 series ITPs.

Figure 2-3 ITP-Group



Pros:

- Two Cisco ITPs share the same point code (fewer point codes are needed).
- Identical Cisco ITPs form an SG.
- The solution is fully hardware redundant and IP network redundant.

Cons:

- GTT cannot be supported on the Cisco ITP itself.
- From the Cisco BTS 10200 to the Cisco ITPs, only load sharing across the Cisco ITPs is supported (there is no allowance for sending to one Cisco ITP at a higher priority than the other.
- The two Cisco ITPs must be colocated (no geographical separation).

Cisco BTS 10200/Cisco ITP Profiles

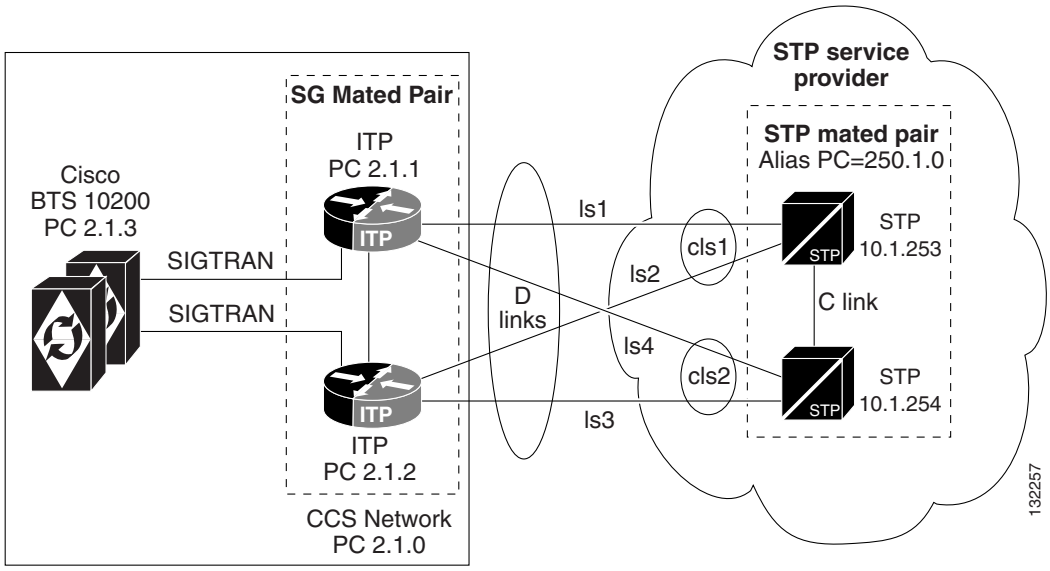
There are four Cisco BTS 10200/Cisco ITP profiles on which all customer-offered profiles are based. In general, the combination of a base profile, as described in this section, and one or more features, as described in the "Cisco BTS 10200/Cisco ITP Features" section on page 2-13, form the profiles described in the "Customer-Offered Cisco BTS 10200/Cisco ITP Profiles" section on page 5-10.

The four base Cisco BTS 10200/Cisco ITP profiles are as follows:

D-link Base Profile Using ITP-Group (Distributed MTP3)

In this configuration (Figure 2-4), each Cisco ITP acts as an STP and has its own point code which is different than any of the point codes on the Cisco BTS 10200 Softswitch. The Cisco ITPs are connected to the SS7 network using diagonal D-links.

Figure 2-4 D-link Base Profile



Pros:

- Redundancy is supported between the Cisco ITPs.
- Multiple originating point codes (OPCs) are supported on the Cisco BTS 10200 with just two Cisco ITPs.
- Geographical separation is allowed between the Cisco ITPs.
- The Cisco ITP supports GTT by using capability point codes.
- High-volume SS7 traffic can be supported by load sharing the traffic between the SG Mated Pair.

- Unlike the A-link solution, there is no need to purchase additional connections to the SS7 network when more OPCs are added to the Cisco BTS 10200.
- The SS7 network is able to distinguish between the status of the Cisco BTS 10200 and that of the Cisco ITP.
- All Cisco ITP platforms can be used as part of the D-link solution.
- In the unlikely event that a Cisco BTS 10200 becomes unavailable, the Cisco ITPs will continue to operate as a fully functional STP pair. In this scenario, one of the Cisco ITPs will send a TFP for the Cisco BTS 10200 point code toward the SS7 network. At the same time they will continue to transfer messages to other point codes in the network. Also, the Cisco ITPs can transfer messages to other Cisco BTS 10200 nodes in the case where there are multiple Cisco BTS 10200 nodes served by the Cisco ITP pair.

Cons:

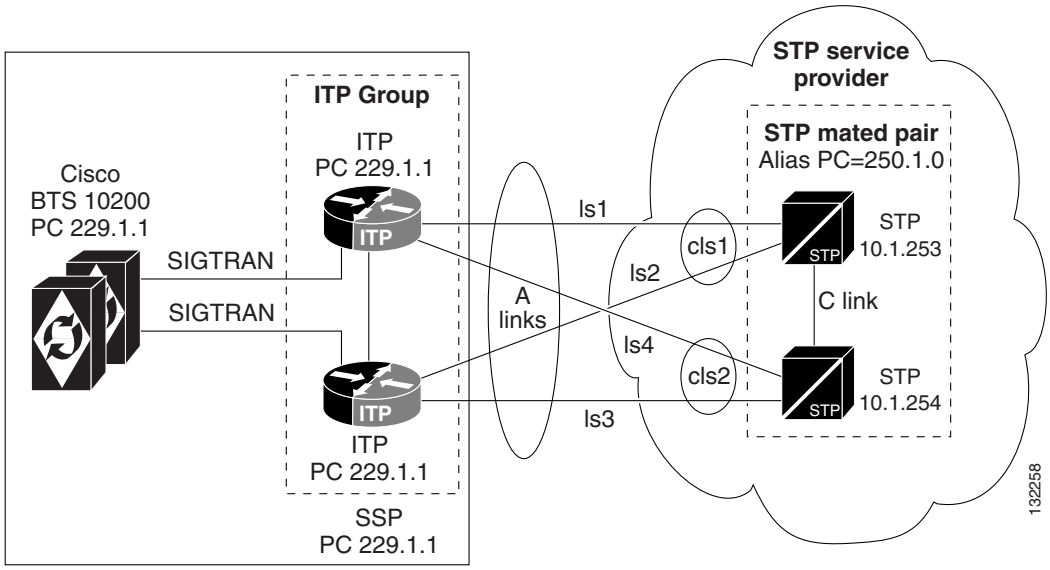
- The Cisco ITPs need their own point codes. This is a con when compared to A-links if the Cisco BTS 10200 only has a single OPC, but allows for much greater scalability when multiple OPCs are needed on the Cisco BTS 10200.
- The service provider will charge more for D-link connections than A-link connections. This is a con if the solution only requires a single OPC on the Cisco BTS 10200. If there are multiple OPCs on the Cisco BTS 10200, the D-link solution is probably more cost effective.

A-link Base Profile Using ITP-Group (Distributed MTP3)

In this profile (Figure 2-5), both Cisco ITPs and the Cisco BTS 10200 are viewed as a single point code Signaling End Point (SEP) from the service provider's SS7 network. The ITP-Group consisting of two Cisco ITPs acts as the SS7 proxy for the Cisco BTS 10200. The Cisco ITPs connect to the SS7 network using A-links.

Note If a Cisco BTS 10200 system becomes unavailable, the Cisco ITP role is limited because it is acting as an STP. In this scenario, the Cisco ITP simply sends a User Part Unavailable (UPU) message to the SS7 network and cannot provide any other services.

Figure 2-5 A-link Base Profile



Pros:

- There is less charge from the service provider for A-link connections than D-link connections. This is a pro if the Cisco BTS 10200 has only one OPC.
- The Cisco BTS 10200 and Cisco ITPs share the same point code value, thereby requiring fewer point codes in the network. This is a pro if the Cisco BTS 10200 has only one OPC.
- There is full hardware redundancy support between Cisco ITPs.
- High-volume SS7 traffic can be supported by a single point code.

Cons:

- GTT is not supported on the Cisco ITP. GTT must be performed on the service provider's STP.
- This profile does not allow geographical separation between Cisco ITPs—they must be colocated.
- A pair of Cisco ITPs is required for each OPC on the Cisco BTS 10200. In the D-link solution, only two Cisco ITPs are required regardless of the number of OPCs on the Cisco BTS 10200.
- Approximately half of the SS7 traffic of each Cisco ITP goes across the inter-ITP connection (based on SLS-to-SLC mapping). Therefore, the traffic between the Cisco ITPs is comparatively heavier than that of the D-link configuration.
- If the Cisco ITPs in an ITP group lose communication with each other and one of the Cisco ITPs also loses communication to the Cisco BTS 10200, the second Cisco ITP (that still has communication to the Cisco BTS 10200) will not keep calls up by running in simplex mode. An example of this is if one Cisco ITP in the ITP group loses all IP communication. In this case, both Cisco ITPs will become isolated from each other. The Cisco ITP that has lost all IP communication will also not be able to communicate with the Cisco BTS 10200. Its default behavior is to send a UPU to the network which will stop all traffic toward the Cisco BTS 10200 even though the other Cisco ITP is still functional. Because there are redundant IP connections between the Cisco ITPs, this is a double fault condition, which is not likely to occur, but needs to be noted.
- The Cisco 7507 platform is not available for ITP-Group mode (only the Cisco 2651, 7206, or 7301).

E-link Configuration Using ITP-Group (Distributed MTP3)

An E-link is basically the same as an A-link (except it serves as a backup in case all A-link connections become unavailable). It has the basic setup and list of pros and cons as the A-link configuration.

F-link Configuration Using ITP-Group (Distributed MTP3)

The F-link configuration is similar to the A-link configuration except that instead of connecting to an STP via 'A' links, it connects to another SEP in the SS7 network via fully associated F-links. It has the basic setup and list of pros and cons as the A-link configuration.

Cisco BTS 10200/Cisco ITP Features

The following is a list of features that are delivered through various configurations and combinations of the Cisco BTS 10200 and the Cisco ITP. These features are built on top of the base configuration profiles defined in the "Cisco BTS 10200/Cisco ITP Profiles" section on page 2-10 to form the profiles defined in the "Customer-Offered Cisco BTS 10200/Cisco ITP Profiles" section on page 5-10.

- A single Cisco ITP to route to several Cisco BTS 10200 nodes (each of which has its own unique point code(s)). This feature is only associated with D-link configurations. The implementation is straightforward and given in the "Basic D-link Profile" section on page 5-10.
- Multiple OPCs on the Cisco BTS 10200. This feature can be implemented for both A-link and D-link configurations. Note that for A-link configurations, it will require a new pair of Cisco ITPs for each OPC on the Cisco BTS 10200. See the "Multiple Cisco BTS 10200 OPCs with D-Link Profile" section on page 5-36 for details.
- Multiple Cisco BTS 10200 nodes sharing the same point code. This should be functional for both the A-link and D-link configurations. Implementation of this feature requires special configuration and the Cisco ITP will have to route traffic based on either destination point code (DPC) value or DPC value and CIC range. The main limitation is that multiple Cisco BTS 10200 nodes sharing a single point code is only valid for ISUP. If TCAP queries are needed, then a separate TCAP OPC will be needed for each Cisco BTS 10200. See the "Multiple Cisco BTS 10200 Nodes Sharing the Same OPC" section on page 5-48 for details.
- Geographically separated ITPs. Here the customer can have a Cisco BTS 10200 communicating with SS7 networks which are in different parts of the country. This is accomplished by connecting to Cisco ITPs that are located in the respective parts of the country. This is only valid for the D-link configuration. It also provides for redundancy so that if IP communication toward one Cisco ITP goes down, calls can be routed through the second Cisco ITP to reach the associated DPC.
- Priority Cisco BTS 10200 SIGTRAN Routing. This feature allows the Cisco BTS 10200 to choose the preferred outbound route between Cisco ITPs in an SG Mated Pair by assigning a route priority to each of the SGs. It is common to use this feature in combination with *geographically separated* ITPs. It is only valid for the D-link solution. See the "Geographically Distributed D-link Profile with SG Routing Priority" section on page 5-46 for details.

QoS Recommendations

The goal of quality of service (QoS) is to help reduce or eliminate delay of voice packets that travel across a network. In the Cisco BLISS for T1 solution, the method used is Class-Based Weighted Fair Queuing (CBWFQ) with a priority queue also known as Low Latency Queuing (LLQ). In this scenario, traffic is classified as voice or data and queued such that voice always gets priority and data receives best-effort service. The customer is free to define the classifications of traffic in a more granular fashion, but voice must always get priority over all other types of data traffic.

End-to-End Voice Delays

Based on ITU-T G.114 recommendations, end-to-end one-way delay of 150 ms is acceptable. In this section we use the codec G.726 as an example to discuss the end-to-end delay budget calculation.

In Cisco IOS VoIP products, the digital signal processor (DSP) generates a speech sample every 10 ms when using G.726. Two of the samples are then placed within one packet. The packet delay is then 20 ms. A lookahead of 5 ms occurs between the frames. The speech samples sent in one packet can be configured by increasing or decreasing the packetization interval. Table 2-2 shows end-to-end VoIP packet delay budget items.

Table 2-2 Example Delay Budget for G.726 Codec

VoIP Delay Factors	Fixed Delay	Variable Delay
Coder Delay G726 (5 ms lookahead)	5 ms	
Coder compression Delay G.726	2 ms	
Packetization Delay (Coder compresses 5 ms sample into one frame, 4 frames are packetized together)	20 ms	
Queuing Delay at the output queue of various network hops		?
Serialization Delay at T1 Trunk of IAD	0.35 ms	
WAN Delay 1: For private lines, network propagation delay is assumed at 6µsec per km	?	
Or WAN Delay 2: public network switching delay	?	
Coder decompression delay G.726	2 ms	
Dejitter buffer	10 – 100 ms	
Total	39.35 ms – 129.35 ms +WAN delay	Queuing delay

As seen in Table 2-2, there are certain unknown delay factors, as indicated by the question marks (?). For calls made across a WAN in a public switched network, the network delay could be a big contributor. The customer can also adjust dejitter buffer size to achieve the balance between jitter and delay.

If the buffer is too small, the end-to-end delay can be minimized for individual voice packets. However, the samples are held in the buffer for too short a time, and variations in delay may cause the buffer to underrun and cause gaps in the speech. If the buffer is too large, the samples are held for too long a time, the buffer can overrun, and the dropped packets again cause gaps in the speech. In addition, the end-to-end packet delay may rise to unacceptable levels. The Playout Buffer is the command used in VoIP in order to adjust the jitter buffer size to achieve balance between jitter and delay.

The queuing delay at various network components is the major contributor of the variable delay in a VoIP network. This includes the queuing/buffer delay in the WAN if a public switched network is used. QoS techniques that can be used to minimize the queuing delay in customer network environments are discussed in the next section. Using the information collected in Table 2-2, a delay budget needs to be calculated. For example, if the WAN delay is estimated at 20 ms, dejitter buffer is 40 ms, and queuing delay is 25 ms, then the end-to-end delay budget is 29.35 + 20 + 40 + 25 ms = 114.35 ms.

End-to-End Voice QoS Consideration

Cisco IOS provides various QoS tools for VoIP networks. An overall QoS strategy needs to be developed to utilize these QoS features to achieve the best voice service quality. QoS techniques such as classification at the network edge, queuing and policing at the output queue of the network aggregation and core points, need to be applied in the network. For the queuing and policing QoS techniques, LLQ is recommended to guarantee bandwidth and latency for different classes of traffic. It assigns absolute high priority to voice traffic and distributes the rest of the link bandwidth fairly among the data traffic. Thus LLQ helps minimize the variable queuing delay as listed in the end-to-end delay budget chart.

In the Cisco BLISS for T1 solution, LLQ has to be applied to all devices that are responsible for transmitting voice and data traffic. Notable components are the Cisco IAD, Cisco 4506 switch, and the Cisco 10000 ESR. The following sections cover examples of these configurations.

LLQ Configuration Example Using MQC

Low Latency Queuing (LLQ) is a combination of Priority Queuing (PQ) and Class Based Weighted Fair Queuing (CBWFQ), meaning LLQ brings the Priority Queuing features into the CBWFQ.

This allows voice strict priority and data to optionally be further classified to provide differentiated classes of service. In some areas of this document that state Priority Queuing, what we are referring to is the PQ functionality that is part of Low Latency Queuing.

The following example illustrates the configuration of priority queuing on a Cisco IAD.

```
<--- snip--->
class-map match-all MGCP<--- create a class for signaling traffic called MGCP
  match ip precedence 4 <--- all traffic with precedence 4 is placed into the class MGCP
class-map match-all RTP<--- create a class for RTP traffic called RTP
  match ip precedence 5<--- all traffic with precedence 5 is placed into the class RTP
!
policy-map T1_QOS<--- create a policy called T1_QOS
  class RTP<--- for traffic that is in the class RTP
    priority percent 90<--- assign RTP class traffic to the priority queue (up to 90%
avail ban)
  class MGCP
   bandwidth percent 4
!
interface Multilink1
service-policy output T1_QOS<--- apply the policy T1-QOS to the interface in the outbound
direction
 …..
 multilink-group 1
!
```

LLQ is configured with the **priority** command. To enqueue classified traffic to the strict priority queue, you configure the **priority** command for the class after you specify the named class within a policy map. (Classes to which the **priority** command is applied are considered priority classes.) Within a policy map, you can give one or more classes priority status. When multiple classes within a single policy map are configured as priority classes, all traffic from them is enqueued to the same single, strict priority queue.

QoS Configuration Example on Catalyst Platforms

Catalyst 4506

```
…
qos map dscp 32 33 34 to tx-queue 2
qos map dscp 35 36 37 38 39 40 41 42 to tx-queue 4
qos map dscp 43 44 45 to tx-queue 4
qos map dscp 24 25 to cos 2
qos map dscp 33 to cos 3
qos map dscp 40 41 42 43 44 45 to cos 4
qos map cos 3 to dscp 26
qos map cos 4 to dscp 34
qos map cos 5 to dscp 46
qos
…
interface GigabitEthernet6/3
…
 no switchport
 ip address 172.17.66.5 255.255.255.252
  qos trust dscp
 tx-queue 3
   priority high
…
```

Catalyst 6509

```
….
mls qos map dscp-cos  24 25 to 2
mls qos map dscp-cos  32 33 to 3
mls qos map dscp-cos  40 41 42 43 44 45 to 4
mls qos map cos-dscp 0 8 16 26 34 46 48 56
mls qos map ip-prec-dscp 0 8 16 26 34 46 48 56
mls qos
…
interface GigabitEthernet1/1
 …
 no ip unreachables
 no ip proxy-arp
 logging event link-status
 wrr-queue cos-map 1 1 0 1 2
 wrr-queue cos-map 1 2 3
 wrr-queue cos-map 2 1 4 6 7
 wrr-queue cos-map 2 2 5
 mls qos trust dscp
```

Voice Loss Plan

A voice loss plan needs to be created in order to optimize voice quality. The purpose of the loss plan is to reduce the effects of echo, distortion, clipping, and noise within the voice environment and counter the effects of power loss due to signal transmission. Inserted loss appears once in the Primary Signal Path and twice in the Talker and Listener Echo Paths.

For more information on the voice loss plan and echo, refer to http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper09186a00800d6b68.shtml

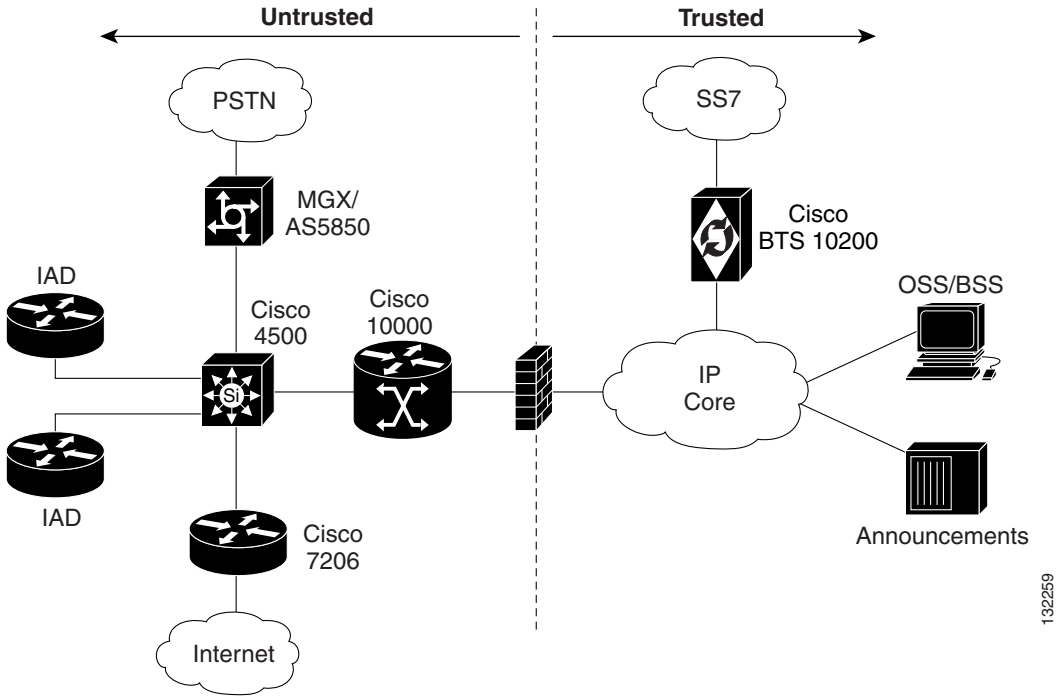
Security Recommendations

This chapter describes the significant threats to service that can occur from the untrusted portion of the Cisco BLISS for T1 network. It also describes the solutions to manage those security threats. The components in the untrusted portion of the network, for the purpose of solution security, are those included in the area to the left of the firewall as indicated in Figure 3-1. Basically, it includes all equipment deployed in the subscriber premises, the Internet Service Providers (ISPs) network, and the Internet. The trusted area can be assumed to be secure and not the source of an attack on the network.

In the Cisco BLISS for T1 network, the probable sources of attack are the Cisco 24xx, 2600, and 37xx in the customer premises equipment (CPE). Malicious traffic can also originate from the ISP's network or the Internet. It is reasonable to assume that all of the core elements, trunking gateways, Feature Servers, and the Call Agent are physically in a secure environment and not easily accessible to unknown or untrusted people.

Only Layer 3 and above security issues are addressed in this chapter. In the Cisco BLISS for T1 solution, it is assumed that each Integrated Access Device (IAD) has a secure and unshared physical connection into the core.

Figure 3-1 Cisco BLISS for T1 Security Zones



Security Design Goals

This section describes the plan for securing the Cisco BLISS for T1 network. Note that it is not possible to guarantee the complete security of an IP network. It is always possible to put more secure measures into the network at additional expense and complexity. The design described here attempts to balance the need for good security against network functionality/flexibility while minimizing the risk of an attack that could affect network operation.

This section includes the following sub-sections:

Trusted Zone

Most networks have a trusted zone where it is assumed an attack will not originate. The trusted zone is protected from the untrusted zone by a Cisco PIX Firewall. In the case of the Cisco BLISS for T1 network, the most important part of the network that must be protected is the Cisco BTS 10200 Call Agent and the Operations Support System (OSS) servers that provide key business functions. This part of the network requires the best possible protection because an intrusion incident can potentially disrupt service for all users.

PIX Filtering

Cisco PIX Firewalls will not restrict any traffic originating from the trusted zone. Hence, personnel working on OSS platforms can telnet to any part of the network. The Cisco PIX Firewalls are configured to allow only certain types of traffic from the untrusted zone of the network into the trusted zone.

The types of traffic allowed from the untrusted zone are listed below:

- **MGCP traffic**—Signaling messages from voice gateways will be permitted through the Cisco PIX Firewalls. The Cisco PIX Firewall (Version 6.3) can be configured to allow MGCP messaging as an allowed application. In this setup, the Cisco PIX Firewall engine has predefined MGCP exchanges that it understands and permits. The MGCP application of the Cisco CallManager (the Enterprise voice solution) and the Cisco BTS 10200 Call Agent has been tested and proven to work well.
- **ISDN backhaul**—The ports used by voice gateways to communicate with the ISDN stack in the Cisco BTS 10200 will be opened in the Cisco PIX Firewall.
- **SNMP traps**—Traffic destined for the SNMP ports on Network Management workstations (such as CIC) should be allowed.
- **Syslog traffic**—Traffic destined for the syslog server and port will be allowed.
- **Ping**—Ping traffic originating from private addresses within the ISPs network would be allowed. This allows maintenance personnel to test network connectivity from any point within the network.

Note Ping traffic originating from a private address range belonging to an IAD would not be allowed through the Cisco PIX firewall. See the "IAD Risks" section on page 3-4. This prevents potentially malicious users from pinging nodes behind the Cisco PIX firewall.

The Cisco 10000 ESR would be configured to allow a ping to the serial interface. This would allow the IAD user to confirm connectivity with the Cisco 10000 ESR. Maintenance personnel can then confirm connectivity from the Cisco 10000 ESR to any point in the network. If it becomes necessary to confirm connectivity directly from the IAD to a point in the network, the ESR ACLs can be temporarily removed for testing.

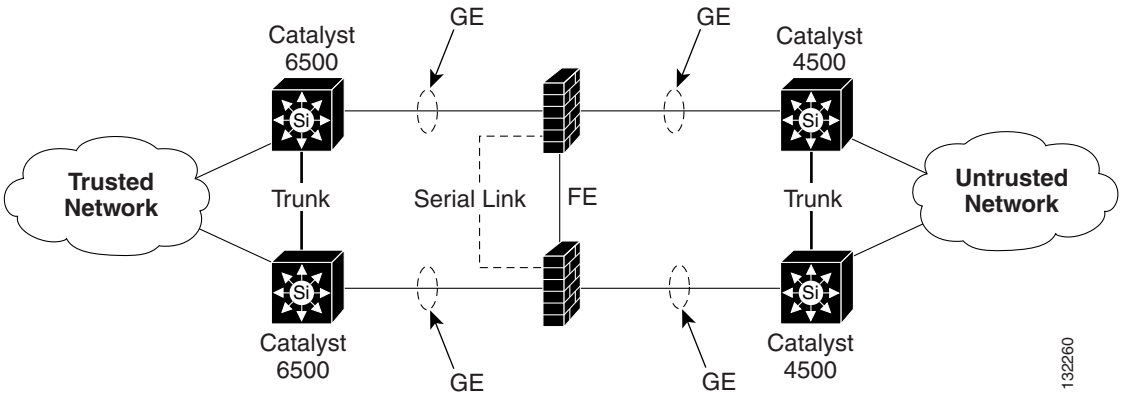
- **TFTP**—Routers within the network will need to originate TFTP sessions to copy Cisco IOS releases from the TFTP server behind the Cisco PIX Firewall to the router.

The current plan would not permit Telnet sessions to originate from the untrusted portion of the network into the area behind the Cisco PIX Firewall. That means that maintenance personnel cannot telnet into a Cisco 10000 ESR, and from the Cisco 10000 ESR telnet to an OSS (or ssh to any point behind the firewall). This helps to protect the Cisco BTS 10200 and OSS if the untrusted portion of the network is breached. Maintenance personnel would be required to originate their Telnet sessions from behind the firewall to other points in the network.

PIX Interconnection Architecture

The Cisco PIX Firewalls are deployed as a redundant pair. The two Cisco PIX Firewalls communicate with each other over a serial link; a dedicated Ethernet connection for stateful operation. If the primary Cisco PIX Firewall fails, the secondary assumes forwarding traffic. The inside and outside LAN interfaces on each Cisco PIX Firewall are connected to an inside and outside VLAN respectively. Routing is handled by the Cisco 6500 switches on the inside and by the Cisco 4500 switches on the outside. Open Shortest Path First (OSPF) is used as the routing protocol to provide path determination as well redundancy.

Figure 3-2 PIX Interconnection Architecture



Untrusted Zone

The Cisco 10000 ESR, Cisco 7206, and Cisco MGX 88xx form the key part of the untrusted zone. The design is to place these three nodes on the same VLAN to allow for fast switching of packets between these devices and minimize jitter and latency. Note that all the internal interfaces on these devices are on private address space. Private address space is the primary mechanism used to protect the untrusted portion of the network from outsiders.

Cisco 7206 Risks

The entry point from the Internet would be via the Cisco 7206, which would require access control lists (ACLs) to perform the following functions:

- Prevent incoming traffic from the Internet destined for a private address. This keeps Internet traffic from hacking any open ports on the private address of a router (Cisco 10000 ESR, Cisco MGX 88xx, or IAD serial interface). Incoming Internet traffic is only allowed to public Internet address space assigned to IADs. The latter is necessary because Cisco BLISS for T1 customers may run servers behind their IADs that need to be accessible to the Internet, such as a web or mail servers.
- Prevent incoming Telnet/SNMP access from any address except those in the OSS private address range. This would keep Internet traffic from attempting to telnet to public IP addresses on the Cisco 7206. This same ACL appears in all routers, and protects the router from access, even if another node in the untrusted part of the network is compromised.
- Prevent incoming traffic from the Internet originating from a private address. This prevents a Denial of Service (DoS) attack from the Internet which attempts to masquerade as coming from a valid internal private address.

IAD Risks

The IAD presents certain risks to the Cisco BLISS for T1 design. Because the IAD is a router located on the customer premise, the service provider does not physically control its network access. Although the vast majority of customers will treat IAD security carefully, it is possible that a customer can break into a router. To prevent a customer from accessing the router configuration through ROMMON, the **no service password-recovery** command can be used. It is also a recommended practice to configure ACLs on the IAD to perform the following functions:

- Prevent incoming traffic from the customer site (via the Ethernet interface) destined for a private address in the Cisco BLISS for T1 network. This prevents customer traffic from reaching the private addresses of any devices in the network. Traffic originating from the IAD Ethernet port is only allowed to travel to devices within the public Internet address space. This also prevents a DoS attack from the customer's network which attempts to masquerade as a valid internal private address.
- Prevent incoming Telnet/SNMP access from any address except those in the OSS private address range. This would keep customers from attempting to telnet to IAD ports on an assigned IP address.

Cisco MGX 88xx

This node does not have traffic originated by client computers and is not a potential source for an attack. We recommend installing an ACL to prevent incoming Telnet/SNMP access from any address except those in the OSS private address range. Using this ACL protects against unauthorized Telnet/SNMP traffic if a privately addressed device is compromised.

Announcement Servers

These nodes should reside behind the Cisco PIX Firewall to afford them the same level of security as other core devices because unavailability can affect large numbers of users. Based on performance numbers, the Cisco PIX 525 can support approximately 1800 Real-Time Protocol (RTP) streams. It is important when passing RTP traffic through the Cisco PIX firewall that you take into account the number of sessions that will have to be supported. The Cisco PIX 535 should be considered where higher capacity is a requirement.

NAT Consideration on IAD

In the Cisco BLISS for T1 network, Network Address Translation (NAT) can be used on the IAD for networks connected to an Ethernet port. Only traffic originating from the Ethernet interface is able to implement NAT. Voice traffic which originates from the IAD is not able to implement NAT. NAT configurations can vary depending on the requirements of the service provider's customer. Possible configurations are as follows:

- **Static Address Translation**—Establishment of a one-to-one mapping between the inside private local addresses and the public global addresses. This static translation is configured in the IAD.
- **Dynamic Source Address Translation**—Establishment of dynamic mapping between the inside private local addresses and public global addresses. This is done by describing local addresses to be translated, the pool of addresses from which to allocate global addresses, and associating the two.
- **Port Address Translation** (PAT)—Conservation of addresses in the pool of global addresses by allowing source ports in TCP connections or UDP conversations to be translated. Different local private addresses will then map to the same public global address, with port translation providing the necessary uniqueness.

  In most cases, PAT is used to translate a range of private addresses that are assigned to the customer to a single public address. There will be cases where customers will require additional public IP addresses, have servers that they want to be publicly accessible, or have applications that do not work with NAT. In these cases NAT alone, NAT in conjunction with PAT, or no translation at all will have to be used to meet customer requirements.

Codec/Compression Alternatives

The G.726-32k, and G.711 codecs were tested as part of the Cisco BLISS for T1 Release 4.0 solution. The decision to use one codec over another is dependent on the amount of bandwidth available for the voice call(s) and the desired quality of the voice call(s). The measurement of quality is based on the Mean Opinion Score (MOS) which is a common benchmark used to determine the quality of sound produced by specific codecs. A higher score indicates a higher level of quality. G.711 has the highest MOS score and uses 64 kbps of bandwidth for a single voice call. G.726 has a lower MOS score than G.711 but only uses 32 kbps of bandwidth per call.

Although it might seem logical from a resource utilization standpoint to convert all calls to low-bit rate codecs to save on infrastructure costs, you should exercise additional care when designing voice networks with low-bit rate compression. One of the main drawbacks is signal distortion due to multiple encodings (called tandem encodings). For example, when a G.729 voice signal is tandem encoded three times, the MOS score drops from 3.92 (very good) to 2.68 (unacceptable). Another drawback is codec-induced delay with low bit-rate codecs.

DNS Redundancy Recommendations

We recommend that Domain Name Service (DNS) be used in a production Cisco BLISS for T1 deployment and that Server Load Balancing (SLB) be used to provide DNS server redundancy.

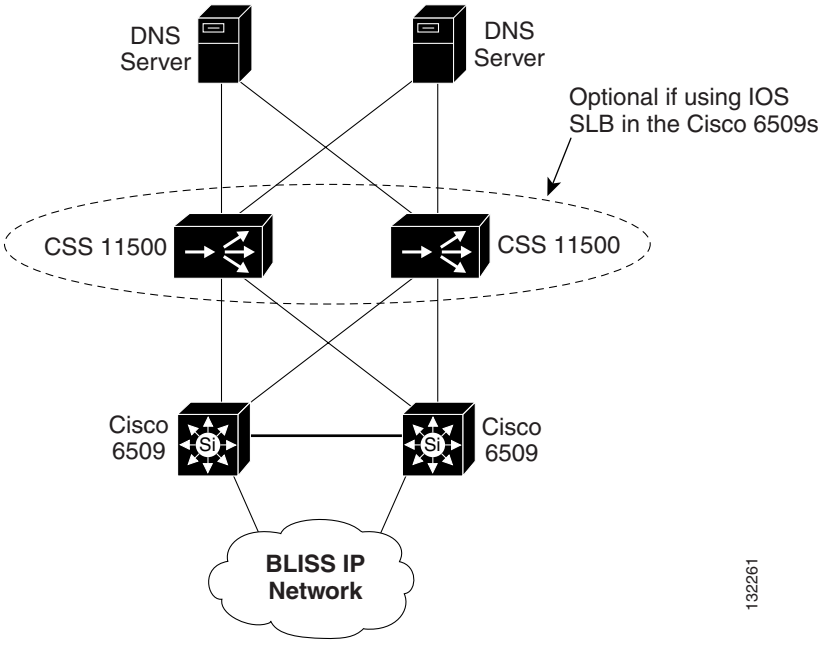
Specifying primary and secondary DNS server names in a device, such as the Cisco BTS 10200 or the IAD:

- results in too much delay in detection of a DNS server failure
- impacts a larger number of devices if a failure occurs
- does not provide adequate control for taking DNS servers in and out of service
- makes the task of readdressing or changing the DNS configuration more complex

By using SLB functionality, either integrated in the Catalyst 6509 or external via CSS 11500 switches, a single DNS IP address (virtual IP address) can be specified in the Cisco BLISS for T1 device, such as the IAD or the Cisco BTS 10200. We recommend that the SLB function be configured using the round-robin load-balancing algorithm. In this way, DNS requests will be distributed evenly over the two DNS servers. If one of the servers fails, only 50 percent of the DNS requests made from the time the server fails until the SLB device detects the failure will be lost.

Figure 3-3 illustrates the use of SLB with external CSS 11500 devices. One could integrate the SLB function into the Catalyst 6509 core switches using IOS SL. The recommended product to provide DNS services is the Cisco Network Registrar (CNR). We also recommend that the DNS servers be dedicated for use by the Cisco BLISS for T1 VoIP network.

Figure 3-3 DNS Configuration with Server Load Balancers



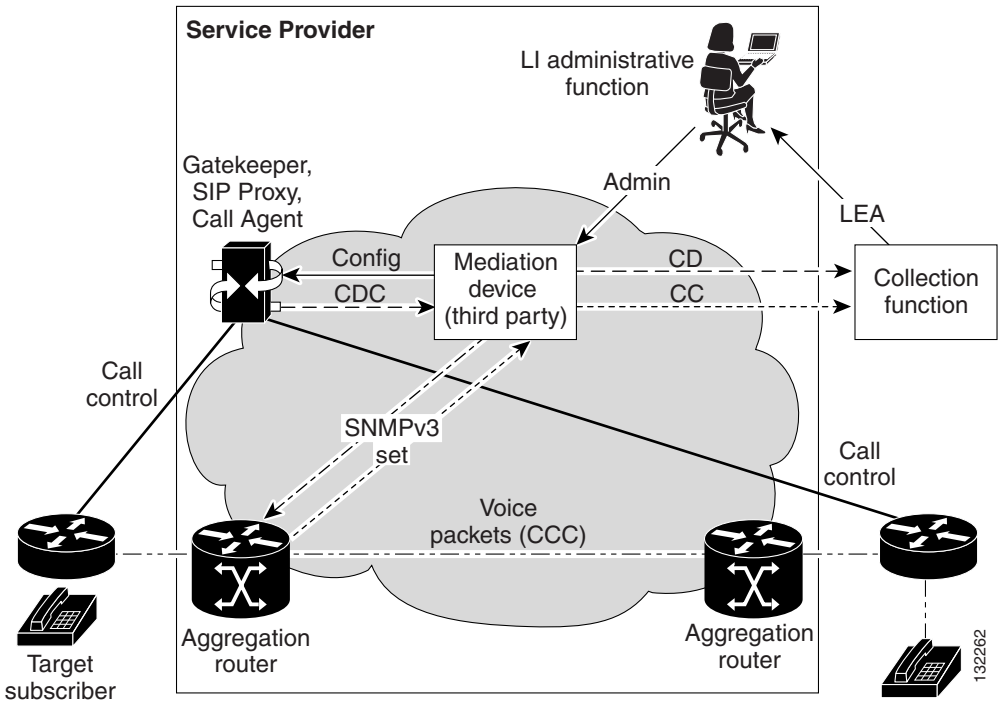
CALEA

The Cisco BLISS for T1 solution provides interfaces for transmission of data used in conjunction with the Communications Assistance for Law Enforcement Act (CALEA). From a design perspective there are no hard guidelines on how the customer must implement the delivery function (DF) server/mediation device other than it must interface with the Cisco BLISS for T1 solution using the Service Independent Interface (SII) specification, as illustrated in Figure 3-4.

Customers have the option to acquire their own DF servers from companies like SS8 or Verint Systems or outsource the DF to a vendor like Fiducianet or Verisign. The advantage of the latter scenario is that the customer does not have to purchase, manage, or maintain the DF server. The typical arrangement is a monthly fee paid to the CALEA service provider with a charge assessed per trace incident. Some other important considerations are as follows:

- In the initial release of the electronic surveillance feature, the default codec was G.711 and there was no support for mid-call codec changes. Support for other codecs, such as G.726, depends on the collection function box being used by the law enforcement agency (LEA). Cisco has tested G.726 with a collection function box and it works well. The collection function box will vary as different LEAs use different collection function boxes.
- In the initial release of the electronic surveillance feature, when both subjects are under surveillance and served by the same access router, if the call is redirected to voicemail the CALEA DF Server must replicate the received call content stream. The replicated call content stream is sent to the LEA because there is only one duplicated voice conversation generated from the edge routers.
- Usage of Service Independent Intercept (SNMP approach) and Packet Cable Intercept (COPS approach) for call-content are mutually exclusive.

Figure 3-4 CALEA Delivery Function

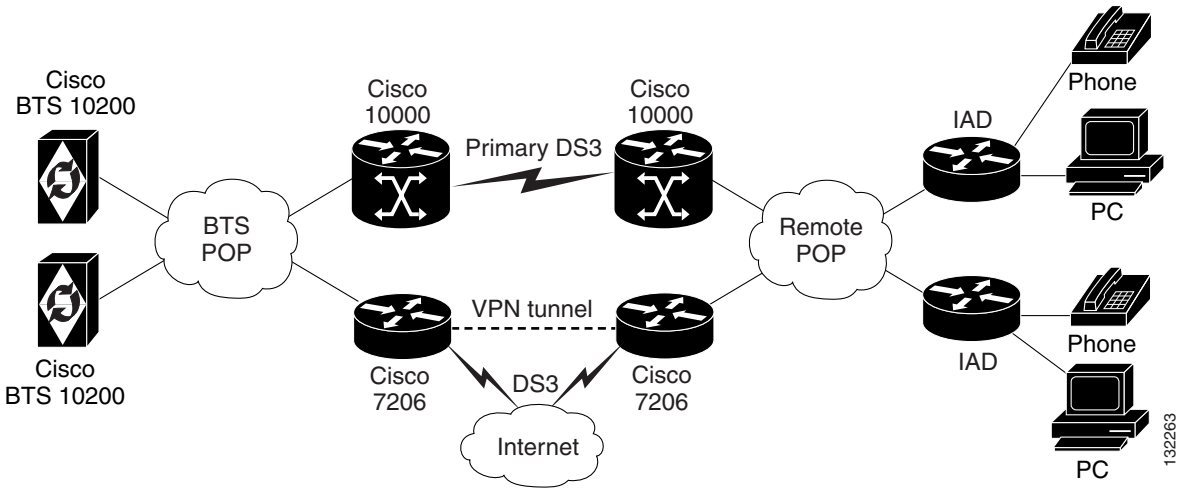


Internet Traffic Engineering Recommendations

The following recommendations are made regarding the Internet connection:

- A full rate DS3 should be provisioned if the customer is going to use the interface as a backup connection to the primary DS3 that connects to the remote POPs. The customer has the option to provision a VPN tunnel over the public Internet as a backup connection, or use a traffic-engineered tunnel from the service provider, as illustrated in Figure 3-5.
- DS3 link utilization should be monitored and capacity augmented when utilization exceeds 80 percent.

Figure 3-5 Internet Connections



Useful Scripts Recommendations

To support operations, we recommend that the Cisco BLISS for T1 customer develop scripts to perform the following functions:

- Control CICs in-service (INS) and out-of-service (OOS) in a particular trunk-group.
- Equip and unequip trunks in a particular trunk-group.
- Compile all messages that went through in the Cisco BTS 10200 logs for a particular originating or terminating phone number.
- Determine whether a CIC in a particular trunk is hung.
- Search on all SS7 messages to see if there are any unusual call failures.
- Script to grep/check for errors in the trace log in the Cisco BTS 10200.

Ancillary Server Recommendations

We recommend that the customer deploy two additional servers in the network: an NFS Server and a login server. These servers provide the functionality deescribed in the following sub-sections.

NFS Server

The NFS server can be any UNIX machine like a Sun Ultra with 40 GB disk space and RAM size like the Cisco BTS 10200 EMS platform. The NFS server has two purposes; namely the flash archiving recommended monthly and Oracle data backup. Ensure that the directory can be shared so the system can have access to it. The NFS server must be on the same subnet as the target Cisco BTS 10200 it serves.

Login Server

The login server acts as a secure gateway for any external user that might want to work on Cisco BTS 10200 or any other products in the Cisco BLISS for T1 network. This helps reduce security risk and also helps vendors, like Cisco, to post any images on this server so that the customer can download the image from here to the corresponding products. Also, if a network down situation occurs, Cisco engineers might need multiple logs and traces from the Cisco BTS 10200 and can just pull them directly from this server rather than stressing the production Cisco BTS 10200. For logs, if you can create separate subdirectories based on days in a month and months in a year, it is easy to go back to that particular directory to view the logs. The memory requirement is 1 GB and disk space of 5 to 10 GB is advisable.

Equipment Power, Space, and Mounting Requirements

The engineer designing the system should use the product datasheets to determine the power, space and mounting requirements for the individual products. Product datasheets can be found on the Cisco website at www.cisco.com.

Voice Traffic Engineering

Voice traffic engineering is used to determine how much voice traffic will be offered to the Cisco BLISS for T1 solution, and to determine the proper sizing of traffic-sensitive parts of the solution. Because Cisco BLISS for T1 is an integrated voice/data solution, there is also a need to properly size parts of the solution to accommodate subscriber Internet data flows. Traffic engineering for the voice application and Internet data traffic engineering are related, as they may share certain components.

This chapter describes the traffic engineering needed to support the voice application. Where there is an associated impact from Internet data flows, this is noted. There is a separate section covering Internet data traffic engineering. It is important to note that voice traffic engineering will differ for each customer depending on design criteria, operational methods, and so forth.

This chapter contains the following sections:

Design Goals

Telephone traffic systems provide a set of network resources that are shared by a large group of subscribers to make phone calls. Certain components in these systems are usually oversubscribed. This means that the system is not sized to allow every subscriber to simultaneously make phone calls to an off-switch location (there are trunk restrictions). Building a system to assure that every subscriber could simultaneously make phone calls to all possible destinations would require that dedicated resources (such as trunks, bandwidth, and so on) be allocated to every single originating line, which is economically prohibitive. This constraint applies for both traditional TDM telephone switches and for new softswitches. This is an acceptable tradeoff, as historical data shows that only a small group of subscribers on a switch needs to make a phone call at any one time.

Typically, the number of users that simultaneously need service varies throughout the day, peaking at a certain hour called the busy hour (BH). The BH can vary based on the day of week (for example, Monday's BH may be higher than all other days), and may vary based on the time of year.

A telephone switch is designed to carry traffic loads offered during a BH with a certain grade of service. The goal of traffic engineering is to size traffic-sensitive components in the switch to provide the desired grade of service. Table 4-1 lists traffic-sensitive components and design goals for the Cisco BLISS for T1 solution.

Table 4-1 Summary of Traffic Engineering Design Goals

Component	Measured Load	Dimensioned Item	Design Goal
Long distance trunk group size	Erlang	Number of trunks	Number of circuits sized for 1% blocking at BH
Local traffic trunk group size	Erlang	Number of trunks	Number of circuits sized for 1% blocking at BH
911 trunk group sizing	Erlang	Number of trunks	Sizing based on customer requirements
SS7 link sizing	Erlang	Number of links	Number of SS7 A-links needed to carry signaling for expected voice loads at BH at ≤ 0.4 Erlang, including A-link redundancy requirements.
Operator Services and Directory Assistance trunks	Erlang	Number of trunks	Number of circuits sized for 1% blocking at BH
Inter-POP DS3	Bps	Number of DS3 facilities and queuing parameters	LLQ sizing **Note** For initial deployment, most customers use the DS3 to transport signaling traffic to/from the Cisco BTS 10200, RTP traffic to/from the Announcement Server, and management traffic to support the nodes in a remote POP. All other traffic egresses at the local POP to the PSTN local or long distance carrier.
Announcement Server	Ports	Number of ports	IP unity ports (Number of simultaneous announcements that can be played)

Trunking Design Methodology

This section describes the methodology used to size the local and long distance trunk groups for initial deployment. The first step is to establish the target engineering forecast timeframe as defined by the customer. Hence, the engineering estimates will size the trunk groups to accommodate traffic for that target timeframe based on customer market forecasts.

The base data for trunk sizing should be provided by the customer and indicate service mix for different service types (PBX, POTS, and so forth), average line/trunks, local minutes, long-distance minutes, and bandwidth consumption for calls.

The design may include the following line types:

- **POTS**—An IAD with standard FXS lines and analog phones
- **POTS-Rotary**—An IAD with standard FXS lines and analog phones, configured as a hunt group in the Cisco BTS 10200
- **PBX-digital PR**—An IAD with a digital PRI interface to a PBX
- **PBX-digital CA**—An IAD with a digital CAS interface to a PBX

The design methodology should estimate the initial deployment load by computing the contribution of a single line (or trunk) toward the traffic offered to the local or long distance trunk group during busy hour (BH). The total offered load to the trunk groups is the contribution of an individual line/trunk type at BH multiplied by the total number of lines of that type.

Note that after the total number of required trunks is computed, you may need to split the required number of trunks into multiple trunk groups (TGs) and hunt through the TGs using a route guide. Having portions of the total egress capacity allocated into smaller trunk groups allows portions of the capacity to be removed from service without completely isolating a POP. This may also prevent "accidents" at the CLI (where someone accidentally forces the wrong TG out of service) from completely isolating a POP.

SS7 Link Sizing

This section describes the methodology used to determine the number of SS7 links required to support Cisco BTS 10200 traffic to/from the PSTN. One key parameter that is required as input to SS7 sizing is an estimate of the total number of calls per second arriving at the Cisco BTS 10200 during BH. Common assumptions that may be used in the calculations are as follows:

- 50 percent of the calls are incoming (all using a standard ISUP call setup sequence). 50 percent of the calls are outgoing.
- Every call originated from an analog line or trunk is destined off-net, either to local or long distance trunks. This results in SS7 messages for every call.
- All outgoing local calls are to exchanges that are portable, hence an LNP query is required. The assumption is that very few dialed numbers will be for numbers ported into the Cisco BTS 10200. Calls dialed to a number ported into the Cisco BTS 10200 should not require an LNP query.
- All outgoing long distance calls will not require LNP queries, just standard ISUP SS7 call setups. LNP for long distance calls, when required, is typically done by the long distance carrier at the switch just prior to delivery of the call to the local exchange carrier (LEC).
- All 800 calls are routed to the long distance carrier, no 800 query or subsequent LNP query for the translated number is required (this will be handled by the long distance carrier).
- Calling Name Delivery (CNAM) may be required for some incoming calls. This would require a CNAM database query.

- CLASS services are not offered between carriers. That means that services such as Automatic Recall do not generate TCAP messaging to local or long distance switches.
- Operator Services/Directory Assistance (OS/DA) calls are routed mobile forwarded (MF) calls (they do not require SS7 signaling).

During a BH, the traffic reaches equilibrium. That means the rate at which new call attempts are made is equal to the rate at which existing calls are terminated. A new call that is in the setup phase will inject the ISUP Initial Address Message (IAM), Address Complete Message (ACM), and Answer Message (ANM) onto the SS7 links.

A call in the terminating phase will contribute REL and RLC messages to the SS7 link. Bcause there is equilibrium at the BH, the total SS7 messaging contributed by a new call setup is all five messages (IAM, ACM, ANM, REL, and RLC). In equilibrium, every new call being launched is matched with a call that is in the teardown phase. Typical sizes for these five message types are listed in Table 4-2.

Table 4-2 Sample SS7 ISUP Message Sizes

Message Type	Approx Size
IAM	43 bytes
ACM	17 bytes
ANM	15 bytes
REL	19 bytes
RLC	14 bytes
Total message byte count for a standard call setup	108 bytes

The total average call rate at BH based on the number lines deployed needs to be calculated. Table 4-3 gives an estimate of the total outbound SS7 load (at 1 cps) for normal outbound calls. The data in the table assumes an average CPS rate of 2.283 cps of which 50 percent are outbound calls (~ 1 cps worth) and will trigger an LNP query in the outbound direction of the SS7 link. It further assumes 50 percent are incoming calls (~1 cps worth) and will trigger a CNAM query in the outbound direction of the SS7 link (assuming all subscribers have CNAM).

Table 4-3 Estimated SS7 Link Usage

Message Type	Approx Size	Comment
Standard SS7 call setup	108 bytes (see Table 4-2)	Incoming and outgoing call rate are assumed equal (1 cps). All outgoing calls are assumed to trigger an LNP query and all incoming calls are assumed to trigger a CNAM query.
LNP query	93 bytes	
CNAM query	68 bytes	
Total per outgoing call	269 bytes	
Total outgoing at 2.283 cps call rate	614.127 bytes (or 4913 bps)	

The SS7 link utilization is dominated in the outbound direction.

614.127 bytes/sec x 8 bits/byte = 4913 bps =0.0877 Erlang
(8.77 percent occupancy on a single 56 kbps SS7 link)

Two A-links are required to meet redundancy requirements, resulting in 4.39 percent occupancy on each A-link.

Note The industry standard design goal for an A-link is ≤ 40 percent occupancy. This lower loading point allows for the failure of any single A-link as the other remaining A-link would still be able to assume the load of the failed link at 80 percent occupancy.

Link Sizing for the VPN Backup Tunnel

This section describes the methodology for sizing the VPN tunnel through the ISP that will carry backup signaling traffic between the POP housing the Cisco BTS 10200 and the individual remote POPs. In the Cisco BLISS for T1 design, a clear channel DS3 is recommended to provide primary connectivity between the Cisco BTS 10200 POP and the remote POPs.

This DS3 will carry the following traffic between the POPs:

- MGCP signaling traffic between the Cisco BTS 10200 and remote gateways. This includes MGCP pings as well as MGCP messages associated with call setup over the course of an average hold-time call, as well as MGCP pings occurring for idle gateways (those not making any calls).
- ISDN backhaul signaling. This is Q.931 traffic from digital PRI IADs that is sent to the Cisco BTS 10200 for call processing. This traffic includes a steady stream of keepalive messages, even when no ISDN call setups are taking place.
- Real Time Protocol (RTP) traffic for calls routed to an announcement server. This is expected to be one-way traffic for callers originating in the remote POP that are routed to an announcement (announcement servers are located in the Cisco BTS 10200 POP).
- SNMP and syslog traffic from routers located in the remote POPs.

If the primary DS3 should fail, the intent is to route the above traffic between the Cisco BTS 10200 POP and the remote POP over a VPN tunnel provided by an ISP. This section provides a method for determining the required characteristics of the tunnel, such as latency and bandwidth, and factors that should be included in the design.

The standard MGCP call setup traffic flows identified above are expected under normal BH operating conditions. It is important to note that MGCP signaling may be temporarily much higher under certain failure conditions. For example, if the Cisco BTS 10200 Softswitch was stopped and restarted (both sides of the duplex system) the resulting endpoint capability exchange may consume a substantial amount of bandwidth in a very short period of time. The potential size of a large-scale gateway restart must be considered, and balanced against the normal operating load of MGCP signaling at BH. The VPN tunnel should be sized to accommodate the larger of the two flows.

MGCP Bandwidth Requirements Under Normal BH Load

The following information is used to compute the MGCP signaling bandwidth at BH. This is similar to the analysis we did previously for SS7 link sizing.

- Capture a sample MGCP ping exchange. This message exchange will occur in the background for every gateway (trunk gateways and IADs), even when the gateway is not involved in a call, and will occur at predetermined intervals. The Cisco BTS 10200 scheduler will schedule pings such that every gateway is pinged within a 10-minute interval.
- Capture a sample MGCP call flow in the lab for a call terminating to an FXS port. Total the number of bytes required for all of these messages in the direction from the Cisco BTS 10200 POP toward the remote POP.

- Capture a sample MGCP call flow in the lab for a call terminating to a PBX-digital CAS trunk. Total the number of bytes required for all of these messages in the direction from the Cisco BTS 10200 POP toward the remote POP.
- Capture a sample MGCP call flow in the lab for a call terminating to a PBX-digital PRI trunk. Total the number of bytes required for all of these messages in the direction from the Cisco BTS 10200 POP toward the remote POP.

Note The PBX-digital PRI requires some MGCP messages, but most of the call setup uses ISDN backhaul. The GW will terminate the PBX Q.921 layer, and will backhaul the Q.931 layer of the signaling channel back to the Cisco BTS 10200 using Reliable UDP (RUDP). This is referred to as an "ISDN backhaul."

There are frequent message exchanges (keepalive messages) between the gateway and Cisco BTS 10200, even when there are no call setups. Therefore, there is "idle" traffic seen at all times (similar to MGCP ping). The ISDN messaging is used to perform call setup between the IAD and the interconnected PBX. The MGCP messaging is used to supply the IAD with information about the far end gateway that it must communicate with over the IP network. The PRI IAD is sent a CRCX which has a Session Description Parameter (SDP) that tells it the far-end IP address and port number with which to setup the RTP stream.

- Capture a sample MGCP call flow in the lab for an incoming call that is forwarded to a PSTN number. Note that extra MDCX messages are expected here. Total the number of bytes required for all of these messages in the direction from the Cisco BTS 10200 POP toward the remote POP.

  The dominant direction is from the Cisco BTS 10200 toward the remote POP, as this direction is expected to carry large messages, such as RQNT, CRCX, and MDCX. The gateways in the remote POP typically reply with very small ACK messages; however, some ACK messages are bigger than others. Specifically, ACK messages sent in response to a CRCX can include a gateway-provided SDP parameter, which can make this particular ACK message much larger than the others. This effect is included when totaling the bandwidth for the individual call flows.

  NTFY messages sent from the remote POP are also expected to be much smaller.

  Table 4-4 shows the size of the MGCP call flow for different call setup scenarios as described in the Comments column. These were captured from various releases of the Cisco BTS 10200 software. While the Cisco BTS 10200 releases are different, the call flow size is sufficiently accurate to determine the approximate bandwidth requirements.

Table 4-4 Sample MGCP and ISDN Backhaul Message Flow Sizes

Call Flow	Cisco BTS 10200 Release	Number of msgs	Cisco BTS 10200 to GW	Comment
MGCP Ping	3.5.1	2	126 bytes	Actual AUEP=96 bytes. Extra bytes are included because the sample endpoint ID was only the IP address. Most endpoint IDs ~50 characters.

Table 4-4 Sample MGCP and ISDN Backhaul Message Flow Sizes (continued)

Call Flow	Cisco BTS 10200 Release	Number of msgs	Cisco BTS 10200 to GW	Comment
FXS-FXS	3.5.1	58	3172 bytes	Because this flow originates from an IAD endpoint and terminates to an IAD endpoint, the required NTFY and RQNT to originate the call are included. When the call terminates, additional NTFY and RQNT messages are required to manage the terminating endpoint's answer and hang up. If the call flow is used to represent an off-net call, the portion terminating to the TGW for egress to the PSTN would not use the NTFY and RQNT at the terminating endpoint. Hence, this call flow includes extra messages not found in an off-net call. However, it puts an upper bound on the required bandwidth for an off-net call. This flow is used to approximate the size of a POTS call off-net, a POTS-Rotary call, or a POTs-analog call to off-net locations. The call flow size would be similar for incoming calls from the PSTN terminating to these line types.
PBX-digital PRI	2.1v24	5	202 bytes	This is the "idle" keepalive traffic for an ISDN backhaul. It includes the keepalive messages to both the primary port and backup port on a single CA. Because this idle traffic would also appear on the secondary CA (the backup CA), it is doubled to compute the net traffic flow to a duplex Cisco BTS 10200.
PBX-digital call setup	2.1v24	12	1810 bytes	This includes a CRCX and 200 SDP to set up the packet side of the call (and the DLCX and 250 ACK for teardown). The ISDN backhaul has Q.931 encoded in the messages. They are much smaller than MGCP messages, due to the non-ASCII encoding.
PBX-digital CAS	2.1v24	52	3983 bytes	This call originates from an IAD endpoint and terminates to a PBX on an IAD-CAS. This call flow is used to aspproximate the size of a PBX-digital CAS call (on-net and off-net to the PSTN). It is larger than a call incoming/outgoing through a TGW because the TGW would not require the NTFY and RQNT messages used to manage the IAD endpoint (as applied in the captured sample flow).
CFNA FXS to FXS	3.5.1	62	6065 bytes	This call flow originated from a port A on an IAD, terminating to port B. The call was allowed to ring with no answer, and was forwarded to port C. This call flow results in additional MDCX messages, because the original termination at port B must be made MDCX inactive, then the connection must be deleted (DLCX), and a new termination must be cross-connected (CRCX) at port C. This call flow is used to approximate the size of an incoming call from the PSTN that is forwarded to another termination (another TGW endpoint). The sample call flow is bigger because the TGW portion would not require the NTFY and RQNT messages used to manage the IAD endpoints. **Note** This sample flow also had some message retransmits in it (increasing the size beyond a normal CFNA flow).

Table 4-5 shows the expected MGCP signaling for each line type in a given population of *n* lines. The following is computed on this table:

- Based on the number of lines of each type (and the number of lines for a particular IAD type), the number of MGCP GWs can be estimated. For example, if there are 10 POTS lines deployed, and there are 8 lines / POTS IAD, then 1.25 MGCP GWs are used for POTS.

  This process continues for all line types to find the total number of MGCP GWs. This method is only used as an approximation, because it is obviously not possible to have fractions of a gateway. This number is used to compute the number of MGCP pings seen in the network over the 10-minute ping interval.

- A similar calculation determines how many PBX-digital PRI GWs are deployed. This is used, in turn, to determine how many ISDN backhaul sessions will be active (even at idle), and the required bandwidth necessary to support the keepalive messages.

- Using the approximated call flow samples, and the per-line contribution to the call rate at BH, the average MGCP signaling for each type of line can be estimated. The MGCP signaling for the different line types is **summed** to form the Total Estimated Average Signaling.

- A "safety factor" is then multiplied by the Total Estimated Avg Signaling to form the column "Total Estimated Average Signaling (with safety factor)." This safety factor is quite large (x10 is used in this calculation).

  This safety factor is large for the following reasons:

  - The calls arrive in a Poisson distribution (standard telephony assumption), which means bursts of call arrivals as high as 6 (.05% probability) could occur. During these bursts, the average bandwidth required would be 6 times higher than normal.
  - The sample call flows use an endpoint identifier that is extremely short (from a lab setup). Real endpoint identifiers will be substantially longer.
  - The sample call flows frequently used very short transaction identifiers (these are randomly chosen). In a real network these could increase the length of each message by a few bytes).
  - The sample call flows are samples used to obtain a baseline number. Other call flows may be found in the real network that are not predicted.

Table 4-5 Example MGCP and ISDN Backhaul Signaling Bandwidth Calculations

Total Number of Lines (per POP)	Estimated Number of MGCP GWs	MGCP Ping Intrval (secs)	MGCP Ping Avg BW (bps)	Number of Digital-PRI MGWs	Idle ISDN Backhaul Avg BW (bps)	Est Avg Signaling BW for POTS, POTS-Rotary, PBX-analog	Est Avg Signaling BW PBX digital PRI	Est Avg Signaling BW for PBX-CAS	Est Avg Signal CFNA (vmail)	Est Avg Signaling for vmail check	Est Avg Signaling BW (excludes Centrex-IP)	Total Est Avg Signal flow (with safety factor)	Cisco BTS 10200 Restart Time (160 endpts/ sec)	Avg MGCP load for recovery
100.000	8.583	4194.175	0.240	1.250	4040	2698.597	428.387	314.229	16.760	164.239	7662.452	76624.516	0.625	1333760
200.000	17.167	2097.087	0.481	2.500	8080	5397.193	856.774	628.458	33.519	328.478	15324.903	153249.031	1.250	1333760
300.000	25.750	1398.058	0.721	3.750	12120	8095.790	1285.160	942.688	50.279	492.717	22987.355	229873.547	1.875	1333760
400.000	34.333	1048.544	0.961	5.000	16160	10794.386	1713.547	1256.917	67.038	656.956	30649.806	306498.063	2.500	1333760
500.000	42.917	838.835	1.202	6.250	20200	13492.983	2141.934	1571.146	83.798	821.196	38312.258	383122.578	3.125	1333760
600.000	51.500	699.029	1.442	7.500	24240	16191.580	2570.321	1885.375	100.557	985.435	45974.709	459747.094	3.750	1333760
700.000	60.083	599.168	1.682	8.750	28280	18890.176	2998.707	2199.604	117.317	1149.674	53637.161	536371.610	4.375	1333760
800.000	68.667	524.272	1.923	10.000	32320	21588.773	3427.094	2513.834	134.076	1313.913	61299.613	612996.125	5.000	1333760
900.000	77.250	466.019	2.163	11.250	36360	24287.370	3855.481	2828.063	150.836	1478.152	68962.064	689620.641	5.625	1333760
1000.000	85.833	419.417	2.403	12.500	40400	26985.966	4283.868	3142.292	167.595	1642.391	76624.516	766245.157	6.250	1333760

Cisco BTS 10200 Restart and Large-Scale Events

The computation of average MGCP signaling bandwidth is shown as one factor that must be considered in sizing the VPN tunnel. Certain failure events will result in a large number of MGCP messages being exchanged between the Cisco BTS 10200 and GWs. If the Cisco BTS 10200 is restarted (both sides in the duplex system), it will audit every endpoint in the network for its full capabilities. The response from the endpoint is large (978 bytes from a sample call flow in the lab). Because every endpoint is hit with this AUEP message, there can be a large MGCP load generated. The Cisco BTS 10200 will pace this restoration procedure using two parameters in the Call Agent configuration (ca-config) table (mgcp-init-duration and mgcp-init-terms). The Cisco BTS 10200 will attempt to recover the number of terminations specified in mgcp-init-terms during the time interval specified in mgcp-init-duration. The default values will recover 160 endpoints in 1 second. Table 4-5 shows that the bandwidth required to support this recovery activity far exceeds the average bandwidth requirements for normal MGCP signaling at BH.

The computation of this number uses:

Avg_MGCP_recovery_load = 160 x [978 + 64] = 160 x 1042 = 166720 bytes

where:

160 = number of terminations recovered in 1 second

978 = number of bytes in an Audit Endpoint (AUEP) response (full capability)

64 = number of bytes for the ESP header

Avg_MGCP_recovery_bitrate=166720 bytes x 8bits/byte = 1333760 bps

Calculation of the MGCP signaling for normal call setup includes the following:

- 14-byte Ethernet header (this would not be present on a DS3 facility, but would be replaced by a 6-byte PPP header). For the purpose of estimating bandwidth, this is almost an even exchange.
- The 64-byte ESP header is not included in the MGCP signaling. Because the MGCP recovery dominates the signaling needs, it was not necessary to compute these numbers with an IPSEC header.

Network Management Bandwidth Requirements for a Remote POP

This section describes calculating the network management bandwidth requirements for a remote POP.

SNMP Traffic

To monitor the remote POP, SNMP polls and traps are collected from the remote nodes (ESR, MGX, AS5850, and so on). SNMP traps are not typically collected from IADs. The customer premise equipment usually logs messages to the logging buffer, and uses the syslog facility to transmit warnings back to the data center (syslog requirements are discussed in the next section).

The polls are conducted every 60 minutes and take approximately 90 seconds to complete (there are 30 pollable items in the MGX MIB). The polls are issued at a rate of approximately one every 3 seconds. The response to the poll is a protocol data unit (PDU) of 796 bytes (largest PDU for the MGX shelf).

Existing experience with a similar network uses the rule of thumb that there is one trap generated every interval of time that corresponds to three poll cycles (for example, approximately one trap every 9 seconds). The maximum trap size is also 796 bytes (PDU size). Hence, the average rate at which SNMP data is exchanged is very low.

A 796-byte SNMP PDU has 20 bytes (IP header), 8 bytes (UDP header), 64 bytes (IPSEC header) = 888 bytes. There is essentially one 888-byte packet sent every 3 seconds during a poll interval (for the next 90 seconds) every 60 minutes. In addition, one 888-byte trap is sent every 9 seconds.

However, calculating the bandwidth capacity for the average SNMP load will result in a serious underestimation when unforeseen events occur. In a critical failure, a large number of SNMP traps could get generated by the MGX shelf in a very short period of time. Many messages would be lost if the bandwidth is sized for an average network management scenario (normal polls/traps.). At a time when it is most important to know what is happening in the network, there will be a loss of information.

To avoid this problem, the bandwidth should be engineered to meet the needs of a critical situation. However, it is very difficult to foresee the peak SNMP load under all possible failure conditions. As an estimate, it is assumed that a catastrophic event could occur on one of the remote POP nodes where up to 100 SNMP traps are sent in a 1-second interval. This would result in an average bandwidth requirement of snmp_bandwidth = 100 x 888 bytes/msg = 88800 bytes = 710400 bps.

Note The assumption is that there is one node affected at the remote POP that causes this high traffic activity. Events can occur that affect more than one node at the remote POP. If multiple nodes were to start spewing SNMP traps at this rate, some messages may be lost.

Syslog Traffic

IADs are monitored remotely by forwarding warning messages to a syslog server at the data center. The IAD is also configured to write messages of informational level (or above) to the logging buffer. This buffer can be retrieved to help diagnose customer issues. In a similar philosophy to the SNMP sizing, the bandwidth should be sized to accommodate the traffic from an event that may affect multiple IADs. (that is, it is not uncommon for multiple IADs to be affected by a power outage, resulting in T1 outages and PBX signaling link failures).

The following assumptions are used to determine the syslog load:

- Based on existing traces from such an event, each syslog message is estimated to be ~ 500 characters (total packet size must add the 20-byte IP header, 8-byte UDP header, 64-byte VPN header) = 592 bytes total per syslog message.
- 60 GWs are present at 700 lines per deployment.
- A failure event affects 25 percent of all GWs.

Based on the above assumption, the required syslog bandwidth is computed as:

syslog_bandwidth = 60 x .25 x 592 bytes/msg x 10 msgs/event x 8 bits/byte = 710400 bps

Reserved Bandwidth for Telnet Sessions

It is important to be able to log in and remotely control equipment at the remote POP. While equipment like the MGX and ESR will have remote dial-in capabilities, CPE equipment like the IAD is only reachable via Telnet. Ensure Telnet capability into remote CPE is provided in case of an emergency. Hence, bandwidth should be allocated for these sessions.

To determine the bandwidth needed to support a Telnet session, the following assumptions were made:

- The goal is to provide an equivalent 9600-bps connection via Telnet (1200 characters/sec)
- From a sample snoop trace of a Telnet session (show run conducted on a router), Telnet packets are 590 bytes (breaking the output of show run into multiple packets). This is a 536-byte payload, with a 14-byte Ethernet header, 20-byte IP header, and a 20-byte TCP header.

- To achieve a 1200-cps throughput, there will need to be:

  telnet_packet_thruput = 1200 chars ÷ 536 chars/packet = 2.23 packets_per_second

  telnet_bandwidth_per_session = 2.23 x [590 + 64] = 1464 bytes/sec = 11713 bps

  590 bytes assumes that the Ethernet header (14 bytes) and 6-byte PPP header are approximately a wash. The 64-byte IPSEC header is then added.

- Allocating enough bandwidth to serve four simultaneous Telnet sessions:

  telnet_bandwidth = 11713 bps x 4 sessions = 46853 bps

RTP Streams to Announcement Server

If a call is incoming at the remote POP and must be routed to the announcement server (AS), it is normally carried on the private facility DS3 link between the Cisco BTS 10200 POP and the remote POP. If that link fails, the RTP stream for these announcements will be routed into the VPN tunnel.

Bandwidth must be allocated for these announcements. Using the publicly available bandwidth calculator on CCO, the required bandwidth for a G.726 (32k) call is 80,222 bps. This factors in a 64-byte IPSEC header on PPP links at a packet rate of 50 packets per second.

Table 4-6 shows the expected rate at which callers will route to the announcement server.

Table 4-6 Estimated Announcement Server Port Requirements

Total Number of Lines (per POP)	Calls to AS at BH (ATB and other causes)	Number of ERL traffic to AS at BH	Number of AS ports	Estimated Number of of MGCP GWs
100	47.367	0.197	4	8.583
200	94.734	0.395	4	17.167
300	142.101	0.592	5	25.750
400	189.468	0.789	6	34.333
500	236.835	0.987	6	42.917
600	284.203	1.184	7	51.500
700	331.570	1.382	7	60.083
800	378.937	1.579	8	68.667
900	426.304	1.776	8	77.250
1000	473.671	1.974	8	85.833

Note The example numbers in Table 4-6 are using a failure rate of 4 percent on calls. Because the trunk groups were engineered for 1 percent blocking at BH, it is expected that at least 1 percent of call attempts at BH will need an announcement. The other 3 percent were allocated for miscellaneous other causes.

Computing the required RTP bandwidth for 700 lines is shown by:

AS_bandwidth = 7 x 80222 bps/announcement = 561554 bps

VPN Tunnel Bandwidth Requirements

Table 4-7 summarizes the bandwidth requirements described in the preceding sections.

Table 4-7 Estimated Total Average VPN Bandwidth Required

Function	Average Bandwidth Requirements	Comment
MGCP Signaling	1333760 bps	Dominated by Cisco BTS 10200 endpoint recovery (paced at 160 terminations /sec)
SNMP Traffic	710400 bps	Allows for worst case loading of 100 SNMP traps/sec (796 byte PDU size)
Syslog Traffic	710400 bps	Assumes 60 GWs, 25% involved in an event, 10 messages per event, 592 chars/msg
Telnet Sessions	46853 bps	Assumes 9600 bps emulation rate, 4 simultaneous sessions
RTP streams for AS	561554 bps	Assumes 7 simultaneous users of AS, g726(32k) compression
Total	3362967 bps (3.37 Mbps)	
Safety factor x2	6725934 bps (6.73 Mbps)	Safety factor covers: • Unforeseen events (need to change recovery rates, increase AS ports, Telnet sessions, increased SNMP or syslog usage) • Uncontrollable burst rates from Cisco BTS 10200 or GW (see Instantaneous Bandwidth)

VPN Tunnel Bandwidth Characteristics

The following bandwidth characteristics are required for the VPN backup tunnel.

Instantaneous Bandwidth

The bandwidth requirements for the functions in Table 4-7are listed as “average bandwidth.” There is a difference between the average bandwidth required and the instantaneous bandwidth required. This is particularly important for the MGCP signaling.

The average bandwidth assumes all packet arrivals are spaced evenly apart, when in reality the packets do not arrive evenly spaced in time. When the Cisco BTS 10200 does a recovery (or sends out a burst of MGCP messages for signaling), it sends at the rate limited by the local media (FastEthernet). The Cisco BTS 10200 or GW will not know there is a bandwidth-constrained tunnel elsewhere in the network. So while the bandwidth used over a longer interval of time conforms to the average, over a short space of time it may far exceed that.

The service provider (SP) providing the tunnel must allow for these bursts without discarding the packets (particularly the signaling). SPs will typically police an input from the edge. If the flow does not conform to the contract, packets will be discarded. Even though the average bit rates are specified, it is necessary to burst up to line rate for some period of time (the longer the period allowed for the burst, the better). The x2 safety factor also helps to provide some "slack" to ensure the bursts do not exceed policing.

This is one difference between a privately owned DS3 and a VPN tunnel. The private DS3 would not be policed for the MGCP flow. If there are no other users (for example, Priority Queue voice packets) on the DS3 competing for the bandwidth (the DS3 is not congested), the MGCP signaling flow can burst at line rate indefinitely.

If the tunnel is policed at a hard rate (based on the average), it is possible that a burst of MGCP packets (sent at FastEthernet rates by the Cisco BTS 10200) will get discarded by the SP. This is an undesirable outcome, as the loss of packets will cause retransmission (generating more packets and increasing the average bandwidth utilization). If enough messages are lost, call setups may fail. It is also possible that lost messages will place trunks or terminations into "hung" states, where manual intervention is necessary to restore them.

It may be possible to traffic shape the MGCP signaling, but there are finite limits to this, as the queue depth for the traffic shaper will be finite. A traffic shaper is a queuing mechanism where the output of the queue is controlled to conform to the contracted rate. Incoming bursts beyond the contract rate are temporarily queued, and will eventually be sent. However, the queued packet will incur additional delay and once the input queue fills, messages will be discarded. The degree to which the Cisco BTS 10200 will cause bursting (especially in recovery) is unknown. It may be possible to compensate with traffic shaping – or it may not be.

Other traffic flows such as syslog and SNMP can also have large bursts in excess of their average rates. Traffic shaping/policing may be necessary on the output queue to prevent these applications from consuming bandwidth allocated to MGCP signaling.

Message Latency

Another key tunnel characteristic that must be controlled is message latency. MGCP messages must be acknowledged within 400 ms, or they will be retransmitted. In addition, the VPN tunnel will also carry ISDN backhaul signaling. ISDN Layer 3 traffic from IAD-digital PRI units is encapsulated in Reliable UDP (RUDP) messages and sent to the Call Agent. RUDP messages are retransmitted after 300 ms (and more than two retransmissions will cause the backhaul link to go out of service). ISDN backhaul messages should also be sequenced properly, as RUDP is attempting to maintain the message ordering normally provided by the ISDN Q.921 layer. Out of sequence RUDP messages can still be acknowledged, but it drives up the bandwidth utilization because the external ACKs (EACKS) are bigger and is undesirable.

The processing delay for the Cisco BTS 10200 and GWs are probably very small for a new deployment. However, as traffic increases, the processing delays for both nodes could increase. As an estimate, it is probably desirable to allow for 250 ms of processing between the nodes at each end. This would allow 150 ms (400 ms – 250 ms = 150 ms) for the round trip delay across the tunnel. This implies the one-way delay should probably not exceed 75 ms. A shorter delay is more desirable.

Note This latency figure assumes that interactive voice services are *not* being provided on the VPN tunnel. In this sizing exercise, this figure is chosen based on signaling needs. Interactive voice conversations are highly susceptible to delay. Excessive delays (> 150 ms one way) can result in speakers talking over each other. If future needs change such that the VPN tunnel is intended to carry interactive voice, this figure needs to be revisited. In this case, the figure may be heavily influenced by the need to stay within the 150-ms voice budget. The announcement server traffic is one way (there is no interaction), and less sensitive to the delay, although excessive delay could still exacerbate existing echo issues.

Message Loss Rate

Message loss rates within the tunnel must be extremely low, which assumes that the MGCP packet has made it past the policer (the issue described in item 1 above). The exact rate at which the loss becomes unacceptable is not known.

Message Sequencing

The tunnel must support message sequencing to prevent ISDN backhaul signaling from arriving out of sequence.

Recommendations for Future Engineering

Overcoming Noncoincident Busy Hours

The method described in this chapter computes total offered load at BH by multiplying the contribution of each line type by the number of lines (of that type), then summing across all line types. This provides a reasonable initial estimate of offered load. However, it is a rather conservative figure because it assumes that all lines will be active and contributing during the BH.

In reality, if there are several lines at a small business, not all of them may be active during the BH. For example, some personnel may be on vacation, working from home, or perhaps a user comes in on a staggered shift (thereby offsetting his individual BH from the overall BH of the switch). The extent to which this happens may vary depending on the nature of the subscribers, and cannot be quantified. Hence, if the estimated total offered load were 20 Erlangs at BH (computed using proposed methods), the observed offered load at BH may only be 15 Erlangs.

To accommodate the possible “noncoincidence” of the BH for individual lines and other usage characteristics outside the initial assumptions, it is proposed that the future traffic engineering methodology measure the actual offered load for groups of 100 to 200 lines/trunks. Instead of measuring the impact of any single line on the trunk group load, the impact of a group of lines is measured. This observed value would include the effects of noncoincidence in individual BH for lines in that group. The future traffic engineering methodology would be used once real trunk group (or CDR) data became available for analysis. This will yield a more accurate picture of true usage. The trunk groups would then be engineered based on the expected addition of 100 to 200 lines.

Note The effects of noncoincident BH may be small, because the target group of small business users probably has a consistent work schedule. This effect may be more evident as the mix of users grows to include multiple dwelling units (residential subscribers), whose usage patterns may differ from small business.

Call Centers and Telemarketing Applications

The models described in this document are useful for initial engineering for a population of normal business users, particularly for the case where all PSTN flows egress at the POP where a call originates.

In cases where large nationwide business subscribers are placed on the network, it is important to have prior knowledge about major call flows for this subscriber, particularly if the subscriber runs call centers or telemarketing applications. This would require obtaining traffic information from the subscriber before they are placed on the network. Large subscribers running these kinds of applications may contribute significant amounts of traffic onto the network, potentially contributing to loads in excess of planned BH levels, which may disrupt the service quality seen by other subscribers. The potential concerns are listed below:

- Call centers are typically the focal point for large streams of incoming traffic. For example, assume that a customer begins providing service for a chain of department stores. This department store chain runs a credit center that grants credit to customers and maintains a call center where store employees may call to check customer credit or grant new credit on the spot. A call center like this may funnel large loads toward a particular POP where the call center resides. This could affect the amount of bandwidth required between POP sites. During peak seasons, such as Christmas, this call center may see especially heavy loads.
- Telemarketing applications are usually on the line continuously, over the hour, and may contribute minutes of usage/line well beyond the 20 minutes at BH used in the engineering estimate.

Fax and Dial-Up Modem Traffic

Fax and modem service on Cisco BLISS for T1 is currently provided using modem and fax passthrough. This means that certain frequency tones unique to FAX and modem are detected by the gateway's DSP chip and are used to load a G.711 codec. G.711 can transparently digitize fax and modem analog signals for the end user. However, this means that the bandwidth requirements for a fax/modem call (~91 kbps) are greater than that for a normal voice call (~58 kbps).

For the initial deployment, voice traffic is usually not carried inter-core on IP links. All off-net traffic is routed via the PSTN. On-net to on-net calls are routed over LAN facilities (there are no fax/modem or interactive voice calls carried on WAN facilities). At initial deployment, the only WAN facility that will carry fax/modem and voice calls will be the T1 drop to the customer premise. This link will require QoS settings to place fax/modem and voice packets into a Priority Queue (PQ).

PQ provides expedited queuing for these packets to reduce latency and jitter for these call types. The bandwidth requirements are different for these call types. The problem in sizing PQ is that the amount of fax/modem traffic over the T1 link is not known prior to deployment. It is desirable to accommodate the worst case scenario where all calls are fax/modem (a very low probability event), but this implies the PQ must be sized to accommodate the case where all voice channels require the G.711 codec.

For the case of an 8-line analog FXS IAD, this is not an issue. Allocating the full 91 kbps for the worst-case scenario (all calls are fax/modem) would only require 728 kbps. PQ can be easily configured for this with plenty of extra bandwidth. If the calls are all G.726 (58 kbps), only 464 kbps of the allocated PQ bandwidth would be used. The unused portion of the bandwidth could be configured to be dynamically allocated for other purposes (if so desired).

However, in the case of a 24-channel digital PRI or CAS IAD, this would imply 24 x 91 kbps = 2.184 Mbps, which is more bandwidth than is available over the T1. Hence, it is not possible to accommodate the scenario where all channels of a digital PRI/CAS IAD are using fax/modem.

There are several problems to deal with when deploying a digital PRI/CAS IAD (from a bandwidth perspective):

- The requirements if all 24 channels are used for G.726 voice at 58 kbps would be 1.392 Mbps. This equates to ~90 percent of the T1 bandwidth allocated to PQ, and 4 percent allocated to signaling, with the remainder allocated to other users of the link (for example, Internet data). This means that 1.392 Mbps is reserved to handle voice calls. Technically, it is possible to deploy a 24-channel digital PRI/CAS IAD and carry voice on all 24 channels. However, there would be only 92 kbps left to run Internet data.

  1.5336 Mbps – 1.392 Mbps (voice) – 61 kbps (signaling) = 92 kbps

  In this scenario, the customer's Internet data would be running extremely slow.

- Assuming that only one T1 WAN link is used, the 1.392 Mbps bandwidth is consumed in different chunks, depending on whether the call is G.726 (~58 kbps) or if the call is fax/modem (~91kbps). Once the bandwidth in PQ is exhausted, the call may proceed with call setup, but packets may be dropped. For example, 22 voice calls + 2 fax/modem calls = [22 x 58 kbps] + [2 x 91 kbps] = 1.458 Mbps. This will oversubscribe the amount of reserved bandwidth in PQ (1.392 Mbps), resulting in packet drops. There is no method currently used in existing production deployments, to perform per-call, call admission control at the gateway.

- For scenarios where a full 24 trunks are provided to the customer premises, it may be required that Multilink PPP (MLPPP) be used to ensure adequate bandwidth to accommodate a variable number of fax/modem calls. Assuming the worst case (all calls are fax/modem), would require that 2.184 Mbps be set aside in PQ. There is 3.06 Mbps of bandwidth available on an MLPPP configuration, allowing ~822 kbps to be used for Internet data (3.06 Mbps – 2.184 Mbps (voice) – 61 kbps (signaling) = 822 kbps).

Configuring the Solution

This chapter covers configuration and provisioning of the major components of the Cisco BLISS for T1 solution where those configurations and provisioning are unique to the solution. For general component configuration guidance, refer to the documentation on the Cisco Technical Support & Documentation website located at http://www.cisco.com/en/US/support/index.html.

This chapter includes the following sections:

Configuring the Cisco BTS 10200 Softswitch

To configure the Cisco BTS 10200 Softswitch, perform the following steps:

Step 1 Fill out the Building Environment and Power Site Survey and Network Site Survey (NSS) for Release 4.4. These are downloadable Microsoft Word documents that you can edit to include the information for your network. You can download them from the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/bts10200/bts4_4/install/surveys/index.htm

Step 2 Install the Cisco BTS 10200 Softswitch server hardware, Cisco 2950 switches, and Catalyst 6500 switches. Perform the cabling and initial configuration per the *Cabling and IRDP-Setup Procedure for 4-2 Configuration* located at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/bts10200/bts4_4/install/index.htm

Step 3 Jumpstart the Cisco BTS 10200 hardware. This installs the Sun operating system, file systems, and necessary patches to the Sun servers. The *Cisco BTS 10200 CD Jumpstart Procedure* is located at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/bts10200/bts4_4/install/index.htm

Step 4 Install the Call Agent/Feature Server and Element Management System software on the Cisco BTS 10200 servers as documented in the *Application Installation Procedure* located at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/bts10200/bts4_4/install/index.htm

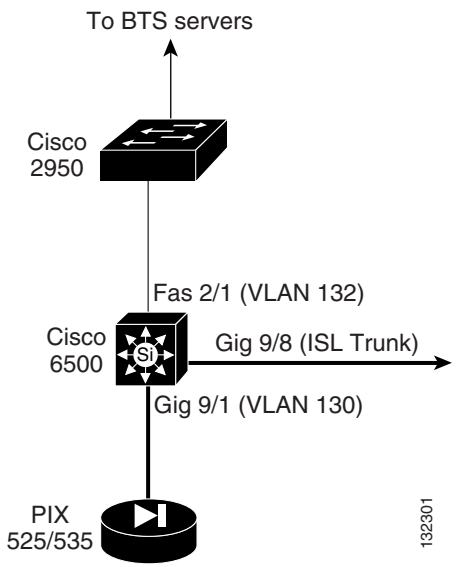
Upon completion of this procedure, the Cisco BTS 10200 software can be started and voice services provisioning can begin.

Configuring the Catalyst 6509

General setup of the Catalyst 6509 switch involves configuring the interfaces, VLANs, and routing protocols to support the network design developed prior to this installation. Figure 5-1 shows the interfaces to the Catalyst 6509 switch. Following Figure 5-11 are excerpts from a Catalyst 6509 configuration that illustrate the items that have to be configured to support the Cisco BLISS for T1 solution. Only those items that are unique to the Cisco BLISS T1 solution are highlighted. For general guidance on configuring the Catalyst 6509 switch, refer to the Cisco documentation located at http://www.cisco.com/univercd/home/home.htm.

Note These configurations are for reference only. Customer requirements might dictate something different.

Figure 5-1 Reference Diagram for Catalyst 6509 Configuration




```
!< Begin Configuration >
Current configuration: 36344 bytes
…
!< The class map section below defines 3 traffic classes for voice signaling, voice
bearer, and telnet traffic. There are a couple of approaches that can be used to do this.
One is to trust traffic that has been marked at the edge and use the TOS/DSCP values to
queue traffic that traverses the network or as in this example do not trust any traffic
and classify it at each hop in the network. >
class-map match-all voice-signaling
  description Match MGCP Signaling and Backhaul
  match access-group 122
```

```
class-map match-all voice-rtp
  description Match Voice Real-Time Transport Protocol
  match access-group 121
class-map match-all gold-data
  description Match Telnet Management
match access-group 123

!< This section defines the policies that assign the appropriate DSCP value to the
classified traffic. The DSCP values used are based on Cisco recommendations. For further
information on QOS in voice networks refer to the Solutions Reference Network Design for
Quality of Service Design. >
policy-map voice
 description Service Policy for QoS Classification
  class voice-rtp
    set ip dscp 46
  class voice-signaling
    set ip dscp 26
  class gold-data
    set ip dscp 10
!
mls flow ip interface-full
mls flow ipx destination
mls sampling time-based 64
mls aclmerge algorithm odm
mls aclmerge odm optimizations
!< The DSCP-to-CoS map is used to map the final DSCP classification to a final CoS. This
final map determines the output queue and threshold to which the packet is assigned. The
CoS map is written into the ISL header or 802.1Q tag of the transmitted packet on trunk
interfaces and contains a table of 64 DSCP values and the corresponding CoS values >
mls qos map dscp-cos  24 25 to 2
mls qos map dscp-cos  32 33 to 3
mls qos map dscp-cos  40 41 42 43 44 45 to 4
!< The CoS-to-DSCP map is used to map the CoS of packets arriving on trusted interfaces
(or flows) to a DSCP where the trust type is trust-cos. This map is a table of eight CoS
values (0 through 7) and their corresponding DSCP values. >
mls qos map cos-dscp 0 8 16 26 34 46 48 56
!< The IP Precedence-to-DSCP map is used to map the IP precedence of IP packets arriving
on trusted interfaces (or flows) to a DSCP when the trust type is trust-ipprec. >
mls qos map ip-prec-dscp 0 8 16 26 34 46 48 56
!< enable QOS globally >
mls qos
!
…
interface FastEthernet2/1
 description Uplink to BTS 2950
 no ip address
 logging event link-status
 speed 100
 duplex full
!< The next 4 lines tell the 6509 who to map CoS values to drop thresholds for a queue >
 wrr-queue cos-map 1 1 0 1 2
 wrr-queue cos-map 1 2 3
 wrr-queue cos-map 2 1 4 6 7
 wrr-queue cos-map 2 2 5
!< In VLAN-based mode, the policy map attached to the Layer 2 interface is ignored, and
QoS is driven by the policy map attached to the corresponding VLAN interface. >
 mls qos vlan-based
 switchport
 switchport access vlan 132
 switchport mode access
…
interface GigabitEthernet9/1
 description L2 interface to PIX525 Inside interface
 no ip address
```

```
 logging event link-status
 wrr-queue cos-map 1 1 0 1 2
 wrr-queue cos-map 1 2 3
 wrr-queue cos-map 2 1 4 6 7
 wrr-queue cos-map 2 2 5
!< Specifies that the TOS bits in the incoming packet is a DSCP value and that it is
trusted. >
 mls qos trust dscp
 switchport
 switchport access vlan 130
 switchport mode access
 spanning-tree portfast
…
interface GigabitEthernet9/8
 description ISL FX Trunk to tpakptp02btsr02 g9/8
 no ip address
 logging event link-status
 wrr-queue cos-map 1 1 0 1 2
 wrr-queue cos-map 1 2 3
 wrr-queue cos-map 2 1 4 6 7
 wrr-queue cos-map 2 2 5
 mls qos trust dscp
 switchport
 switchport trunk encapsulation isl
 switchport trunk allowed vlan 1-912,914-4094
 switchport trunk pruning vlan 2-900,902-1001
 switchport mode trunk
!
interface Vlan130
 description BTS DMZ PIX Firewalls Inside
 ip address 10.152.130.3 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 7 12345
 ip ospf cost 1
 ip ospf hello-interval 3
 ip ospf priority 110
 logging event link-status
 load-interval 30
 arp timeout 1200
!
interface Vlan132
 description Primary (1st)  BTS External Subnet
 ip address 10.152.132.3 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
!< Enable ICMP Router Discover Protocol (IRDP) >
 ip irdp
!< Max interval between IRDP advertisements >
 ip irdp maxadvertinterval 4
!< Min interval between IRDP advertisements >
 ip irdp minadvertinterval 3
!< IRDP advertisement lifetime >
 ip irdp holdtime 10
!< Sets the preference for a device sending IRDP advertisements >
 ip irdp preference 110
 logging event link-status
 load-interval 30
!< This line applies the policy defined for voice signaling, voice bearer, and telnet
traffic. >
 service-policy input voice
```

```
 arp timeout 1200
!
interface Vlan133
 description Secondary (2nd)  BTS External Subnet
 ip address 10.152.133.3 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip irdp
 ip irdp maxadvertinterval 4
 ip irdp minadvertinterval 3
 ip irdp holdtime 10
 ip irdp preference 100
 logging event link-status
 load-interval 30
 service-policy input voice
 arp timeout 1200
…
!
!< These are the access lists used by the class-map statements to select the traffic for a
particular class >
access-list 121 remark Voice RTP Traffic
access-list 121 permit udp 10.0.0.0 0.255.255.255 range 16384 32767 any
access-list 121 permit udp 172.17.0.0 0.0.255.255 range 16384 32767 any
access-list 121 permit udp any 10.0.0.0 0.255.255.255 range 16384 32767
access-list 121 permit udp any 172.17.0.0 0.0.255.255 range 16384 32767
access-list 122 remark MGCP Voice Signaling
access-list 122 permit udp any any range 2427 2428
access-list 122 permit udp any any range 2727 2728
access-list 122 permit udp any any range 5555 5556
!< The next two statement allow MGCP ping traffic from the BTS to the media gateway >
access-list 122 permit udp any eq 12100 any
access-list 122 permit udp any any eq 12100
access-list 123 remark Gold Data
access-list 123 permit tcp any any range 22 telnet
access-list 123 permit udp any 10.152.136.32 0.0.1.7 eq domain
access-list 123 permit udp any 10.170.136.32 0.0.1.7 eq domain
!
…
end
```

Cisco IOS SLB for DNS Redundancy

The recommended method for providing Domain Name Server (DNS) redundancy to the Cisco BLISS for T1 solution is to use external load balancers with the Cisco IOS Server Load Balancer (SLB) on the Catalyst 6509. The configuration is conceptually the same for an external Cisco CSS 11500 switch.

```
…
ip slb serverfarm DNS-FARM<--- define the server farm that contains the DNS servers
 nat server
 probe DNS-PROBE<---  reference to probe that monitors the DNS application
 !
 real 10.151.66.138<--- IP address of primary DNS server
  inservice
 !
 real 10.151.66.148<--- IP address of the secondary DNS server
  inservice
!
ip slb vserver DNS-SERVER<--- define the virtual server
 virtual 10.151.66.99 tcp 53<--- specify virtual IP address and port for the server farm
 serverfarm DNS-FARM<--- specify the server farm
 inservice standby VLAN-66<--- VLAN to communicate to secondary 6509 for redundancy
```

Configuring the Cisco ITP

This section describes the procedures for configuring the Cisco IP Transfer Points (ITPs) to provide SS7 connectivity. It includes the following sub-sections:

Configuring Cisco ITP Routing Over SIGTRAN

Cisco ITP configuration is straightforward to those who have a basic understanding of Cisco IOS and how to configure SS7 network elements. This section provides an overview of the SIGTRAN-specific areas of the Cisco ITP configuration because the concepts and terminologies used may be new to the user. For a complete guide to configuring the Cisco ITP, go to the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/wireless/moblwrls/itp/25sw/index.htm

You can also view Cisco ITP example configurations at the following URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/products_feature_guide_chapter09186a008032a266.html.

Application Servers, Routing Keys, and Routing Context

The IETF SIGTRAN documentation defines how a signaling gateway (such as the Cisco ITP) routes traffic from the SS7 service provider toward a SIGTRAN-enabled IP endpoint (such as the Cisco BTS 10200). The following are associated descriptive terms:

- **Routing key**—Describes a set of SS7 parameters (DPC, OPC, SI, CIC-range, SSN, and so on) that uniquely defines the range of signaling traffic to be handled by a particular AS.
- **Routing context—**A value that uniquely identifies a routing key.
- **Application server** (AS)—A logical entity serving a specific routing key. An example of an application server is a switch element handling all call processing for a unique range of SS7 network trunks, identified by an SS7 SI/DPC/OPC/CIC-range. The AS contains two application server processes, one of which actively processes traffic. Note that there is a 1:1 relationship between an AS and a routing key.
- **Application Server Process (ASP)**—An active or standby process instance of an application server (in the Cisco BTS 10200, it is either the active or standby SGA or TSA software process). An ASP is defined by its SCTP endpoint information (two IP addresses and port) and may be configured to process signaling traffic within more than one Application Server.

AS and ASP Configuration Example

This section includes a basic configuration example and a diagram which depicts the example. Refer to Figure 5-2 when reading the following configuration information.

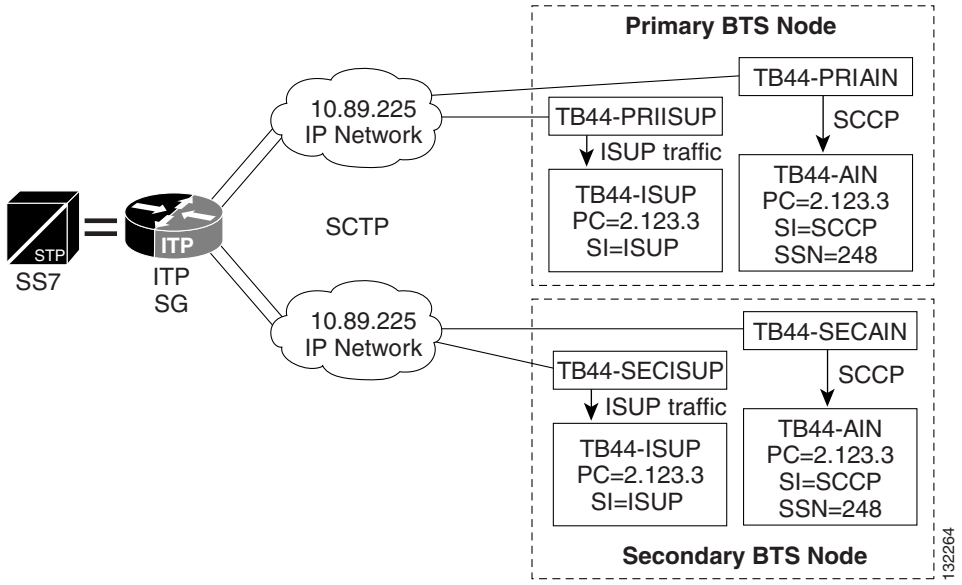
The following ASP configuration defines the primary-side TSA process. TB44-PRIAIN is the variable name of the ASP, 12205 is the remote (BTS) port number, 14001 is the local (ITP) port number, and sua defines the layer 3 SIGTRAN protocol used to transfer information to the ASP. This configuration also shows two IP addresses of the Cisco BTS 10200 that the TSA process uses for SUA communication.

```
cs7 asp TB44-PRIAIN 12205 14001 sua
 remote-ip 10.89.225.234
 remote-ip 10.89.226.234
```

The following configuration is very similar to the first, except that it defines information for the secondary-side TSA process.

```
cs7 asp TB44-SECAIN 12205 14001 sua
 remote-ip 10.89.225.235
 remote-ip 10.89.226.235
```

Figure 5-2 Configuring a Basic AS and ASP on the Cisco ITP



The following configuration is similar to the previous examples except that it defines an ASP that uses m3ua to transfer information to the ASP. This configuration is for the primary-side SGA process.

```
cs7 asp TB44-PRIISUP 11146 2905 m3ua
 remote-ip 10.89.225.234
 remote-ip 10.89.226.234
```

The following configuration is for the secondary-side SGA process.

```
cs7 asp TB44-SECISUP 11146 2905 m3ua
 remote-ip 10.89.225.235
 remote-ip 10.89.226.235
```

The AS configuration defines the routing key, which defines a filter for the traffic that will be sent toward the associated ASPs. The filter is based on parameters (such as DPC, OPC, CIC range, service indicator, and SSN) within incoming messages from the SS7 network.

- The first line of the AS configuration defines an AS name of TB44-ISUP and also indicates that the AS is defined for m3ua.
- The second line defines the routing key. It is identified by a routing context value of 1. It also includes a DPC value of 2.1.3 (which is the Cisco BTS 10200 OPC). The next parameter in the routing key is the service indicator si isup. This means that when a layer 4 SS7 message (such as an ISUP message) is received from the SS7 network, if the DPC in the MTP3 header is 2.1.3 and the SI indicates ISUP, it will be processed by this AS.

- The third and forth lines define the two associated ASPs. These represent the active and standby Cisco BTS 10200 processes, one of which will actually do the processing.
- The fifth line indicates that override mode is being used for this AS. This means that either asp TB44-PRIISUP or asp TB44-SECISUP will process the traffic (as opposed to a load-share mode which is not supported).

Note The network-appearance parameter is set to 1. This is a workaround for Cisco BTS 10200 Release 4.4 and should not be provisioned at all in Release 4.5.

```
cs7 as TB44-ISUP m3ua
routing-key 1 2.1.3 si isup
asp TB44-PRIISUP
asp TB44-SECISUP
traffic-mode override
network-appearance 1
```

The following AS definition processes AIN traffic. It defines an ASP that uses sua instead of m3ua as the SIGTRAN protocol that communicates with this AS. The routing key definition includes DPC and SI values as well as an SSN value of 248 to further refine the filter.

```
cs7 as TB44-AIN sua
routing-key 2 2.1.3 si sccp ssn 248
 asp TB44-SECAIN
 asp TB44-PRIAIN
 traffic-mode override
 network-appearance 1
```

Overlapping AS Configurations

The following AS configuration example is similar to the ones in the previous section, but has more information in the routing key definition.

In this example, the AS routes messages toward asp PRI_ISUP_BTS2 or SEC_ISUP_BTS2. The routing key has a routing context value of 10. The routing key defines the DPC value as 2.1.3, and the OPC value as 3.50.3. This OPC has a mask value of 255.255.255 (which means all bits of the OPC will be considered when routing). It defines a service indicator (si) of ISUP and a cic range of 1 to 23.

Note The network-appearance parameter is set to 1. This was a workaround for Cisco BTS 10200 Release 4.4 and should not be provisioned at all in Release 4.5.

```
cs7 as ISUP_BTS1 m3ua
routing-key 10 2.1.3 opc 3.50.3 255.255.255 si isup cic 1 23
asp PRI_ISUP_BTS2
asp SEC_ISUP_BTS2
traffic-mode override
 network-appearance 1
```

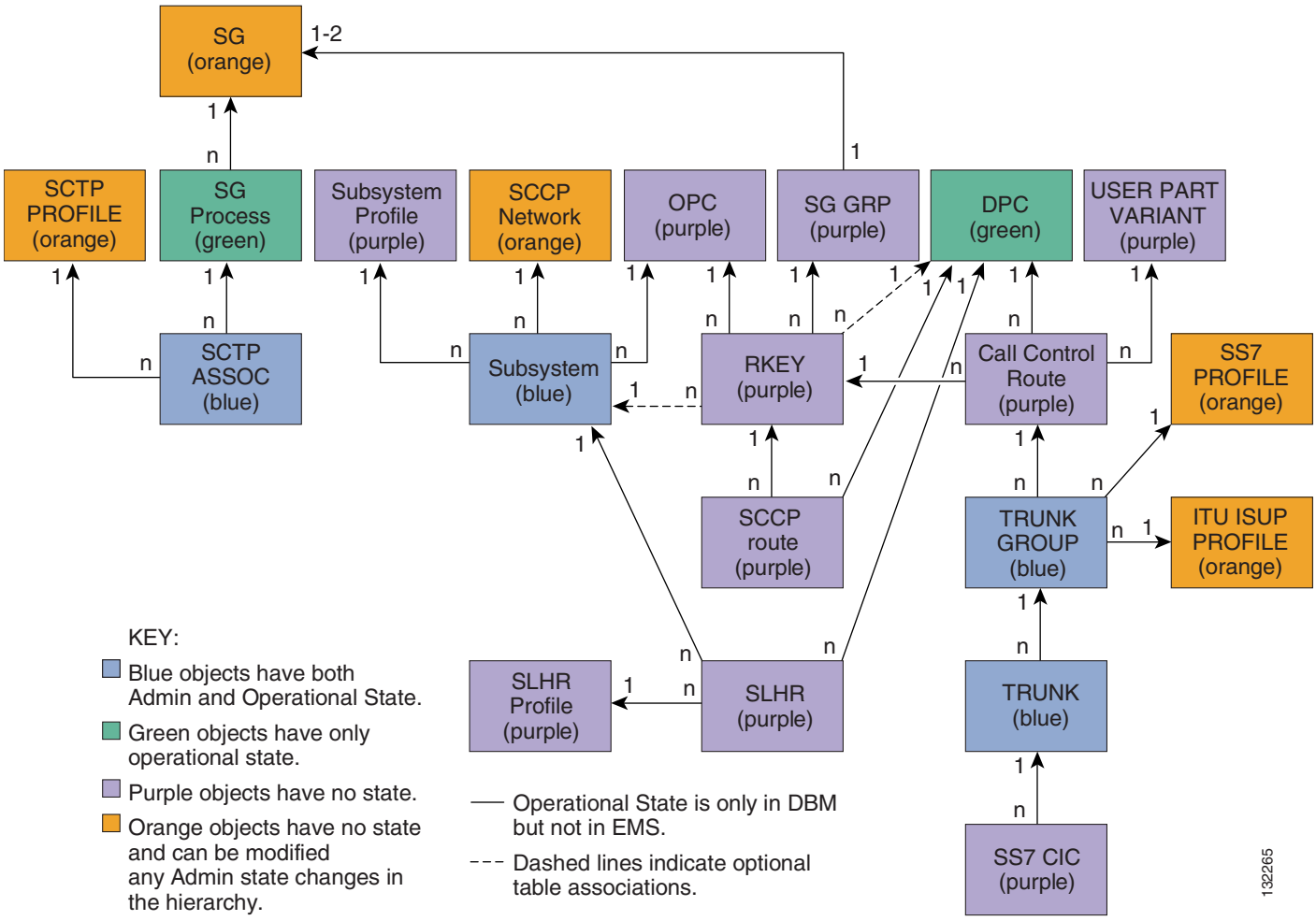
This AS (ISUP_BTS1) and the AS in the previous section (TB44-ISUP) both route ISUP messages from the SS7 network that have DPC values of 2.1.3. The question becomes Which ASP will the Cisco ITP route toward when the DPC in the incoming ISUP message is 2.1.3? The answer is the one that matches best. ISUP_BTS1 requires that four parameters from the incoming SS7 message match its routing key. TB44-ISUP only requires two parameters. If all four parameters of routing-key 10 match, then ISUP_BTS1 will be chosen. If only three parameters of routing-key 10 match, then routing key 1 is a better match and TB44-ISUP will be chosen to process the message.

Provisioning SS7-Related Elements of the Cisco BTS 10200

Each subsection of the "Customer-Offered Cisco BTS 10200/Cisco ITP Profiles" section that follows includes example provisioning for the Cisco BTS 10200 that is related to the associated ITP profile. Refer to Figure 5-3 when provisioning SS7-related components for the Cisco BTS 10200. Note that the objects must be provisioned from the top down (for instance, the SG is provisioned before the SG Process or SG Group).

For a complete description of provisioning SS7-related objects on the Cisco BTS 10200 in Release 4.4, refer to http://lbj/push_targets1/ucdit/cc/td/doc/product/voice/bts10200/bts4_1/provgd/41_ss7.htm.

Figure 5-3 Cisco BTS 10200 SIGTRAN SS7 Object Diagram



Customer-Offered Cisco BTS 10200/Cisco ITP Profiles

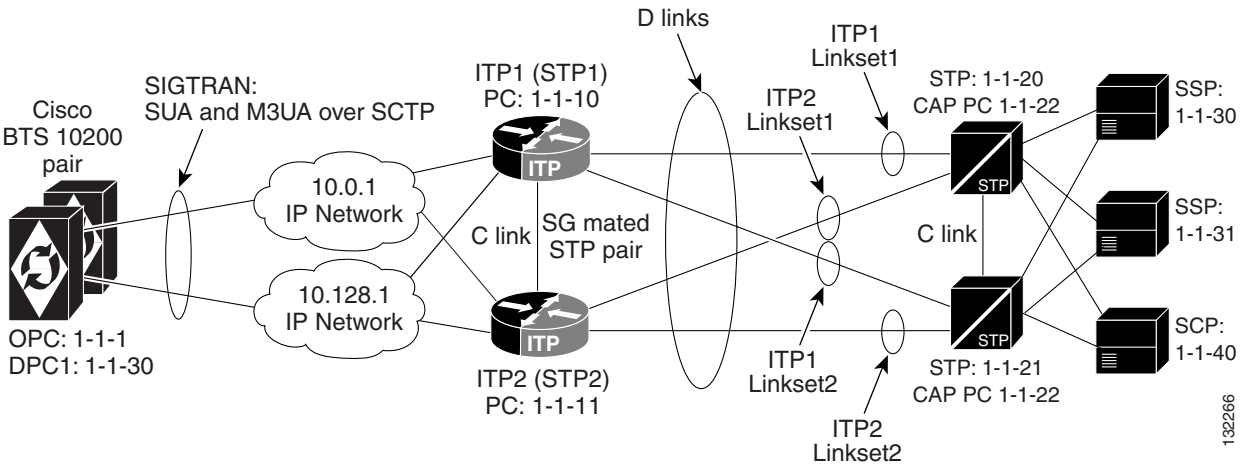
This section includes several Cisco BTS 10200/Cisco ITP profiles that are offered to customers. This section provides the basic D-link and A-link profiles and the building blocks and then adds features to create more complex profiles.

Several features can be combined to form hybrid profiles not listed in the following subsections.

Basic D-link Profile

The basic D-link profile is used when a customer wants to access the SS7 network using D-links.

Figure 5-4 Basic D-link Profile



For pros and cons of this profile, refer to the "SG Mated Pair" section on page 2-9.

Usage

The Basic D-link Profile is used if the customer wants multiple OPCs on the Cisco BTS 10200. It is also used when the customer wants global title translation (GTT) support on the Cisco ITP. It provides for geographical separation of Cisco ITPs (see the "Geographically Distributed D-link Profile with SG Routing Priority" section on page 5-46).

ITP Configuration Information

This section provides a configuration example for ITP1 and ITP2 in the basic D-link profile. For additional Cisco ITP configuration information, see the *Cisco ITP Configuration Guide and Command Reference* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/wireless/moblwrls/itp/25sw/itp25swi.pdf

The *Cisco ITP Configuration Guide and Command Reference* is a very large document. In particular, focus on the following sections:

- Overview of Cisco ITP
- Configuring Cisco ITP Basic Functionality
- Configuring M3UA and SUA SS7 Over IP Signaling Gateways

For other Cisco ITP example configurations, see the following URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/products_feature_guide_chapter09186a008032a266.html

ITP1 Configuration

```
##############################################################################
# ITP1 - The first ITP in the sg-pair (each ITP in the sg-pair functions as an STP).
##############################################################################

Current configuration : 3470 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ITP1
!
boot-start-marker
boot system flash c2600-itp-mz.topsail_s_nightly_040915
boot-end-marker
!
redundancy inter-device
!
enable secret 5 $1$XCoU$j0Y2wFRoks2pocHa1gHhi0
enable password cisco
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 9001
    local-ip 10.0.1.54
    local-ip 10.128.1.239
   remote-port 9000
    remote-ip 10.0.1.55
    remote-ip 10.128.1.240
!
memory-size iomem 20
ip subnet-zero
!
ip domain-name cisco.com
ip name-server 10.0.0.6
!
#
# Note that for the D-link configuration (SG Mated Pair) configuration, the local
# point code value is 1.1.10, which is different than the BTS OPC and the other ITP (ITP1)
# that makes up the SG Mated Pair.
#
cs7 variant ANSI
cs7 point-code 1.1.10
!
controller E1 0/0
 framing NO-CRC4
 channel-group 0 timeslots 1
!
controller E1 0/1
 framing NO-CRC4
 channel-group 0 timeslots 1
!
controller E1 0/2
 shutdown
```

```
!
controller E1 0/3
 shutdown
!
interface Serial0/0:0
 description connect to link 0 of STP 1-1-20
 no ip address
 encapsulation mtp2
 no clns route-cache
!
interface Serial0/1:0
 description connect to link 0 of STP 1-1-21
 no ip address
 encapsulation mtp2
 no clns route-cache

interface FastEthernet0/0
 ip address 10.0.1.54 255.255.0.0
 speed auto
 half-duplex
 no clns route-cache
!
interface FastEthernet0/1
 ip address 10.128.1.239 255.255.0.0
 speed auto
 half-duplex
 no clns route-cache

#
#
# In the D-link configuration, instead of defining a cs7 group (as is done in
# the A-link configuration, a "local-peer" and "mated-sg" are defined. Here
# we define the local-peer which is the local definition for the C-link connection
# between the two ITPs that make up the redundant STP pair.
#
#
cs7 local-peer 7000
 local-ip 10.0.1.54
 local-ip 10.128.1.239

#
# Linkset definitions. Note: the number after 'link' represents SLC
#
cs7 linkset lset1chn 1.1.20
 link 0 Serial0/0:0
!
cs7 linkset lset2chn 1.1.21
 link 0 Serial0/1:0

#
# C-link linkset definition. Here the point code value and IP information for
# the mated-sg is defined. Note that the local IP information is defined in
# the local-peer definition above.
#
cs7 linkset c-link 1.1.11
 link 0 sctp 10.0.1.55 10.128.1.240 7000 7000

#
# SS7 ROUTE DEFINITIONS
#
# In the following entries, note the following:
# 1) All of the routes towards all DPCs are configured with equal priority when
# using lset1chn or lset2chn.
# 2) There are lower priority routes towards each destination across the c-link.
```

```
# 3) Routing towards the Capability PC of the adjacent STPs is treated as if the
# Capabilty PC is a DPC beyond the STP.
#
#
cs7 route-table system
 update route 1.1.30 255.255.255 linkset lset1chn priority 1
 update route 1.1.30 255.255.255 linkset lset2chn priority 1
 update route 1.1.31 255.255.255 linkset lset1chn priority 1
 update route 1.1.31 255.255.255 linkset lset2chn priority 1
 update route 1.1.40 255.255.255 linkset lset2chn priority 1
 update route 1.1.40 255.255.255 linkset lset1chn priority 1

# Lower priority C-link routes
 update route 1.1.30 255.255.255 linkset c-link priority 2
 update route 1.1.31 255.255.255 linkset c-link priority 2
 update route 1.1.40 255.255.255 linkset c-link priority 2

# Routing to Capability Pt Codes of adjacent STPs
update route 1.1.22 255.255.255 linkset lset1chn priority 1
update route 1.1.22 255.255.255 linkset lset2chn priority 1

#
# With the mated-sg (D-link configuration), you must also define a connection
# between the ITPs to pass Sigtran specific state information and other data.
# This is done by defining the local IP information in the "cs7 sgmp" configuration
# and the peer IP information in the "cs7 mated-sg" configuration.
#
#
cs7 sgmp 9101
 local-ip 10.0.1.54
 local-ip 10.128.1.239
!
cs7 mated-sg ITP2 9101
 remote-ip 10.0.1.55
 remote-ip 10.128.1.240

#
# The M3UA definition that declares local IP addresses and port #
#
cs7 m3ua 2905
 local-ip 10.0.1.54
 local-ip 10.128.1.239
 keepalive 2000

#
#
# Here as with all configurations, there are *at least* two ASPs defined
# for each AS (one for the primary BTS node and one for the Secondary).
# In reality, there will be at least one for each "User Part" on the BTS10200.
# So if you have a TCAP Service going over SUA and ISUP traffic, you will
# have a total of at least four ASPs. Primary ISUP, Secondary ISUP, Primary
# TCAP Service, Secondary TCAP Service.
#
# Note that the remote port value of 11146 is configured on the BTS10200 in the
# platform.cfg file (as an SGA command line argument). 2905 is the local port
# value. The remote IP addresses are the BTS IP addresses. They are also obtained
# through the FQDN that is an SGA command line argument.
#
#
cs7 asp PrimaryBtsIsupAsp 11146 2905 m3ua
 remote-ip 10.0.1.5
 remote-ip 10.128.1.2
!
cs7 asp SecondaryBtsIsupAsp 11146 2905 m3ua
```

```
 remote-ip 10.0.1.6
 remote-ip 10.128.1.3
!

#
# Note that the routing key is a very simple one. It has a
# routing context of 1 defined, the DPC (BTS OPC) of 1.1.1 defined
# and a service indicator of ISUP defined. This means that all traffic
# coming from the SS7 Service Provider Network that has a DPC of 1.1.1
# and a service indicator of ISUP will be sent to either PrimaryBtsIsupAsp
# or SecondaryBtsIsupAsp (depending on which one is active).
#
# The traffic mode is always set to override (not loadshare)
#
# In BTS release 4.4 only, there is a work around that requires
# network-appearance to be configured with a value of 1. In
# BTS release 4.5, this work-around will be removed and
# network-appearance should not be provisioned on the ITP.
#
cs7 as BtsIsupAs m3ua
 routing-key 1 1.1.1 si isup
 asp PrimaryBtsIsupAsp
 asp SecondaryBtsIsupAsp
 traffic-mode override
 network-appearance 1
#
# The SUA definition that declares local IP addresses and port #
#
cs7 sua 14001
 local-ip 10.0.1.54
 local-ip 10.128.1.239
 keepalive 2000
#
# Here we are defining an ASPs that will process AIN related traffic. Note that
# the remote port 12205 is a TSA command line parameter in platform.cfg on the BTS.
# 14001 is the local port number.
#
#
cs7 asp PrimaryBtsAinAsp 12205 14001 sua
 remote-ip 10.0.1.5
 remote-ip 10.128.1.2
!
cs7 asp SecondaryBtsAinAsp 12205 14001 sua
 remote-ip 10.0.1.6
 remote-ip 10.128.1.3
#
# The following AS is defined for LNP related message flows. The routing context
# value is 4, the DPC (BTS OPC) is 1.1.1, the service indicator is SCCP and the
# Subsystem number is 247. This means that any message received from the SS7
# Service Provider that has a DPC of 1.1.1, a service indicator of SCCP and an
# SSN of 247 will be sent to either PrimaryBtsAinAsp or SecondaryBtsAinAsp
# (depending on which one is active).
#
#
cs7 as BtsLnpAs sua
 routing-key 4 1.1.1 si sccp ssn 247
 asp PrimaryBtsAinAsp
 asp SecondaryBtsAinAsp
 traffic-mode override
```

ITP2 Configuration

```
##############################################################################
#
# ITP2 - The second ITP in the sg-pair (each ITP in the sg-pair functions as an STP).
# FOR THE ITP2 CONFIGURATION, PLEASE REFER TO THE COMMENTS THAT WERE MADE IN
# THE ITP1 CONFIGURATION.
#

Current configuration : 4054 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ITP2
!
boot-start-marker
boot system flash 2600/c2600-itp-mz.topsail_s_nightly_040915
boot-end-marker
!
redundancy inter-device
!
enable secret 5 $1$B6u2$gI4fFgjOQo5XppDSWJDfI.
enable password cisco
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 9000
    local-ip 10.0.1.55
    local-ip 10.128.1.240
   remote-port 9001
    remote-ip 10.0.1.54
    remote-ip 10.128.1.239
!
memory-size iomem 10
ip subnet-zero
!
ip domain-name cisco.com
ip name-server 10.0.0.6
!
cs7 variant ANSI
#
# Note that for the D-link configuration (SG Mated Pair) configuration, the local
# point code value is 1.1.11, which is different than the BTS OPC and the other ITP (ITP1)
# that makes up the SG Mated Pair.
#
cs7 point-code 1.1.11
!
controller E1 0/0
 framing NO-CRC4
 channel-group 0 timeslots 1
!
controller E1 0/1
 framing NO-CRC4
 channel-group 0 timeslots 1
!
controller E1 0/2
 shutdown
!
```

```
controller E1 0/3
 shutdown
!
interface FastEthernet0/0
 ip address 10.0.1.55 255.255.0.0
 speed auto
 half-duplex
 no clns route-cache
!
interface FastEthernet0/1
 ip address 10.128.1.240 255.255.0.0
 speed auto
 half-duplex
 no clns route-cache
!
interface Serial0/0:0
 description connect to link 1 of STP 1-1-20
 no ip address
 encapsulation mtp2
 no clns route-cache

interface Serial0/1:0
 description connect to link 1 of STP 1-1-21
 no ip address
 encapsulation mtp2
 no clns route-cache
!
#
# local-peer definition
#
cs7 local-peer 7000
 local-ip 10.0.1.55
 local-ip 10.128.1.240
!
#
# Linkset definitions. Note: the number after 'link' represents SLC
#
cs7 linkset lset1chn 1.1.20
 link 1 Serial0/0:0
!
cs7 linkset lset2chn 1.1.21
 link 1 Serial0/1:0
!
#
# C-link linkset definition.
#
cs7 linkset c-link 1.1.10
 link 0 sctp 10.0.1.54 10.128.1.239 7000 7000
!
cs7 route-table system
 update route 1.1.30 255.255.255 linkset lset1chn priority 1
 update route 1.1.30 255.255.255 linkset lset2chn priority 1
 update route 1.1.31 255.255.255 linkset lset1chn priority 1
 update route 1.1.31 255.255.255 linkset lset2chn priority 1
 update route 1.1.40 255.255.255 linkset lset2chn priority 1
 update route 1.1.40 255.255.255 linkset lset1chn priority 1

# C-link routes
 update route 1.1.30 255.255.255 linkset c-link priority 2
 update route 1.1.31 255.255.255 linkset c-link priority 2
 update route 1.1.40 255.255.255 linkset c-link priority 2
```

```
# Routing to Capability Pt Codes of adjacent STPs
update route 1.1.22 255.255.255 linkset lset1chn priority 1
update route 1.1.22 255.255.255 linkset lset2chn priority 1

!
cs7 sgmp 9101
 local-ip 10.0.1.55
 local-ip 10.128.1.240
!
cs7 mated-sg ITP1 9101
 remote-ip 10.0.1.54
 remote-ip 10.128.1.239
cs7 m3ua 2905
 local-ip 10.0.1.55
 local-ip 10.128.1.240
!
cs7 asp PrimaryBtsIsupAsp 11146 2905 m3ua
 remote-ip 10.0.1.5
 remote-ip 10.128.1.2
!
cs7 asp SecondaryBtsIsupAsp 11146 2905 m3ua
 remote-ip 10.0.1.6
 remote-ip 10.128.1.3
!
cs7 as BtsIsupAs m3ua
 routing-key 2 1.1.1 si isup
 asp PrimaryBtsIsupAsp
 asp SecondaryBtsIsupAsp
 traffic-mode override
 network-appearance 1
!
cs7 sua 14001
 local-ip 10.0.1.55
 local-ip 10.128.1.240
 keepalive 2000
!
cs7 asp PrimaryBtsAinAsp 12205 14001 sua
 remote-ip 10.0.1.5
 remote-ip 10.128.1.2
!
cs7 asp SecondaryBtsAinAsp 12205 14001 sua
 remote-ip 10.0.1.6
 remote-ip 10.128.1.3
!
cs7 as BtsLnpAs sua
 routing-key 4 1.1.1 si sccp ssn 247
 asp PrimaryBtsAinAsp
 asp SecondaryBtsAinAsp
 traffic-mode override
```

Cisco BTS 10200 Provisioning for the Basic D-link Profile

The local IP addresses and port are determined by command-line arguments that are passed to the SGA process and TSA processes when they start up. This information is contained in the platform.cfg file. For instance, an example SGA command line is:

```
Args=-t 1 -h crit-aSYS11CA.ipclab.cisco.com -p 11146 -mdldir ../mdl -mdltracedir
../mdltrace -mdltestmode 0 -mdlloadmdo 0 -mdltriggertimer 200 -mdlgarbagetimer 5146
-resetcics 1 -fcmtimer 900 -fcmparalleljobs 4
```

In this list of arguments, the –h argument *crit-aSYS11CA.ipclab.cisco.com* is a fully qualified domain name (FQDN) that resolves to two local IP addresses. In most cases the FQDN can be viewed in the /etc/hosts file. To determine the IP addresses to which the FQDN resolves, enter nslookup <FQDN>.

Call Agent (CA) Configuration

```
##########################################################################
#
# CA Configuration
#
##########################################################################

add ca-config type=MGCP-INIT-TERMS;value=160;datatype=integer;
add ca-config type=MGCP-INIT-DURATION;value=5;datatype=integer;
add ca-config type=MGCP-ICMP-PING-RETRANSMIT-DURATION;value=5;datatype=integer;
add ca-config type=MGCP-ICMP-PING-RETRY-COUNT;value=5;datatype=integer;
add ca-config type=MGCP-MAX-UNREACH-COUNT;value=5;datatype=integer;
add ca-config type=MGCP-MAX-FAULT-COUNT;value=5;datatype=integer;
add ca-config type=MGCP-ADM-RESP-TIME;value=300;datatype=integer;
add ca-config type=MGCP-SIG-TOS-LOWDELAY;value=Y;datatype=boolean;
add ca-config type=MGCP-SIG-TOS-PRECEDENCE;value=1;datatype=integer;
add ca-config type=MGCP-SIG-TOS-RELIABILITY;value=Y;datatype=boolean;
add ca-config type=MGCP-SIG-TOS-THROUGHPUT;value=Y;datatype=boolean;
#
# CA & FS
#
add call-agent id=CA146; tsap-addr-sidea=hrn11ca; mgw-monitoring-enabled=N;
add feature-server id=FSAIN205; tsap-addr-sidea=hrn11ca:11205; type=AIN;

#
# Sigtran components
#
add user-part-variant id=ANSISS7_GR317;

#
# Note for the D-link configuration, there are two SGs defined for redundancy.
# They are essentually mated STPs. This is different than the A, F, or E link
# configurations which derive redundancy at the SGP level.
#
add sg id=sg1; description=Signaling gateway 1;
add sg id=sg2; description=Signaling gateway 2;

#
# In the D-link configuration The SG-GRP has two SGs defined in the SG-GRP. The
# A,F, and E link configurations *must* only have one SG defined in an SG-GRP.
#
add sg-grp id=sg-grp1; sg1-id=sg1; sg2-id=sg2 description=SG group 1;
#
# In the D-link configuration, there is *only* one SGP per SG. Note that the
# two SGPs defined here have a one-to-one correspondence to the SGs that were
# defined above. This is in contrast to the A,F, and E link configurations
# which must have two SGPs per SG.
#
```

```
add sgp id=sg1-sgp1 ; sg-id=sg1; description=SG process 1 for sg1;
add sgp id=sg2-sgp1 ; sg-id=sg2; description=SG process 1 for sg2;

add opc id=opc1; point-code=1-1-1; description=OPC; point-code-type=ANSI_CHINA;
add dpc id=dpc1; point-code=1-1-30; description=DPC 1; point-code-type=ANSI_CHINA;
add dpc id=dpc2; point-code=1-1-31; description=DPC 2; point-code-type=ANSI_CHINA;

# THE ISUP ROUTING KEYS
add routing-key id=rk1; opc-id=opc1; sg-grp-id=sg-grp1; si=ISUP; rc=1; platform-id=CA146;

add call-ctrl-route id=dpc1-route1; dpc-id=dpc1; routing-key-id=rk1; si=isup;
user-part-variant-id= ANSISS7_GR317
add call-ctrl-route id=dpc2-route1; dpc-id=dpc2; routing-key-id=rk1; si=isup;
user-part-variant-id= ANSISS7_GR317;

add sctp-assoc-profile id=sctp-prof;

# THE SCTP ASSOCIATIONS
# Note that the chosen id name in this statement reflects the fact that this is the
# sctp association for SGP1 of SG1
#
add sctp-assoc id=sg1-sgp1-sctp; sgp-id=sg1-sgp1; sctp-assoc-profile-id=sctp-prof;
platform-id=CA146; remote-port=2905; remote-tsap-addr1=10.0.1.54;
remote-tsap-addr2=10.128.1.239; dscp=AF11; ip-tos-precedence=ROUTINE;

add sctp-assoc id=sg2-sgp1-sctp; sgp-id=sg2-sgp1; sctp-assoc-profile-id=sctp-prof;
platform-id=CA146; remote-port=2905; remote-tsap-addr1=10.0.1.55;
remote-tsap-addr2=10.128.1.240; dscp=AF11; ip-tos-precedence=ROUTINE;

#
# dial plan profile
#
add digman-profile id=pretrans;
add digman id=pretrans; rule=1; match-string=^*; replace-string=&; match-noa=any;
replace-noa=VSC;
add digman id=pretrans; rule=2; match-string=^#; replace-string=&; match-noa=any;
replace-noa=VSC;
add digman-profile id=ani_20;
add digman id=ani_20; rule=1; match-string=^20; replace-string=none;
add dial-plan-profile id=dp-1; nanp-dial-plan=Y; description=NA dial plan profile;
dnis-digman-id=pretrans; ani-digman-id=ani_20;
#
# SS7 TG
#
add ss7-ansi-tg-profile ID=ansi-tg-prof;
add trunk-grp ID=1; call_agent_id=CA146; tg_type=SS7; direction=BOTH;
tg_profile_id=ansi-tg-prof; call-ctrl-route-id=dpc1-route1; dial-plan-id=dp-1;
description=TG to DPC 1;  MGCP_PKG_TYPE=T;
add trunk-grp ID=2; call_agent_id=CA146; tg_type=SS7; direction=BOTH;
tg_profile_id=ansi-tg-prof; call-ctrl-route-id=dpc2-route1; dial-plan-id=dp-1;
description=TG to DPC 2;  MGCP_PKG_TYPE=T;
#
# MGW
#
add mgw-profile id=as5300-prof; vendor=Cisco; mgcp-hairpin-supp=n; MGCP_RSIPSTAR_SUPP=N;
MGCP_TERM_INIT_LEVEL=0; RBK_ON_CONN_SUPP=N; MGCP_VERSION=MGCP_1_0; mgcp-max2-retries=3;
fax-t38-camode-supp=Y; mgcp-keepalive-interval=60; mgcp-keepalive-retries=10;
mgcp-t-tran=400; mgcp-max1-retries=2; mgcp-t-longtran=5; mgcp-default-pkg=NONE;
MGCP_3WAY_HSHAKE_SUPP=N; mgw_type=AS5300; PC_MPTIME_SUPP=N;
##
MGCP_VERSION=MGCP_1_0; PC_MPTIME_SUPP=N;
add mgw id=va-5350-23; tsap-addr=va-5350-23.hrndevtest.cisco.com; call-agent-id=CA146;
mgw-profile-id=as5300-prof; type=TGW;
```

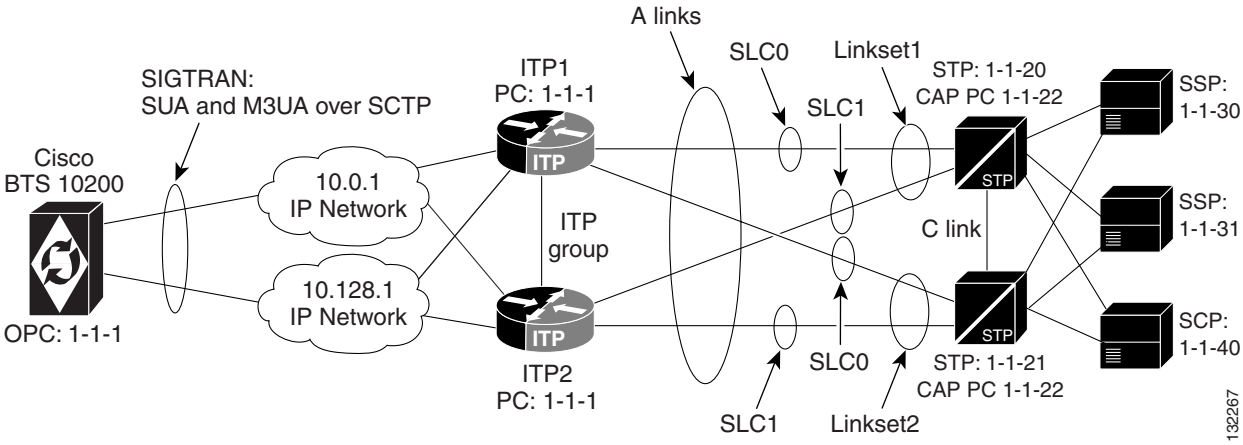
```
#
# SS7 terminations and trunks
#
add termination prefix=S3/DS1-4/; port-start=1; port-end=31; type=trunk;
mgw-id=va-5350-23;
add termination prefix=S3/DS1-5/; port-start=1; port-end=31; type=trunk;
mgw-id=va-5350-23;
add trunk cic-start=1; cic-end=31; tgn-id=1; mgw-id=va-5350-23;
termination-prefix=S3/DS1-4/; termination-port-start=1; termination-port-end=31;
add trunk cic-start=1; cic-end=31; tgn-id=2; mgw-id=va-5350-23;
termination-prefix=S3/DS1-5/; termination-port-start=1; termination-port-end=31;
#
# SS7 routes, route guides and destinations
#
add route id=dpc1-route; tg_selection=RR; tgn1_id=1;
add route id=dpc2-route; tg_selection=RR; tgn1_id=2;
add route-guide id=dpc1-rg; policy-type=ROUTE; policy-id=dpc1-route;
add route-guide id=dpc2-rg; policy-type=ROUTE; policy-id=dpc2-route;
add destination dest-id=dpc1-dest; call-type=LOCAL; route-type=ROUTE;
route-guide-id=dpc1-rg;
add destination dest-id=dpc2-dest; call-type=LOCAL; route-type=ROUTE;
route-guide-id=dpc2-rg;

#####################################
# TCAP/SUA Provisioning for LNP
#####################################

add sccp-nw id=1;NET_IND=NATIONAL;SUB_SVC=NATIONAL;HOP_COUNT=3;

add subsystem-profile id=SSN_LNP1;platform_id=FSAIN205;

add subsystem id=SSN_LNP1; OPC-ID=opc1; LOCAL-SSN=247;REMOTE_SSN=247;
sccp-nw-id=1;SCCP_VERSION=ANS92; TCAP_VERSION=ANS92; APPLICATION_VERSION=AIN01;

add routing-key id=itp-grp-rk2; opc-id=opc1; sg-grp-id=sg-grp1; si=sccp; ssn-id=SSN_LNP1;
platform-id=FSAIN205; rc=4; description=Routing Key for SUA User Adaptation layer;

########################################
# Provisioned DPC is the STP Capabilty Pt Code
########################################
add dpc id=stp_cap_pc; point-code=1-1-22; point-code-type=ANSI_CHINA;
description=Capability Point Code of STPs

add feature fname=LNP; feature-server-id=FSAIN205; description=Local number portability;
tdp1=COLLECTED_INFORMATION; tid1=LNP_TRIGGER; ttype1=R;

add ported-office-code digit-string=301-612; in-call-agent=n;

add CA-Config type=DEFAULT-LNP-SLHR-ID; datatype=string;  value=slhr_lnp;

add slhr-profile id=slhr_lnp;

add slhr id=slhr_lnp; gtt-req=Y; tt=11; GTT_ADDR_TYPE=CDPN; GTT_ADDR=3; opc-id=opc1;
dpc-id=stp_cap_pc; ssn_id=SSN_LNP1;

add sccp-route opc-id=opc1; dpc-id=stp_cap_pc; rk-id=itp-grp-rk2; ssn-id=SSN_LNP1;
description=LNP for opc1;

add pop ID=50901; STATE=tx; COUNTRY=US; TIMEZONE=CDT; LOCAL_7D_DIALING=Y; ITP=N;
ZERO_MINUS=LEC; BLOCK_EAWOPIC=Y; CNAM_OPTION=EXT_LIDB; PIC2_REQD=N; MY_LRN=4692559999;
TREAT_IMS_ANONYMOUS=N; OPC_ID=opc1; ZERO_PLUS_LOCAL=N
```

```
#####################################################
# Control network entities in-service for ANSI SS7
#####################################################
control trunk-grp id=1; mode=forced; target-state=ins;
control trunk-grp id=2; mode=forced; target-state=ins;
equip trunk-termination tgn-id=1; cic=all;
equip trunk-termination tgn-id=2; cic=all;
control trunk-termination tgn-id=1; cic=all; target-state=INS;  mode=FORCED;
control trunk-termination tgn-id=2; cic=all; target-state=INS;  mode=FORCED;
control subsystem id=SSN_LNP1;mode=forced;target-state=uis;opc-id=opc1
control sctp-assoc id=sg1-sgp1-sctp; mode=forced; target-state=INS;
control sctp-assoc id=sg2-sgp1-sctp; mode=forced; target-state=INS;

#########################################################
# Status commands
#########################################################
#status trunk-grp id=1;
#status trunk-grp id=2;
#status trunk-termination tgn-id=1; cic=all;
#status trunk-termination tgn-id=2; cic=all;
#status sctp-assoc id=sg1-sgp1-sctp;
#status sctp-assoc id=sg2-sgp1-sctp;
```

Basic A-link Profile (Distributed MTP3 Feature)

The basic A-link profile is used when a customer wants to access the SS7 network using A-links.

Figure 5-5 Basic A-link Profile (Distributed MTP3)



For pros and cons of this profile, see the "ITP-Group" section on page 2-9.

Usage

The Basic A-link Profile provides a solution that is low cost yet fully hardware and network redundant. Cost reduction is accomplished by minimizing the number of point codes that are connected to the SS7 service provider network and by connecting via A-links rather than D-links (which require more setup and maintenance).

ITP Configuration Information

This section provides a configuration example for the basic A-link profile. For additional Cisco ITP configuration information, see the *Cisco ITP Configuration Guide and Command Reference* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/wireless/moblwrls/itp/25sw/itp25swi.pdf

In particular, focus on the following sections:

- Overview of Cisco ITP
- Configuring Cisco ITP Basic Functionality
- Configuring M3UA and SUA SS7 Over IP Signaling Gateways
- Configuring Cisco ITP-Group (specifically used in A-link/Distributed MTP3 configs)

For other Cisco ITP example configurations, see the following URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/products_feature_guide_chapter09186a008032a266.html.

ITP1 Configuration

```
#
# This is the first ITP in the ITP-Group (the first SGP in the SG).
#
Current configuration : 3470 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ITP1
!
boot-start-marker
boot system flash c2600-itp-mz.topsail_s_nightly_040915
boot-end-marker
!
redundancy inter-device
!
enable secret 5 $1$XCoU$j0Y2wFRoks2pocHa1gHhi0
enable password cisco
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 9001
    local-ip 10.0.1.54
    local-ip 10.128.1.239
   remote-port 9000
    remote-ip 10.0.1.55
    remote-ip 10.128.1.240
!
memory-size iomem 20
ip subnet-zero
!
ip domain-name cisco.com
ip name-server 10.0.0.6
!
#
# Note that for the A-link (ITP-Group/Distributed MTP) configuration, the local
# point code value is 1.1.1, which is the same as the BTS OPC.
```

```
#
cs7 variant ANSI
cs7 point-code 1.1.1
!
controller E1 0/0
 framing NO-CRC4
 channel-group 0 timeslots 1
!
controller E1 0/1
 framing NO-CRC4
 channel-group 0 timeslots 1
!
controller E1 0/2
 shutdown
!
controller E1 0/3
 shutdown
!
interface FastEthernet0/0
 ip address 10.0.1.54 255.255.0.0
 speed auto
 half-duplex
 no clns route-cache
!
interface Serial0/0:0
 description connect to link 0 of STP 1-1-20
 no ip address
 encapsulation mtp2
 no clns route-cache
!
interface FastEthernet0/1
 ip address 10.128.1.239 255.255.0.0
 speed auto
 half-duplex
 no clns route-cache
!
interface Serial0/1:0
 description connect to link 0 of STP 1-1-21
 no ip address
 encapsulation mtp2
 no clns route-cache
!
#
# Unlike the D-link connection which defines a local-peer and mated-sg for
# redundancy, for the Distributed  MTP3 feature A-link configuration, you
# define a cs7 group. This enables both ITPs in the ITP-group (or SGPs in the
# SG) to communicate with each other. In this configuration you define the
# IP addresses and port values for both sides of the connection.
##
cs7 group grp-ITP1 9004
 local-ip 10.0.1.54
 local-ip 10.128.1.239
 peer grp-ITP2 9003
  remote-ip 10.0.1.55
  remote-ip 10.128.1.240
!
#
# Note here that when the linksets are defined, for redundancy each linkset
# has links from each ITP in the ITP-Group (or SGP in the SG).
#

cs7 linkset lset1chn 1.1.20
 link 0 grp-ITP1 Serial0/0:0
 link 1 grp-ITP2 Serial0/0:0
```

```
!
cs7 linkset lset2chn 1.1.21
 link 0 grp-ITP1 Serial0/1:0
 link 1 grp-ITP2 Serial0/1:0
#
# Note that unlike the D-link configuration, there are no low priority routes
# defined to the DPCs. This is because in the ITP-group setup the STPs view the
# combination of the two ITPs is as a single entity (the two SGPs form one SG).
# Because of this, there are no lower priority routes that travel across a C link
# between the two ITPs like there is in the D-link configuration.
#
cs7 route-table system
 update route 1.1.30 255.255.255 linkset lset1chn priority 1
 update route 1.1.31 255.255.255 linkset lset2chn priority 1
 update route 1.1.30 255.255.255 linkset lset2chn priority 1
 update route 1.1.31 255.255.255 linkset lset1chn priority 1
 update route 1.1.40 255.255.255 linkset lset2chn priority 1
 update route 1.1.40 255.255.255 linkset lset1chn priority 1

# Routing to Capability Pt Codes of adjacent STPs
 update route 1.1.22 255.255.255 linkset lset1chn priority 1
 update route 1.1.22 255.255.255 linkset lset2chn priority 1
!
#
# The M3UA definition that declares local IP addresses and port #
#
cs7 m3ua 2905
 local-ip 10.0.1.54
 local-ip 10.128.1.239
 keepalive 2000
!
#
# Here as with all configurations, there are *at least* two ASPs defined for each AS
# (one for the primary BTS node and one for the Secondary). In reality, there will be
# at least one for each "User Part" on the BTS10200. So if you have a TCAP Service going
# over SUA and ISUP traffic, you will have a total of at least four ASPs. Primary ISUP,
# Secondary ISUP, Primary TCAP Service, Secondary TCAP Service.
#
# Note that the remote port value of 11146 is configured on the BTS10200 in the
# platform.cfg file (as an SGA command line argument). 2905 is the local port
# value. The remote IP addresses are the BTS IP addresses. They are also obtained
# through the FQDN that is an SGA command line argument.
#
cs7 asp PrimaryBtsIsupAsp 11146 2905 m3ua
 remote-ip 10.0.1.5
 remote-ip 10.128.1.2
!
cs7 asp SecondaryBtsIsupAsp 11146 2905 m3ua
 remote-ip 10.0.1.6
 remote-ip 10.128.1.3
!
#
# Note that the routing key is a very simple one. It has a routing context of 1
# defined, the DPC (BTS OPC) of 1.1.1 defined and a service indicator of ISUP defined.
# This means that all traffic coming from the SS7 Service Provider Network that has a
# DPC of 1.1.1 and a service indicator of ISUP will be sent to either PrimaryBtsIsupAsp
# or SecondaryBtsIsupAsp (depending on which one is active).
#
# The traffic mode is always set to override (not loadshare)
#
# In BTS release 4.4 only, there is a workaround that mandates network-appearance to be
# configured with a value of 1. In BTS release 4.5, this work-around will be removed and
# network-appearance should not be provisioned on the ITP.
#
```

```
cs7 as BtsIsupAs m3ua
 routing-key 1 1.1.1 si isup
 asp PrimaryBtsIsupAsp
 asp SecondaryBtsIsupAsp
 traffic-mode override
 network-appearance 1
!
#
# The SUA definition that declares local IP addresses and port #
#
cs7 sua 14001
 local-ip 10.0.1.54
 local-ip 10.128.1.239
 keepalive 2000
!
#
# Here we are defining an ASPs that will process AIN related traffic. Note that
# the remote port 12205 is a TSA command line parameter in platform.cfg on the BTS.
# 14001 is the local port number.
#
#
cs7 asp PrimaryBtsAinAsp 12205 14001 sua
 remote-ip 10.0.1.5
 remote-ip 10.128.1.2
!
cs7 asp SecondaryBtsAinAsp 12205 14001 sua
 remote-ip 10.0.1.6
 remote-ip 10.128.1.3
!
#
# The following AS is defined for LNP related message flows. The routing context value
# is 4, the DPC (BTS OPC) is 1.1.1, the service indicator is SCCP and the Subsystem number
# is 247. This means that any message received from the SS7 Service Provider that has a
# DPC of 1.1.1, a service indicator of SCCP and an SSN of 247 will be sent to either
# PrimaryBtsAinAsp or SecondaryBtsAinAsp (depending on which one is active).
#
cs7 as BtsLnpAs sua
 routing-key 4 1.1.1 si sccp ssn 247
 asp PrimaryBtsAinAsp
 asp SecondaryBtsAinAsp
 traffic-mode override
```

ITP2 Configuration

```
# This is the second ITP in the ITP-Group (the second SGP in the SG).
#
# FOR THE ITP2 CONFIGURATION, PLEASE REFER TO THE COMMENTS THAT WERE MADE IN
# THE ITP1 CONFIGURATION. IT IS PRETTY MUCH A DUPLICATE OF ITP1 EXCEPT FOR THE
# ITP GROUP DEFINITION (and the comments in the link section).
!
Current configuration : 4054 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ITP2
!
boot-start-marker
boot system flash 2600/c2600-itp-mz.topsail_s_nightly_040915
boot-end-marker
!
```

```
redundancy inter-device
!
enable secret 5 $1$B6u2$gI4fFgjOQo5XppDSWJDfI.
enable password cisco
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 9000
    local-ip 10.0.1.55
    local-ip 10.128.1.240
   remote-port 9001
    remote-ip 10.0.1.54
    remote-ip 10.128.1.239
!
memory-size iomem 10
ip subnet-zero
!
ip domain-name cisco.com
ip name-server 10.0.0.6
!
cs7 variant ANSI
cs7 point-code 1.1.1
!
controller E1 0/0
 framing NO-CRC4
 channel-group 0 timeslots 1
!
controller E1 0/1
 framing NO-CRC4
 channel-group 0 timeslots 1
!
controller E1 0/2
 shutdown
!
controller E1 0/3
 shutdown
!
interface FastEthernet0/0
 ip address 10.0.1.55 255.255.0.0
 speed auto
 half-duplex
 no clns route-cache
!
interface Serial0/0:0
 description connect to link 1 of STP 1-1-20
 no ip address
 encapsulation mtp2
 no clns route-cache
!
interface FastEthernet0/1
 ip address 10.128.1.240 255.255.0.0
 speed auto
 half-duplex
 no clns route-cache
!
interface Serial0/1:0
 description connect to link 1 of STP 1-1-21
 no ip address
 encapsulation mtp2
 no clns route-cache
!
cs7 group grp-ITP2 9003
```

```
 local-ip 10.0.1.55
 local-ip 10.128.1.240
 peer grp-ITP1 9004
  remote-ip 10.0.1.54
  remote-ip 10.128.1.239
!
cs7 linkset lset1chn 1.1.20
 link 0 grp-ITP1 Serial0/0:0
 link 1 grp-ITP2 Serial0/0:0
!
cs7 linkset lset2chn 1.1.21
 link 0 grp-ITP1 Serial0/1:0
 link 1 grp-ITP2 Serial0/1:0
!
cs7 route-table system
 update route 1.1.30 255.255.255 linkset lset1chn priority 1
 update route 1.1.31 255.255.255 linkset lset2chn priority 1
 update route 1.1.30 255.255.255 linkset lset2chn priority 1
 update route 1.1.31 255.255.255 linkset lset1chn priority 1
 update route 1.1.40 255.255.255 linkset lset2chn priority 1
 update route 1.1.40 255.255.255 linkset lset1chn priority 1
# Routing to Capability Pt Codes of adjacent STPs
 update route 1.1.22 255.255.255 linkset lset1chn priority 1
 update route 1.1.22 255.255.255 linkset lset2chn priority 1
!
cs7 m3ua 2905
 local-ip 10.0.1.55
 local-ip 10.128.1.240
!
cs7 asp PrimaryBtsIsupAsp 11146 2905 m3ua
 remote-ip 10.0.1.5
 remote-ip 10.128.1.2
!
cs7 asp SecondaryBtsIsupAsp 11146 2905 m3ua
 remote-ip 10.0.1.6
 remote-ip 10.128.1.3
!
cs7 as BtsIsupAs m3ua
 routing-key 2 1.1.1 si isup
 asp PrimaryBtsIsupAsp
 asp SecondaryBtsIsupAsp
 traffic-mode override
 network-appearance 1
!
cs7 sua 14001
 local-ip 10.0.1.55
 local-ip 10.128.1.240
 keepalive 2000
!
cs7 asp PrimaryBtsAinAsp 12205 14001 sua
 remote-ip 10.0.1.5
 remote-ip 10.128.1.2
!
cs7 asp SecondaryBtsAinAsp 12205 14001 sua
 remote-ip 10.0.1.6
 remote-ip 10.128.1.3
!
cs7 as BtsLnpAs sua
 routing-key 4 1.1.1 si sccp ssn 247
 asp PrimaryBtsAinAsp
 asp SecondaryBtsAinAsp
 traffic-mode override
```

Cisco BTS 10200 Provisioning for the Basic A-link Profile

CA Configuration

```
########################################################################
#
# CA Configuration
#
########################################################################
add ca-config type=MGCP-INIT-TERMS;value=160;datatype=integer;
add ca-config type=MGCP-INIT-DURATION;value=5;datatype=integer;
add ca-config type=MGCP-ICMP-PING-RETRANSMIT-DURATION;value=5;datatype=integer;
add ca-config type=MGCP-ICMP-PING-RETRY-COUNT;value=5;datatype=integer;
add ca-config type=MGCP-MAX-UNREACH-COUNT;value=5;datatype=integer;
add ca-config type=MGCP-MAX-FAULT-COUNT;value=5;datatype=integer;
add ca-config type=MGCP-ADM-RESP-TIME;value=300;datatype=integer;
add ca-config type=MGCP-SIG-TOS-LOWDELAY;value=Y;datatype=boolean;
add ca-config type=MGCP-SIG-TOS-PRECEDENCE;value=1;datatype=integer;
add ca-config type=MGCP-SIG-TOS-RELIABILITY;value=Y;datatype=boolean;
add ca-config type=MGCP-SIG-TOS-THROUGHPUT;value=Y;datatype=boolean;
#
# CA & FS
#
add call-agent id=CA146; tsap-addr-sidea=hrn11ca; mgw-monitoring-enabled=N;
add feature-server id=FSAIN205; tsap-addr-sidea=hrn11ca:11205; type=AIN;

#
# Sigtran components
#
add user-part-variant id=ANSISS7_GR317;
#
# Unlike the D-link solution that requires two SG definitions for each SG-GRP,
# A-link (Basic Distributed MTP3) solution requires that only one SG be associated
# with the SG-GRP. This is because redundancy in the A-link solution is at the SGP
# level (not the SG level).
#
add sg id=sg1; description=Siganling gateway 1;
add sg-grp id=sg-grp1; sg1-id=sg1; description=SG group 1;

#
# Note that there are two SGP definitions per SG. This is in contrast to the
# D-link solution that only allows one SGP per SG. It is at the SGP level that
# the A-link/Distributed MTP3 solution provides hardware and IP network
# redundancy. Note that the naming convention used in this example is
# descriptive.. i.e. SGP1 of SG1 or SGP2 of SG1.
#
add sgp id=sg1-sgp1 ; sg-id=sg1; description=SG process 1 for sg1;
add sgp id=sg1-sgp2 ; sg-id=sg1; description=SG process 2 for sg1;

add opc id=opc1; point-code=1-1-1; description=OPC; point-code-type=ANSI_CHINA;
add dpc id=dpc1; point-code=1-1-30; description=DPC 1; point-code-type=ANSI_CHINA;
add dpc id=dpc2; point-code=1-1-31; description=DPC 2; point-code-type=ANSI_CHINA;

#
# THE ISUP ROUTING KEYS
#
add routing-key id=rk1; opc-id=opc1; sg-grp-id=sg-grp1; si=ISUP; rc=1; platform-id=CA146;

add call-ctrl-route id=dpc1-route1; dpc-id=dpc1; routing-key-id=rk1; si=isup;
user-part-variant-id= ANSISS7_GR317
add call-ctrl-route id=dpc2-route1; dpc-id=dpc2; routing-key-id=rk1; si=isup;
user-part-variant-id= ANSISS7_GR317;
```

```
#
# SCTP configuration.
#
add sctp-assoc-profile id=sctp-prof;

#
# Note that the id used in the add sctp-assoc statement reflects the fact that
# this is the sctp association for SGP1 of SG1.
#
add sctp-assoc id=sg1-sgp1-sctp; sgp-id=sg1-sgp1; sctp-assoc-profile-id=sctp-prof;
platform-id=CA146; remote-port=2905; remote-tsap-addr1=10.0.1.54;
remote-tsap-addr2=10.128.1.239; dscp=AF11; ip-tos-precedence=ROUTINE;

add sctp-assoc id=sg2-sgp1-sctp; sgp-id=sg2-sgp1; sctp-assoc-profile-id=sctp-prof;
platform-id=CA146; remote-port=2905; remote-tsap-addr1=10.0.1.55;
remote-tsap-addr2=10.128.1.240; dscp=AF11; ip-tos-precedence=ROUTINE;

#
# dial plan profile
#
add digman-profile id=pretrans;
add digman id=pretrans; rule=1; match-string=^*; replace-string=&; match-noa=any;
replace-noa=VSC;
add digman id=pretrans; rule=2; match-string=^#; replace-string=&; match-noa=any;
replace-noa=VSC;
add digman-profile id=ani_20;
add digman id=ani_20; rule=1; match-string=^20; replace-string=none;
add dial-plan-profile id=dp-1; nanp-dial-plan=Y; description=NA dial plan profile;
dnis-digman-id=pretrans; ani-digman-id=ani_20;
#
# SS7 TG
#
add ss7-ansi-tg-profile ID=ansi-tg-prof;
add trunk-grp ID=1; call_agent_id=CA146; tg_type=SS7; direction=BOTH;
tg_profile_id=ansi-tg-prof; call-ctrl-route-id=dpc1-route1; dial-plan-id=dp-1;
description=TG to DPC 1;  MGCP_PKG_TYPE=T;
add trunk-grp ID=2; call_agent_id=CA146; tg_type=SS7; direction=BOTH;
tg_profile_id=ansi-tg-prof; call-ctrl-route-id=dpc2-route1; dial-plan-id=dp-1;
description=TG to DPC 2;  MGCP_PKG_TYPE=T;
#
# MGW
#
add mgw-profile id=as5300-prof; vendor=Cisco; mgcp-hairpin-supp=n; MGCP_RSIPSTAR_SUPP=N;
MGCP_TERM_INIT_LEVEL=0; RBK_ON_CONN_SUPP=N; MGCP_VERSION=MGCP_1_0; mgcp-max2-retries=3;
fax-t38-camode-supp=Y; mgcp-keepalive-interval=60; mgcp-keepalive-retries=10;
mgcp-t-tran=400; mgcp-max1-retries=2; mgcp-t-longtran=5; mgcp-default-pkg=NONE;
MGCP_3WAY_HSHAKE_SUPP=N; mgw_type=AS5300; PC_MPTIME_SUPP=N;
##
MGCP_VERSION=MGCP_1_0; PC_MPTIME_SUPP=N;
add mgw id=va-5350-23; tsap-addr=va-5350-23.hrndevtest.cisco.com; call-agent-id=CA146;
mgw-profile-id=as5300-prof; type=TGW;
#
# SS7 terminations and trunks
#
add termination prefix=S3/DS1-4/; port-start=1; port-end=31; type=trunk;
mgw-id=va-5350-23;
add termination prefix=S3/DS1-5/; port-start=1; port-end=31; type=trunk;
mgw-id=va-5350-23;
add trunk cic-start=1; cic-end=31; tgn-id=1; mgw-id=va-5350-23;
termination-prefix=S3/DS1-4/; termination-port-start=1; termination-port-end=31;
add trunk cic-start=1; cic-end=31; tgn-id=2; mgw-id=va-5350-23;
termination-prefix=S3/DS1-5/; termination-port-start=1; termination-port-end=31;
```

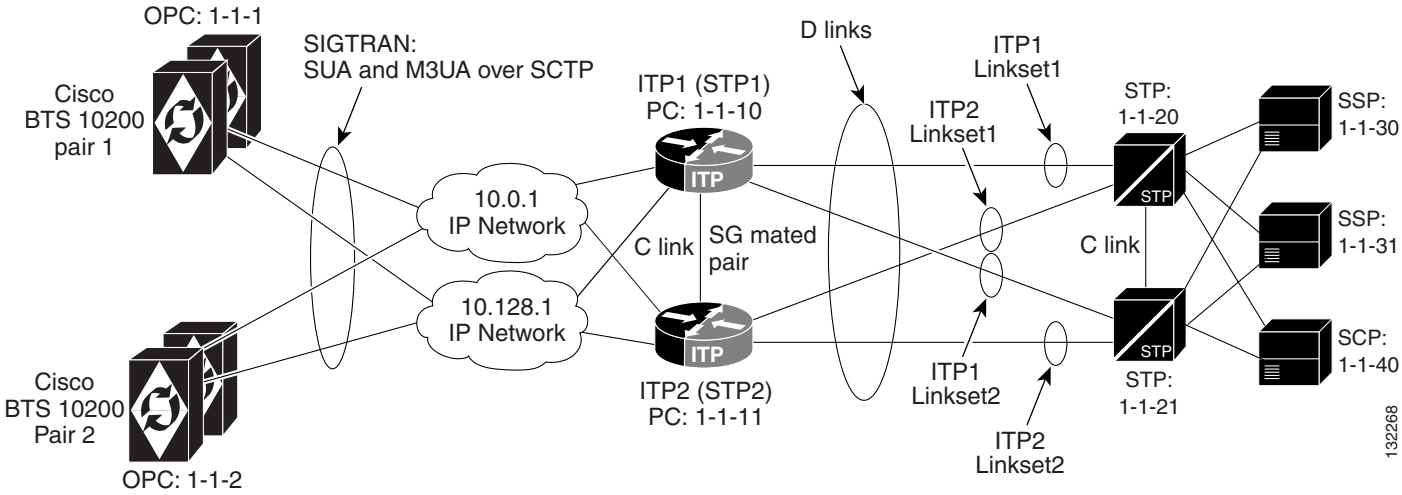
```
#
# SS7 routes, route guides and destinations
#
add route id=dpc1-route; tg_selection=RR; tgn1_id=1;
add route id=dpc2-route; tg_selection=RR; tgn1_id=2;
add route-guide id=dpc1-rg; policy-type=ROUTE; policy-id=dpc1-route;
add route-guide id=dpc2-rg; policy-type=ROUTE; policy-id=dpc2-route;
add destination dest-id=dpc1-dest; call-type=LOCAL; route-type=ROUTE;
route-guide-id=dpc1-rg;
add destination dest-id=dpc2-dest; call-type=LOCAL; route-type=ROUTE;
route-guide-id=dpc2-rg;

#####################################
#   TCAP/SUA Provisioning for LNP
#####################################

add sccp-nw id=1;NET_IND=NATIONAL;SUB_SVC=NATIONAL;HOP_COUNT=3;

add subsystem-profile id=SSN_LNP1;platform_id=FSAIN205;

add subsystem id=SSN_LNP1; OPC-ID=opc1; LOCAL-SSN=247;REMOTE_SSN=247;
sccp-nw-id=1;SCCP_VERSION=ANS92; TCAP_VERSION=ANS92; APPLICATION_VERSION=AIN01;

add routing-key id=itp-grp-rk2; opc-id=opc1; sg-grp-id=sg-grp1; si=sccp; ssn-id=SSN_LNP1;
platform-id=FSAIN205; rc=4; description=Routing Key for SUA User Adaptation layer;

########################################
# Provisioned DPC is the STP Capabilty Pt Code
########################################
add dpc id=stp_cap_pc; point-code=1-1-22; point-code-type=ANSI_CHINA;
description=Capability Point Code of STPs

add feature fname=LNP; feature-server-id=FSAIN205; description=Local number portability;
tdp1=COLLECTED_INFORMATION; tid1=LNP_TRIGGER; ttype1=R;

add ported-office-code digit-string=301-612; in-call-agent=n;

add CA-Config type=DEFAULT-LNP-SLHR-ID; datatype=string;  value=slhr_lnp;

add slhr-profile id=slhr_lnp;

add slhr id=slhr_lnp; gtt-req=Y; tt=11; GTT_ADDR_TYPE=CDPN; GTT_ADDR=3; opc-id=opc1;
dpc-id=stp_cap_pc; ssn_id=SSN_LNP1;

add sccp-route opc-id=opc1; dpc-id=stp_cap_pc; rk-id=itp-grp-rk2; ssn-id=SSN_LNP1;
description=LNP for opc1;

add pop ID=50901; STATE=tx; COUNTRY=US; TIMEZONE=CDT; LOCAL_7D_DIALING=Y; ITP=N;
ZERO_MINUS=LEC; BLOCK_EAWOPIC=Y; CNAM_OPTION=EXT_LIDB; PIC2_REQD=N; MY_LRN=4692559999;
TREAT_IMS_ANONYMOUS=N; OPC_ID=opc1; ZERO_PLUS_LOCAL=N

#####################################################
# Control network entities in-service for ANSI SS7
#####################################################
control trunk-grp id=1; mode=forced; target-state=ins;
control trunk-grp id=2; mode=forced; target-state=ins;
equip trunk-termination tgn-id=1; cic=all;
equip trunk-termination tgn-id=2; cic=all;
control trunk-termination tgn-id=1; cic=all; target-state=INS;  mode=FORCED;
control trunk-termination tgn-id=2; cic=all; target-state=INS;  mode=FORCED;
control subsystem id=SSN_LNP1;mode=forced;target-state=uis;opc-id=opc1
control sctp-assoc id=sg1-sgp1-sctp; mode=forced; target-state=INS;
control sctp-assoc id=sg2-sgp1-sctp; mode=forced; target-state=INS;
```

```
############################################################
# Status commands
############################################################
#status trunk-grp id=1;
#status trunk-grp id=2;
#status trunk-termination tgn-id=1; cic=all;
#status trunk-termination tgn-id=2; cic=all;
#status sctp-assoc id=sg1-sgp1-sctp;
#status sctp-assoc id=sg2-sgp1-sctp;
```

Multiple Cisco BTS 10200 Nodes per Cisco ITP

This profile is a scalable IP telephony network profile that fits the customer who wants to set up an all-IP telephony network based on Cisco BTS 10200 Softswitches and a long-term need of network expansion.

Figure 5-6 Multiple Cisco BTS 10200 Nodes per Cisco ITP



Usage

Because each Cisco BTS 10200 has just one OPC code rather than having multiple OPCs, this profile is ideal when there is a requirement for very high-capacity traffic to each OPC. A pair of high-capacity Cisco 73XX or 7507 series Cisco ITP nodes will most likely be required to provide the necessary throughput. The topology between ITPs and STPs forms a typical SS7 STP quad. GTT can be supported on the Cisco ITP.

Alternate Base Profiles

There are no alternate profiles. This profile is only available when connecting to the SS7 network via D-links.

ITP Configuration Information

The Cisco ITP configuration information is essentially the same as the configuration for the basic D-link profile provided in the "ITP Configuration Information" section on page 5-10. The main exception is that in this case, there is extra ASP configuration information for communicating to the second CA (BTS2). Also, there is extra information in the AS configuration section for routing to each of the Call Agents (based on DPC [Cisco BTS 10200 OPC value]). The following example shows the ASP and AS configuration elements for ITP1.

ITP1 Configuration.

```
################################################################################
## ITP1 Configuration -
## It is important to note that ITP2 will have the same ASP and AS
## configuration information that is shown below for ITP1.
################################################################################
## ASP configuration for BTS1 Active and Standby Nodes
# For ISUP - M3UA
cs7 asp PRI_ISUP_BTS1 11146 2905 m3ua
 remote-ip 10.0.1.5
 remote-ip 10.128.1.2

cs7 asp SEC_ISUP_BTS1 11146 2905 m3ua
 remote-ip 10.0.1.6
 remote-ip 10.128.1.3

# For TCAP/AIN - SUA
cs7 asp PRI_AIN_BTS1 12205 14001 sua
remote-ip 10.0.1.5
 remote-ip 10.128.1.2
!
cs7 asp SEC_AIN_BTS1 12205 14001 sua
remote-ip 10.0.1.6
 remote-ip 10.128.1.3

## AS configuration for BTS1
#
# Note: In the following configuration the routing context entries are as follows:
# routing context = 1, DPC(BTS OPC)=1.1.1 service indicator=ISUP
# Configuring network-appearance 1 is required for release 4.4, but will not be required
# in release 4.5 and beyond.

cs7 as ISUP_BTS1 m3ua
 routing-key 1 1.1.1 si isup
 asp PRI_ISUP_BTS1
 asp SEC_ISUP_BTS1
 traffic-mode override
 network-appearance 1

cs7 as LNP_BTS1 sua
 routing-key 4 1.1.1 si sccp ssn 247
 asp PRI_AIN_BTS1
 asp SEC_AIN_BTS1
 traffic-mode override

## ASP configuration for BTS2 Active and Standby Nodes
## For ISUP - M3UA
cs7 asp PRI_ISUP_BTS2 11146 2905 m3ua
 remote-ip 10.0.1.7
 remote-ip 10.128.1.4

cs7 asp SEC_ISUP_BTS2 11146 2905 m3ua
 remote-ip 10.0.1.8
 remote-ip 10.128.1.5

# For TCAP/AIN - SUA
cs7 asp PRI_AIN_BTS2 12205 14001 sua
 remote-ip 10.0.1.7
 remote-ip 10.128.1.4
!
cs7 asp SEC_AIN_BTS2 12205 14001 sua
remote-ip 10.0.1.8
 remote-ip 10.128.1.5
```

```
## AS configuration for BTS2
# Note that the DPC value changes to 1.1.2 for sending messages to BTS2
cs7 as ISUP_BTS2 m3ua
 routing-key 2 1.1.2 si isup
 asp PRI_ISUP_BTS2
 asp SEC_ISUP_BTS2
 traffic-mode override
 network-appearance 1

cs7 as LNP_BTS2 sua
 routing-key 5 1.1.2 si sccp ssn 247
 asp PRI_AIN_BTS2
 asp SEC_AIN_BTS2
 traffic-mode override
```

Cisco BTS 10200 Provisioning Information

The Cisco BTS 10200 provisioning for this profile is essentially the same as the basic D-link profile in the "Cisco BTS 10200 Provisioning for the Basic D-link Profile" section on page 5-18, except that there is a second Cisco BTS 10200 provisioning script that is needed for BTS2. It is shown here:

CA Configuration

```
###############################################################################
#
# CA Configuration
#
###############################################################################

add ca-config type=MGCP-INIT-TERMS;value=160;datatype=integer;
add ca-config type=MGCP-INIT-DURATION;value=5;datatype=integer;
add ca-config type=MGCP-ICMP-PING-RETRANSMIT-DURATION;value=5;datatype=integer;
add ca-config type=MGCP-ICMP-PING-RETRY-COUNT;value=5;datatype=integer;
add ca-config type=MGCP-MAX-UNREACH-COUNT;value=5;datatype=integer;
add ca-config type=MGCP-MAX-FAULT-COUNT;value=5;datatype=integer;
add ca-config type=MGCP-ADM-RESP-TIME;value=300;datatype=integer;
add ca-config type=MGCP-SIG-TOS-LOWDELAY;value=Y;datatype=boolean;
add ca-config type=MGCP-SIG-TOS-PRECEDENCE;value=1;datatype=integer;
add ca-config type=MGCP-SIG-TOS-RELIABILITY;value=Y;datatype=boolean;
add ca-config type=MGCP-SIG-TOS-THROUGHPUT;value=Y;datatype=boolean;
#
# CA & FS
#
# Note that the ids: CA147 and FSAIN206 are different than on BTS1.
#
add call-agent id=CA147; tsap-addr-sidea=hrn11ca; mgw-monitoring-enabled=N;
add feature-server id=FSAIN206; tsap-addr-sidea=hrn11ca:11205; type=AIN;
#
# Sigtran components
#
add user-part-variant id=ANSISS7_GR317;

add sg id=sg1; description=Signaling gateway 1;
add sg id=sg2; description=Signaling gateway 2;

add sg-grp id=sg-grp1; sg1-id=sg1; sg2-id=sg2 description=SG group 1;

add sgp id=sg1-sgp1 ; sg-id=sg1; description=SG process 1 for sg1;
add sgp id=sg2-sgp1 ; sg-id=sg2; description=SG process 1 for sg2;

#
# Note that the OPC value for BTS2 is 1-1-2
#
```

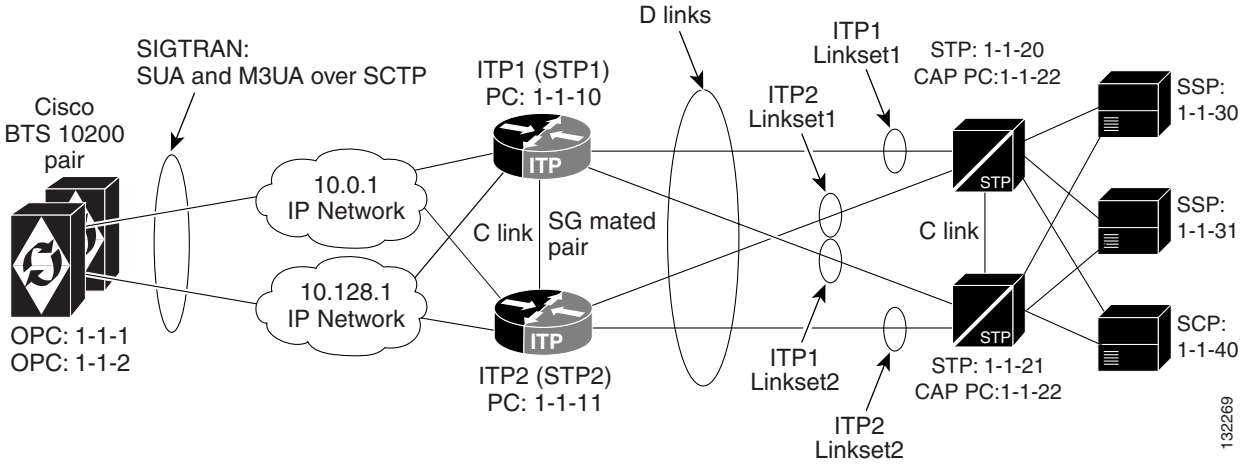
```
add opc id=opc1; point-code=1-1-2; description=OPC; point-code-type=ANSI_CHINA;
add dpc id=dpc1; point-code=1-1-30; description=DPC 1; point-code-type=ANSI_CHINA;
add dpc id=dpc2; point-code=1-1-31; description=DPC 2; point-code-type=ANSI_CHINA;
#
# THE ISUP ROUTING KEYS
#
# Note that a unique rc value was needed when defining the routing-key. It must match
# the rc value that is defined in the associated AS/routing-key definition in the ITPs.
# This routing key has a different OPC value than defined for BTS1.
#
add routing-key id=rk1; opc-id=opc1; sg-grp-id=sg-grp1; si=ISUP; rc=2; platform-id=CA147;

add call-ctrl-route id=dpc1-route1; dpc-id=dpc1; routing-key-id=rk1; si=isup;
user-part-variant-id= ANSISS7_GR317
add call-ctrl-route id=dpc2-route1; dpc-id=dpc2; routing-key-id=rk1; si=isup;
user-part-variant-id= ANSISS7_GR317;

add sctp-assoc-profile id=sctp-prof;
#
# THE SCTP ASSOCIATIONS
#
add sctp-assoc id=sg1-sgp1-sctp; sgp-id=sg1-sgp1; sctp-assoc-profile-id=sctp-prof;
platform-id=CA147; remote-port=2905; remote-tsap-addr1=10.0.1.54;
remote-tsap-addr2=10.128.1.239; dscp=AF11; ip-tos-precedence=ROUTINE;

add sctp-assoc id=sg2-sgp1-sctp; sgp-id=sg2-sgp1; sctp-assoc-profile-id=sctp-prof;
platform-id=CA147; remote-port=2905; remote-tsap-addr1=10.0.1.55;
remote-tsap-addr2=10.128.1.240; dscp=AF11; ip-tos-precedence=ROUTINE;

#
# dial plan profile
#
add digman-profile id=pretrans;
add digman id=pretrans; rule=1; match-string=^*; replace-string=&; match-noa=any;
replace-noa=VSC;
add digman id=pretrans; rule=2; match-string=^#; replace-string=&; match-noa=any;
replace-noa=VSC;
add digman-profile id=ani_20;
add digman id=ani_20; rule=1; match-string=^20; replace-string=none;
add dial-plan-profile id=dp-1; nanp-dial-plan=Y; description=NA dial plan profile;
dnis-digman-id=pretrans; ani-digman-id=ani_20;
#
# SS7 TG
#
add ss7-ansi-tg-profile ID=ansi-tg-prof;
add trunk-grp ID=1; call_agent_id=CA147; tg_type=SS7; direction=BOTH;
tg_profile_id=ansi-tg-prof; call-ctrl-route-id=dpc1-route1; dial-plan-id=dp-1;
description=TG to DPC 1;  MGCP_PKG_TYPE=T;
add trunk-grp ID=2; call_agent_id=CA147; tg_type=SS7; direction=BOTH;
tg_profile_id=ansi-tg-prof; call-ctrl-route-id=dpc2-route1; dial-plan-id=dp-1;
description=TG to DPC 2;  MGCP_PKG_TYPE=T;
#
# MGW
#
add mgw-profile id=as5300-prof; vendor=Cisco; mgcp-hairpin-supp=n; MGCP_RSIPSTAR_SUPP=N;
MGCP_TERM_INIT_LEVEL=0; RBK_ON_CONN_SUPP=N; MGCP_VERSION=MGCP_1_0; mgcp-max2-retries=3;
fax-t38-camode-supp=Y; mgcp-keepalive-interval=60; mgcp-keepalive-retries=10;
mgcp-t-tran=400; mgcp-max1-retries=2; mgcp-t-longtran=5; mgcp-default-pkg=NONE;
MGCP_3WAY_HSHAKE_SUPP=N; mgw_type=AS5300; PC_MPTIME_SUPP=N;
##
MGCP_VERSION=MGCP_1_0; PC_MPTIME_SUPP=N;
add mgw id=va-5350-23; tsap-addr=va-5350-23.hrndevtest.cisco.com; call-agent-id=CA147;
mgw-profile-id=as5300-prof; type=TGW;
```

```
#
# SS7 terminations and trunks
#
add termination prefix=S3/DS1-4/; port-start=1; port-end=31; type=trunk;
mgw-id=va-5350-23;
add termination prefix=S3/DS1-5/; port-start=1; port-end=31; type=trunk;
mgw-id=va-5350-23;
add trunk cic-start=1; cic-end=31; tgn-id=1; mgw-id=va-5350-23;
termination-prefix=S3/DS1-4/; termination-port-start=1; termination-port-end=31;
add trunk cic-start=1; cic-end=31; tgn-id=2; mgw-id=va-5350-23;
termination-prefix=S3/DS1-5/; termination-port-start=1; termination-port-end=31;
#
# SS7 routes, route guides and destinations
#
add route id=dpc1-route; tg_selection=RR; tgn1_id=1;
add route id=dpc2-route; tg_selection=RR; tgn1_id=2;
add route-guide id=dpc1-rg; policy-type=ROUTE; policy-id=dpc1-route;
add route-guide id=dpc2-rg; policy-type=ROUTE; policy-id=dpc2-route;
add destination dest-id=dpc1-dest; call-type=LOCAL; route-type=ROUTE;
route-guide-id=dpc1-rg;
add destination dest-id=dpc2-dest; call-type=LOCAL; route-type=ROUTE;
route-guide-id=dpc2-rg;

#####################################
# TCAP/SUA Provisioning for LNP
#####################################

add sccp-nw id=1;NET_IND=NATIONAL;SUB_SVC=NATIONAL;HOP_COUNT=3;

add subsystem-profile id=SSN_LNP1;platform_id=FSAIN206;

add subsystem id=SSN_LNP1; OPC-ID=opc1; LOCAL-SSN=247;REMOTE_SSN=247;
sccp-nw-id=1;SCCP_VERSION=ANS92; TCAP_VERSION=ANS92; APPLICATION_VERSION=AIN01;

# Note this routing key differs from the one on BTS1
add routing-key id=itp-grp-rk2; opc-id=opc1; sg-grp-id=sg-grp1; si=sccp; ssn-id=SSN_LNP1;
platform-id=FSAIN206; rc=5; description=Routing Key for SUA User Adaptation layer;

########################################
# Provisioned DPC is the STP Capabilty Pt Code
########################################
add dpc id=stp_cap_pc; point-code=1-1-22; point-code-type=ANSI_CHINA;
description=Capability Point Code of STPs

add feature fname=LNP; feature-server-id=FSAIN206; description=Local number portability;
tdp1=COLLECTED_INFORMATION; tid1=LNP_TRIGGER; ttype1=R;

add ported-office-code digit-string=301-612; in-call-agent=n;

add CA-Config type=DEFAULT-LNP-SLHR-ID; datatype=string;  value=slhr_lnp;

add slhr-profile id=slhr_lnp;

add slhr id=slhr_lnp; gtt-req=Y; tt=11; GTT_ADDR_TYPE=CDPN; GTT_ADDR=3; opc-id=opc1;
dpc-id=stp_cap_pc; ssn_id=SSN_LNP1;

add sccp-route opc-id=opc1; dpc-id=stp_cap_pc; rk-id=itp-grp-rk2; ssn-id=SSN_LNP1;
description=LNP for opc1;

add pop ID=50901; STATE=tx; COUNTRY=US; TIMEZONE=CDT; LOCAL_7D_DIALING=Y; ITP=N;
ZERO_MINUS=LEC; BLOCK_EAWOPIC=Y; CNAM_OPTION=EXT_LIDB; PIC2_REQD=N; MY_LRN=4692559999;
TREAT_IMS_ANONYMOUS=N; OPC_ID=opc1; ZERO_PLUS_LOCAL=N
```

Multiple Cisco BTS 10200 OPCs with D-Link Profile

This profile, based on the D-link profile, fits the customer who wants to emulate multiple legacy SS7 switches with one high-capacity Cisco BTS 10200 Softswitch.

Figure 5-7 Multiple Cisco BTS 10200 OPCs with D-link Profile



Alternate Base Profiles

Although this profile is based on the D-link profile, a similar A-link profile can be implemented. However, it is not a very desirable method for achieving multiple OPCs on the Cisco BTS 10200 because it requires a separate ITP-Group for each OPC.

ITP Configuration Information

The Cisco ITP configuration is essentially the same as the configuration for the D-link profile in the "ITP Configuration Information" section on page 5-10. The only difference is that there is an extra AS configuration information for the added OPC on BTS1. This additional AS configuration information is shown here:

```
cs7 as BtsIsupAs2 m3ua
 routing-key 2 1.1.2 si isup
 asp PrimaryBtsIsupAsp
 asp SecondaryBtsIsupAsp
 traffic-mode override
 network-appearance 1

cs7 as BtsLnpAs2 sua
 routing-key 5 1.1.2 si sccp ssn 247
 asp PrimaryBtsAinAsp
 asp SecondaryBtsAinAsp
 traffic-mode override
```

Cisco BTS 10200 Provisioning Information

The Cisco BTS 10200 Provisioning information is essentially the same as the basic D-link configuration in the "Cisco BTS 10200 Provisioning for the Basic D-link Profile" section on page 5-18 with some added objects based on the OPC 1.1.2. The Cisco BTS 10200 configuration is shown here.

```
###############################################################################
#
# CA Configuration
#
###############################################################################

add ca-config type=MGCP-INIT-TERMS;value=160;datatype=integer;
add ca-config type=MGCP-INIT-DURATION;value=5;datatype=integer;
add ca-config type=MGCP-ICMP-PING-RETRANSMIT-DURATION;value=5;datatype=integer;
add ca-config type=MGCP-ICMP-PING-RETRY-COUNT;value=5;datatype=integer;
add ca-config type=MGCP-MAX-UNREACH-COUNT;value=5;datatype=integer;
add ca-config type=MGCP-MAX-FAULT-COUNT;value=5;datatype=integer;
add ca-config type=MGCP-ADM-RESP-TIME;value=300;datatype=integer;
add ca-config type=MGCP-SIG-TOS-LOWDELAY;value=Y;datatype=boolean;
add ca-config type=MGCP-SIG-TOS-PRECEDENCE;value=1;datatype=integer;
add ca-config type=MGCP-SIG-TOS-RELIABILITY;value=Y;datatype=boolean;
add ca-config type=MGCP-SIG-TOS-THROUGHPUT;value=Y;datatype=boolean;
#
# CA & FS
#
add call-agent id=CA146; tsap-addr-sidea=hrn11ca; mgw-monitoring-enabled=N;
add feature-server id=FSAIN205; tsap-addr-sidea=hrn11ca:11205; type=AIN;

#
# Sigtran / SS7 components
#
add user-part-variant id=ANSISS7_GR317;
add sg id=sg1; description=Signaling gateway 1;
add sg id=sg2; description=Signaling gateway 2;

add sg-grp id=sg-grp1; sg1-id=sg1; sg2-id=sg2 description=SG group 1;

add sgp id=sg1-sgp1 ; sg-id=sg1; description=SG process 1 for sg1;
add sgp id=sg2-sgp1 ; sg-id=sg2; description=SG process 1 for sg2;

add opc id=opc1; point-code=1-1-1; description=OPC1; point-code-type=ANSI_CHINA;

# The Second OPC
add opc id=opc2; point-code=1-1-2; description=OPC2; point-code-type=ANSI_CHINA;

add dpc id=dpc1; point-code=1-1-30; description=DPC 1; point-code-type=ANSI_CHINA;
add dpc id=dpc2; point-code=1-1-31; description=DPC 2; point-code-type=ANSI_CHINA;

# THE ISUP ROUTING KEYS
add routing-key id=rk1; opc-id=opc1; sg-grp-id=sg-grp1; si=ISUP; rc=1; platform-id=CA146;

# The new ISUP routing key added for OPC2
add routing-key id=rk2; opc-id=opc2; sg-grp-id=sg-grp1; si=ISUP; rc=2; platform-id=CA146;

add call-ctrl-route id=dpc1-route1; dpc-id=dpc1; routing-key-id=rk1; si=isup;
user-part-variant-id= ANSISS7_GR317
add call-ctrl-route id=dpc2-route1; dpc-id=dpc2; routing-key-id=rk1; si=isup;
user-part-variant-id= ANSISS7_GR317;

# Two New Routes added for OPC2
add call-ctrl-route id=dpc1-route2; dpc-id=dpc1; routing-key-id=rk2; si=isup;
user-part-variant-id= ANSISS7_GR317
```

```
add call-ctrl-route id=dpc2-route2; dpc-id=dpc2; routing-key-id=rk2; si=isup;
user-part-variant-id= ANSISS7_GR317;


add sctp-assoc-profile id=sctp-prof;

# THE SCTP ASSOCIATIONS
add sctp-assoc id=sg1-sgp1-sctp; sgp-id=sg1-sgp1; sctp-assoc-profile-id=sctp-prof;
platform-id=CA146; remote-port=2905; remote-tsap-addr1=10.0.1.54;
remote-tsap-addr2=10.128.1.239; dscp=AF11; ip-tos-precedence=ROUTINE;

add sctp-assoc id=sg2-sgp1-sctp; sgp-id=sg2-sgp1; sctp-assoc-profile-id=sctp-prof;
platform-id=CA146; remote-port=2905; remote-tsap-addr1=10.0.1.55;
remote-tsap-addr2=10.128.1.240; dscp=AF11; ip-tos-precedence=ROUTINE;

#
# dial plan profile
#
add digman-profile id=pretrans;
add digman id=pretrans; rule=1; match-string=^*; replace-string=&; match-noa=any;
replace-noa=VSC;
add digman id=pretrans; rule=2; match-string=^#; replace-string=&; match-noa=any;
replace-noa=VSC;
add digman-profile id=ani_20;
add digman id=ani_20; rule=1; match-string=^20; replace-string=none;
add dial-plan-profile id=dp-1; nanp-dial-plan=Y; description=NA dial plan profile;
dnis-digman-id=pretrans; ani-digman-id=ani_20;
#
# SS7 TG
#
add ss7-ansi-tg-profile ID=ansi-tg-prof;
add trunk-grp ID=1; call_agent_id=CA146; tg_type=SS7; direction=BOTH;
tg_profile_id=ansi-tg-prof; call-ctrl-route-id=dpc1-route1; dial-plan-id=dp-1;
description=TG to DPC 1;  MGCP_PKG_TYPE=T;
add trunk-grp ID=2; call_agent_id=CA146; tg_type=SS7; direction=BOTH;
tg_profile_id=ansi-tg-prof; call-ctrl-route-id=dpc2-route1; dial-plan-id=dp-1;
description=TG to DPC 2;  MGCP_PKG_TYPE=T;

# Two new trunk-groups added for OPC2
add trunk-grp ID=3; call_agent_id=CA146; tg_type=SS7; direction=BOTH;
tg_profile_id=ansi-tg-prof; call-ctrl-route-id=dpc1-route2; dial-plan-id=dp-1;
description=TG2 to DPC 1;  MGCP_PKG_TYPE=T;
add trunk-grp ID=4; call_agent_id=CA146; tg_type=SS7; direction=BOTH;
tg_profile_id=ansi-tg-prof; call-ctrl-route-id=dpc2-route2; dial-plan-id=dp-1;
description=TG2 to DPC 2;  MGCP_PKG_TYPE=T;


#
# MGW
#
add mgw-profile id=as5300-prof; vendor=Cisco; mgcp-hairpin-supp=n; MGCP_RSIPSTAR_SUPP=N;
MGCP_TERM_INIT_LEVEL=0; RBK_ON_CONN_SUPP=N; MGCP_VERSION=MGCP_1_0; mgcp-max2-retries=3;
fax-t38-camode-supp=Y; mgcp-keepalive-interval=60; mgcp-keepalive-retries=10;
mgcp-t-tran=400; mgcp-max1-retries=2; mgcp-t-longtran=5; mgcp-default-pkg=NONE;
MGCP_3WAY_HSHAKE_SUPP=N; mgw_type=AS5300; PC_MPTIME_SUPP=N;
##
MGCP_VERSION=MGCP_1_0; PC_MPTIME_SUPP=N;
add mgw id=va-5350-23; tsap-addr=va-5350-23.hrndevtest.cisco.com; call-agent-id=CA146;
mgw-profile-id=as5300-prof; type=TGW;
#
# SS7 terminations and trunks
#
add termination prefix=S3/DS1-4/; port-start=1; port-end=31; type=trunk;
mgw-id=va-5350-23;
```

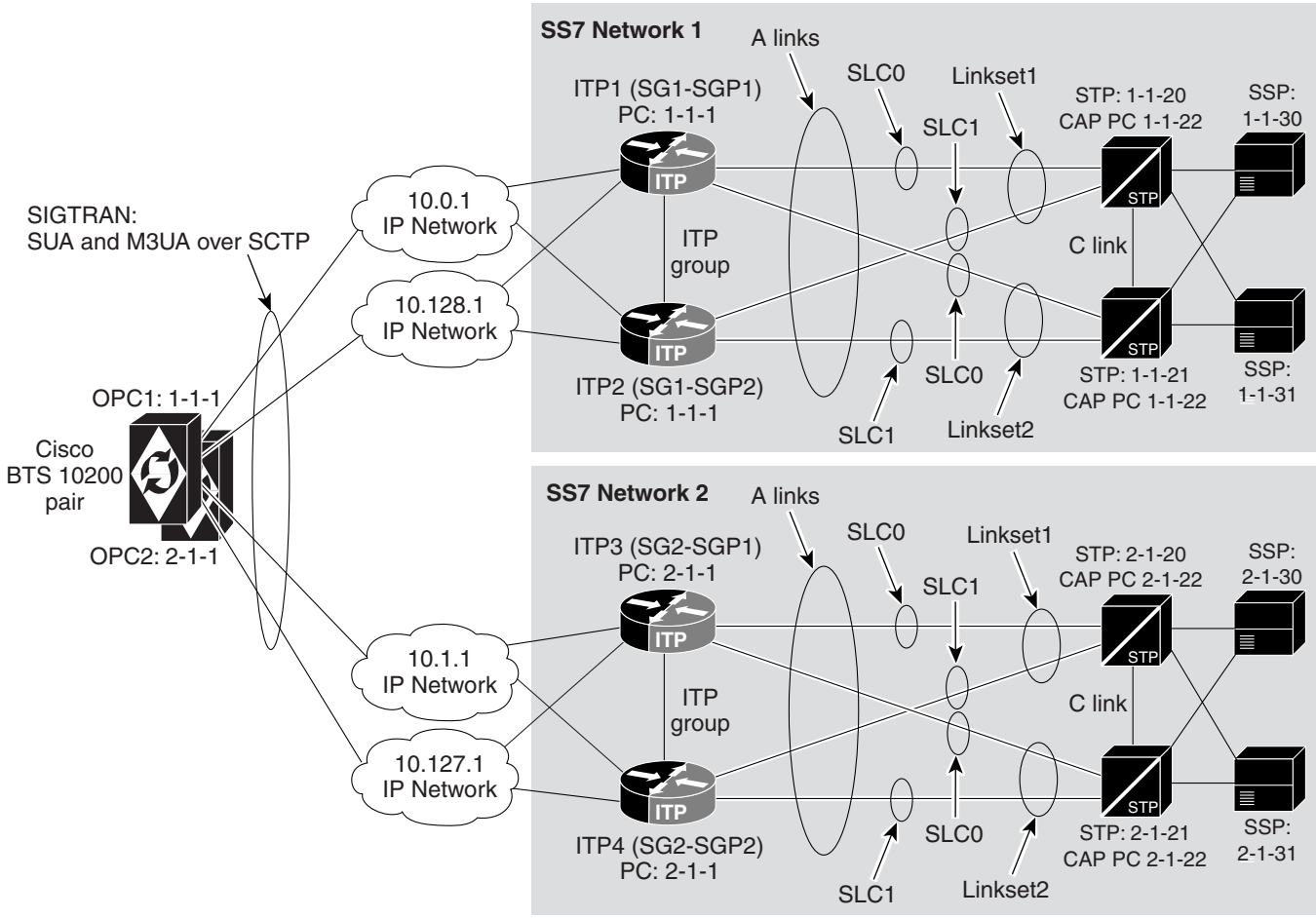
```
add termination prefix=S3/DS1-5/; port-start=1; port-end=31; type=trunk;
mgw-id=va-5350-23;

add trunk cic-start=1; cic-end=31; tgn-id=1; mgw-id=va-5350-23;
termination-prefix=S3/DS1-4/; termination-port-start=1; termination-port-end=31;

add trunk cic-start=1; cic-end=31; tgn-id=2; mgw-id=va-5350-23;
termination-prefix=S3/DS1-5/; termination-port-start=1; termination-port-end=31;

# New termination and trunk information for OPC2
add termination prefix=S3/DS1-6/; port-start=1; port-end=31; type=trunk;
mgw-id=va-5350-23;

add termination prefix=S3/DS1-7/; port-start=1; port-end=31; type=trunk;
mgw-id=va-5350-23;

add trunk cic-start=1; cic-end=31; tgn-id=3; mgw-id=va-5350-23;
termination-prefix=S3/DS1-6/; termination-port-start=1; termination-port-end=31;

add trunk cic-start=1; cic-end=31; tgn-id=4; mgw-id=va-5350-23;
termination-prefix=S3/DS1-7/; termination-port-start=1; termination-port-end=31;

#
# SS7 routes, route guides and destinations
#
add route id=dpc1-route; tg_selection=RR; tgn1_id=1;
add route id=dpc2-route; tg_selection=RR; tgn1_id=2;
add route-guide id=dpc1-rg; policy-type=ROUTE; policy-id=dpc1-route;
add route-guide id=dpc2-rg; policy-type=ROUTE; policy-id=dpc2-route;
add destination dest-id=dpc1-dest; call-type=LOCAL; route-type=ROUTE;
route-guide-id=dpc1-rg;
add destination dest-id=dpc2-dest; call-type=LOCAL; route-type=ROUTE;
route-guide-id=dpc2-rg;

# New route, route guide and destination information for OPC2
add route id=dpc1-route2; tg_selection=RR; tgn1_id=3;
add route id=dpc2-route2; tg_selection=RR; tgn1_id=4;
add route-guide id=dpc1-rg2; policy-type=ROUTE; policy-id=dpc1-route2;
add route-guide id=dpc2-rg2; policy-type=ROUTE; policy-id=dpc2-route2;
add destination dest-id=dpc1-dest2; call-type=LOCAL; route-type=ROUTE;
route-guide-id=dpc1-rg2;
add destination dest-id=dpc2-dest2; call-type=LOCAL; route-type=ROUTE;
route-guide-id=dpc2-rg2;


#####################################
# TCAP/SUA Provisioning for LNP
#####################################

add sccp-nw id=1;NET_IND=NATIONAL;SUB_SVC=NATIONAL;HOP_COUNT=3;

add subsystem-profile id=SSN_LNP1;platform_id=FSAIN205;

add subsystem id=SSN_LNP1; OPC-ID=opc1; LOCAL-SSN=247;REMOTE_SSN=247;
sccp-nw-id=1;SCCP_VERSION=ANS92; TCAP_VERSION=ANS92; APPLICATION_VERSION=AIN01;

# New subsystem ID for OPC2
add subsystem id=SSN_LNP2; OPC-ID=opc2; LOCAL-SSN=247;REMOTE_SSN=247;
sccp-nw-id=1;SCCP_VERSION=ANS92; TCAP_VERSION=ANS92; APPLICATION_VERSION=AIN01;

add routing-key id=itp-grp-rk2; opc-id=opc1; sg-grp-id=sg-grp1; si=sccp; ssn-id=SSN_LNP1;
platform-id=FSAIN205; rc=4; description=Routing Key for SUA User Adaptation layer;
```

```
# New routing-key for OPC2
add routing-key id=itp-grp-rk3; opc-id=opc2; sg-grp-id=sg-grp1; si=sccp; ssn-id=SSN_LNP1;
platform-id=FSAIN205; rc=5; description=Routing Key for SUA User Adaptation layer;

########################################
# Provisioned DPC is the STP Capabilty Pt Code
########################################
add dpc id=stp_cap_pc; point-code=1-1-22; point-code-type=ANSI_CHINA;
description=Capability Point Code of STPs

add feature fname=LNP; feature-server-id=FSAIN205; description=Local number portability;
tdp1=COLLECTED_INFORMATION; tid1=LNP_TRIGGER; ttype1=R;

add ported-office-code digit-string=301-612; in-call-agent=n;

add CA-Config type=DEFAULT-LNP-SLHR-ID; datatype=string;  value=slhr_lnp;

add slhr-profile id=slhr_lnp;

add slhr id=slhr_lnp; gtt-req=Y; tt=11; GTT_ADDR_TYPE=CDPN; GTT_ADDR=3; opc-id=opc1;
dpc-id=stp_cap_pc; ssn_id=SSN_LNP1;

# New slhr for OPC2
add slhr id=slhr_lnp1; gtt-req=Y; tt=11; GTT_ADDR_TYPE=CDPN; GTT_ADDR=3; opc-id=opc2;
dpc-id=stp_cap_pc; ssn_id=SSN_LNP1;

add sccp-route opc-id=opc1; dpc-id=stp_cap_pc; rk-id=itp-grp-rk2; ssn-id=SSN_LNP1;
description=LNP for opc1;

# New sccp-route for OPC2
add sccp-route opc-id=opc2; dpc-id=stp_cap_pc; rk-id=itp-grp-rk3; ssn-id=SSN_LNP1;
description=LNP for opc2;

add pop ID=50901; STATE=tx; COUNTRY=US; TIMEZONE=CDT; LOCAL_7D_DIALING=Y; ITP=N;
ZERO_MINUS=LEC; BLOCK_EAWOPIC=Y; CNAM_OPTION=EXT_LIDB; PIC2_REQD=N; MY_LRN=4692559999;
TREAT_IMS_ANONYMOUS=N; OPC_ID=opc1; ZERO_PLUS_LOCAL=N

# New pop for OPC2
add pop ID=50902; STATE=tx; COUNTRY=US; TIMEZONE=CDT; LOCAL_7D_DIALING=Y; ITP=N;
ZERO_MINUS=LEC; BLOCK_EAWOPIC=Y; CNAM_OPTION=EXT_LIDB; PIC2_REQD=N; MY_LRN=4692559991;
TREAT_IMS_ANONYMOUS=N; OPC_ID=opc2; ZERO_PLUS_LOCAL=N
```

Connecting with Multiple SS7 Networks via A-links

This profile (Figure 5-8) fits the customer who operates in two different service provider's networks and uses only a single point code for each of those networks. Note that OPC 1-1-1 communicates with SS7 Network 1 and OPC 2-1-1 communicates with SS7 Network 2.

Figure 5-8 Communicating with Multiple SS7 Networks via A-links



Limitations

The A-link profile requires an ITP-Group (two Cisco ITP nodes) per Cisco BTS 10200 OPC.

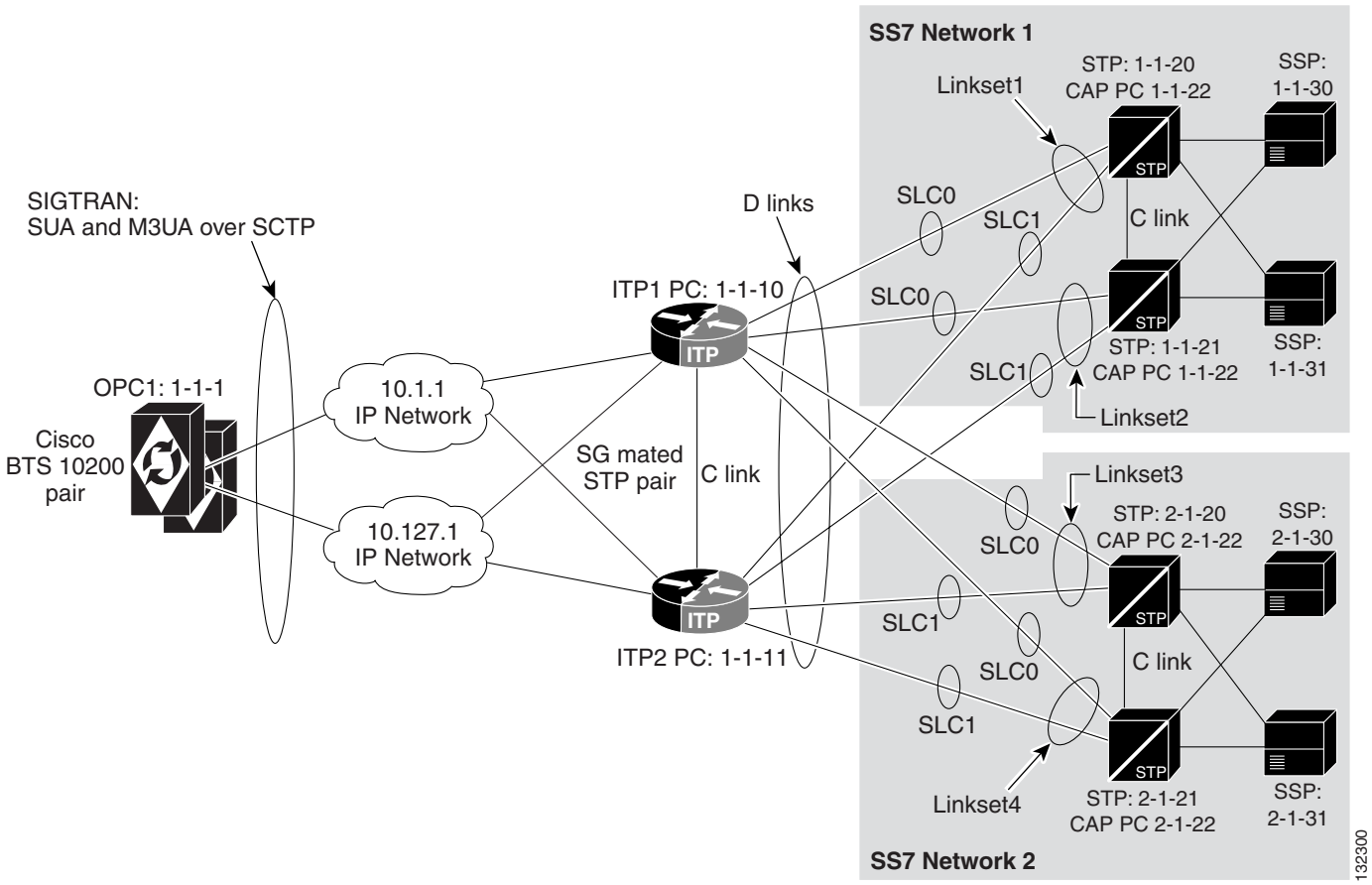
Alternate Base Profiles

A profile based on the D-link profile is also an option (see Figure 5-9). It is generally preferred over the A-link based profile if there are more than two OPCs on the Cisco BTS 10200.

ITP Configuration Information

The Cisco ITP configuration for the A-links to multiple SS7 Networks profile is essentially a doubling of the basic A-link configuration shown in the "ITP Configuration Information" section on page 5-22. ITP1 and ITP2 are configured exactly the same as in that section. The configurations for ITP3 and ITP4 are very similar, except that they have different IP address, point code, and routing key information added in the respective configuration entries to match the values shown in Figure 5-8.

Figure 5-9 Communicating to Multiple SS7 Networks via D-links



Cisco BTS 10200 Provisioning Information

The provisioning information for the A-links to multiple SS7 networks is the same as the basic A-link provisioning in the "Cisco BTS 10200 Provisioning for the Basic A-link Profile" section on page 5-28 except there is double SS7-related information. The provisioning script is as follows:

```
######################################################################
#
# CA Configuration
#
######################################################################
add ca-config type=MGCP-INIT-TERMS;value=160;datatype=integer;
add ca-config type=MGCP-INIT-DURATION;value=5;datatype=integer;
add ca-config type=MGCP-ICMP-PING-RETRANSMIT-DURATION;value=5;datatype=integer;
add ca-config type=MGCP-ICMP-PING-RETRY-COUNT;value=5;datatype=integer;
add ca-config type=MGCP-MAX-UNREACH-COUNT;value=5;datatype=integer;
add ca-config type=MGCP-MAX-FAULT-COUNT;value=5;datatype=integer;
add ca-config type=MGCP-ADM-RESP-TIME;value=300;datatype=integer;
add ca-config type=MGCP-SIG-TOS-LOWDELAY;value=Y;datatype=boolean;
add ca-config type=MGCP-SIG-TOS-PRECEDENCE;value=1;datatype=integer;
add ca-config type=MGCP-SIG-TOS-RELIABILITY;value=Y;datatype=boolean;
add ca-config type=MGCP-SIG-TOS-THROUGHPUT;value=Y;datatype=boolean;
#
# CA & FS
#
add call-agent id=CA146; tsap-addr-sidea=hrn11ca; mgw-monitoring-enabled=N;
add feature-server id=FSAIN205; tsap-addr-sidea=hrn11ca:11205; type=AIN;
```

```
#
# Sigtran components
#
add sg id=sg1; description=Signaling gateway 1;
add sg-grp id=sg-grp1; sg1-id=sg1; description=SG group 1;

add sgp id=sg1-sgp1 ; sg-id=sg1; description=SG process 1 for sg1;
add sgp id=sg1-sgp2 ; sg-id=sg1; description=SG process 2 for sg1;

add sctp-assoc-profile id=sctp-prof;

add sctp-assoc id=sg1-sgp1-sctp; sgp-id=sg1-sgp1; sctp-assoc-profile-id=sctp-prof;
platform-id=CA146; remote-port=2905; remote-tsap-addr1=10.0.1.54;
remote-tsap-addr2=10.128.1.239; dscp=AF11; ip-tos-precedence=ROUTINE;

add sctp-assoc id=sg2-sgp1-sctp; sgp-id=sg2-sgp1; sctp-assoc-profile-id=sctp-prof;
platform-id=CA146; remote-port=2905; remote-tsap-addr1=10.0.1.55;
remote-tsap-addr2=10.128.1.240; dscp=AF11; ip-tos-precedence=ROUTINE;
#
# Added Sigtran components for SS7 Network 2
#
add sg id=sg2; description=Signaling gateway 2;
add sg-grp id=sg-grp2; sg1-id=sg2; description=SG group 2;

add sgp id=sg2-sgp1 ; sg-id=sg2; description=SG process 1 for sg2;
add sgp id=sg2-sgp2 ; sg-id=sg2; description=SG process 2 for sg2;

add sctp-assoc id=sg1-sgp1-sctp; sgp-id=sg1-sgp1; sctp-assoc-profile-id=sctp-prof;
platform-id=CA146; remote-port=2905; remote-tsap-addr1=10.1.1.54;
remote-tsap-addr2=10.127.1.239; dscp=AF11; ip-tos-precedence=ROUTINE;

add sctp-assoc id=sg2-sgp1-sctp; sgp-id=sg2-sgp1; sctp-assoc-profile-id=sctp-prof;
platform-id=CA146; remote-port=2905; remote-tsap-addr1=10.1.1.55;
remote-tsap-addr2=10.127.1.240; dscp=AF11; ip-tos-precedence=ROUTINE;
#
# SS7 Related Objects
#
add user-part-variant id=ANSISS7_GR317;

add opc id=opc1; point-code=1-1-1; description=OPC1; point-code-type=ANSI_CHINA;
add dpc id=dpc1; point-code=1-1-30; description=DPC 1-1-30; point-code-type=ANSI_CHINA;
add dpc id=dpc2; point-code=1-1-31; description=DPC 1-1-31; point-code-type=ANSI_CHINA;

add routing-key id=rk1; opc-id=opc1; sg-grp-id=sg-grp1; si=ISUP; rc=1; platform-id=CA146;

add call-ctrl-route id=dpc1-route1; dpc-id=dpc1; routing-key-id=rk1; si=isup;
user-part-variant-id= ANSISS7_GR317
add call-ctrl-route id=dpc2-route1; dpc-id=dpc2; routing-key-id=rk1; si=isup;
user-part-variant-id= ANSISS7_GR317;
#
# Added SS7 components for SS7 Network 2
#
add opc id=opc2; point-code=2-1-1; description=OPC2; point-code-type=ANSI_CHINA;
add dpc id=dpc3; point-code=2-1-30; description=DPC 2-1-30; point-code-type=ANSI_CHINA;
add dpc id=dpc4; point-code=2-1-31; description=DPC 2-1-31; point-code-type=ANSI_CHINA;

add routing-key id=rk2; opc-id=opc2; sg-grp-id=sg-grp2; si=ISUP; rc=2; platform-id=CA146;

add call-ctrl-route id=dpc3-route1; dpc-id=dpc3; routing-key-id=rk2; si=isup;
user-part-variant-id= ANSISS7_GR317
add call-ctrl-route id=dpc4-route1; dpc-id=dpc4; routing-key-id=rk2; si=isup;
user-part-variant-id= ANSISS7_GR317;
```

```
#
# dial plan profile
#
add digman-profile id=pretrans;
add digman id=pretrans; rule=1; match-string=^*; replace-string=&; match-noa=any;
replace-noa=VSC;
add digman id=pretrans; rule=2; match-string=^#; replace-string=&; match-noa=any;
replace-noa=VSC;
add digman-profile id=ani_20;
add digman id=ani_20; rule=1; match-string=^20; replace-string=none;
add dial-plan-profile id=dp-1; nanp-dial-plan=Y; description=NA dial plan profile;
dnis-digman-id=pretrans; ani-digman-id=ani_20;
#
# SS7 TG
#
add ss7-ansi-tg-profile ID=ansi-tg-prof;
add trunk-grp ID=1; call_agent_id=CA146; tg_type=SS7; direction=BOTH;
tg_profile_id=ansi-tg-prof; call-ctrl-route-id=dpc1-route1; dial-plan-id=dp-1;
description=TG to DPC 1;  MGCP_PKG_TYPE=T;
add trunk-grp ID=2; call_agent_id=CA146; tg_type=SS7; direction=BOTH;
tg_profile_id=ansi-tg-prof; call-ctrl-route-id=dpc2-route1; dial-plan-id=dp-1;
description=TG to DPC 2;  MGCP_PKG_TYPE=T;
#
# Additional TG Information for SS7 Network 2
#
add trunk-grp ID=3; call_agent_id=CA146; tg_type=SS7; direction=BOTH;
tg_profile_id=ansi-tg-prof; call-ctrl-route-id=dpc3-route1; dial-plan-id=dp-1;
description=TG to DPC 3;  MGCP_PKG_TYPE=T;
add trunk-grp ID=4; call_agent_id=CA146; tg_type=SS7; direction=BOTH;
tg_profile_id=ansi-tg-prof; call-ctrl-route-id=dpc4-route1; dial-plan-id=dp-1;
description=TG to DPC 4;  MGCP_PKG_TYPE=T;
#
# MGW
#
add mgw-profile id=as5300-prof; vendor=Cisco; mgcp-hairpin-supp=n; MGCP_RSIPSTAR_SUPP=N;
MGCP_TERM_INIT_LEVEL=0; RBK_ON_CONN_SUPP=N; MGCP_VERSION=MGCP_1_0; mgcp-max2-retries=3;
fax-t38-camode-supp=Y; mgcp-keepalive-interval=60; mgcp-keepalive-retries=10;
mgcp-t-tran=400; mgcp-max1-retries=2; mgcp-t-longtran=5; mgcp-default-pkg=NONE;
MGCP_3WAY_HSHAKE_SUPP=N; mgw_type=AS5300; PC_MPTIME_SUPP=N; MGCP_VERSION=MGCP_1_0;
PC_MPTIME_SUPP=N;

add mgw id=va-5350-23; tsap-addr=va-5350-23.hrndevtest.cisco.com; call-agent-id=CA146;
mgw-profile-id=as5300-prof; type=TGW;
#
# Additional MGW Information for SS7 Network 2
#
add mgw id=va-5350-24; tsap-addr=va-5350-24.hrndevtest.cisco.com; call-agent-id=CA146;
mgw-profile-id=as5300-prof; type=TGW;
#
# SS7 terminations and trunks
#
add termination prefix=S3/DS1-4/; port-start=1; port-end=31; type=trunk;
mgw-id=va-5350-23;
add termination prefix=S3/DS1-5/; port-start=1; port-end=31; type=trunk;
mgw-id=va-5350-23;
add trunk cic-start=1; cic-end=31; tgn-id=1; mgw-id=va-5350-23;
termination-prefix=S3/DS1-4/; termination-port-start=1; termination-port-end=31;
add trunk cic-start=1; cic-end=31; tgn-id=2; mgw-id=va-5350-23;
termination-prefix=S3/DS1-5/; termination-port-start=1; termination-port-end=31;
#
# Additional SS7 termination and trunk info for SS7 Network 2
#
add termination prefix=S3/DS1-4/; port-start=1; port-end=31; type=trunk;
mgw-id=va-5350-24;
```

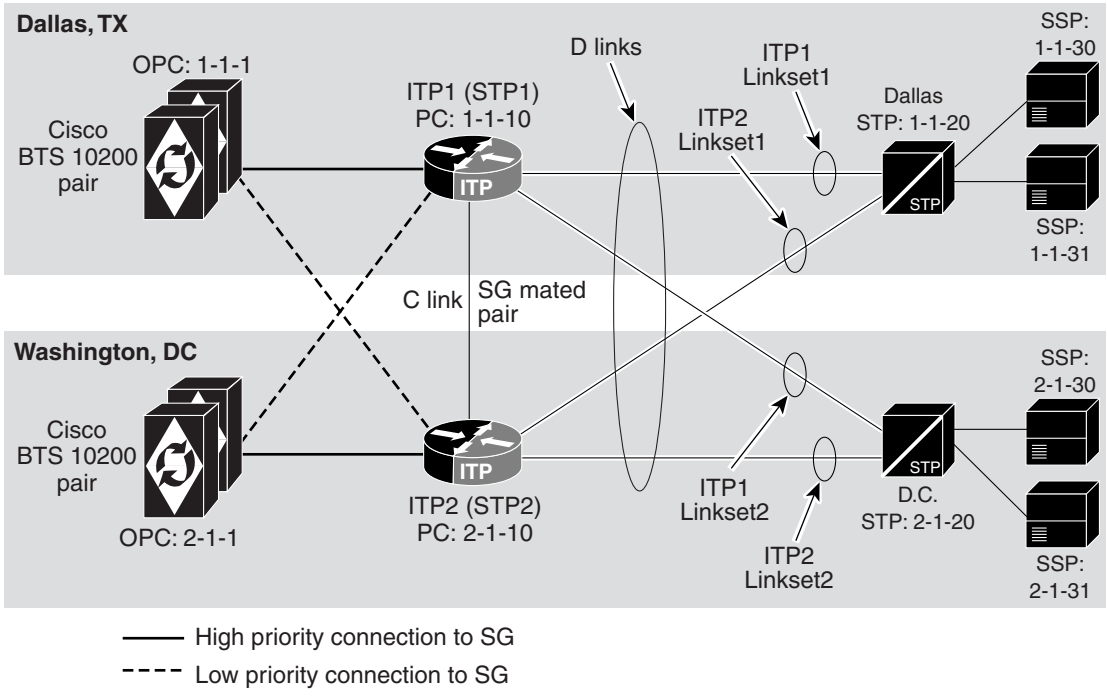
```
add termination prefix=S3/DS1-5/; port-start=1; port-end=31; type=trunk;
mgw-id=va-5350-24;
add trunk cic-start=1; cic-end=31; tgn-id=3; mgw-id=va-5350-24;
termination-prefix=S3/DS1-4/; termination-port-start=1; termination-port-end=31;
add trunk cic-start=1; cic-end=31; tgn-id=4; mgw-id=va-5350-24;
termination-prefix=S3/DS1-5/; termination-port-start=1; termination-port-end=31;
#
# SS7 routes, route guides and destinations
#
add route id=dpc1-route; tg_selection=RR; tgn1_id=1;
add route id=dpc2-route; tg_selection=RR; tgn1_id=2;
add route-guide id=dpc1-rg; policy-type=ROUTE; policy-id=dpc1-route;
add route-guide id=dpc2-rg; policy-type=ROUTE; policy-id=dpc2-route;
add destination dest-id=dpc1-dest; call-type=LOCAL; route-type=ROUTE;
route-guide-id=dpc1-rg;
add destination dest-id=dpc2-dest; call-type=LOCAL; route-type=ROUTE;
route-guide-id=dpc2-rg;
#
# Additional SS7 routes, route guides and destinations for SS7 Network 2
#
add route id=dpc3-route; tg_selection=RR; tgn1_id=3;
add route id=dpc4-route; tg_selection=RR; tgn1_id=4;
add route-guide id=dpc3-rg; policy-type=ROUTE; policy-id=dpc3-route;
add route-guide id=dpc4-rg; policy-type=ROUTE; policy-id=dpc4-route;
add destination dest-id=dpc3-dest; call-type=LOCAL; route-type=ROUTE;
route-guide-id=dpc3-rg;
add destination dest-id=dpc4-dest; call-type=LOCAL; route-type=ROUTE;
route-guide-id=dpc4-rg;

#####################################
#   TCAP/SUA Provisioning for LNP
#####################################
add sccp-nw id=1;NET_IND=NATIONAL;SUB_SVC=NATIONAL;HOP_COUNT=3;

add subsystem-profile id=SSN_LNP1;platform_id=FSAIN205;

add subsystem id=SSN_LNP1; OPC-ID=opc1; LOCAL-SSN=247;REMOTE_SSN=247;
sccp-nw-id=1;SCCP_VERSION=ANS92; TCAP_VERSION=ANS92; APPLICATION_VERSION=AIN01;

add routing-key id=itp-grp-rk2; opc-id=opc1; sg-grp-id=sg-grp1; si=sccp; ssn-id=SSN_LNP1;
platform-id=FSAIN205; rc=4; description=Routing Key for SUA User Adaptation layer;

########################################
# Provisioned DPC is the STP Capabilty Pt Code
########################################
add dpc id=stp_cap_pc; point-code=1-1-22; point-code-type=ANSI_CHINA;
description=Capability Point Code of STPs

add feature fname=LNP; feature-server-id=FSAIN205; description=Local number portability;
tdp1=COLLECTED_INFORMATION; tid1=LNP_TRIGGER; ttype1=R;

add ported-office-code digit-string=301-612; in-call-agent=n;

add CA-Config type=DEFAULT-LNP-SLHR-ID; datatype=string;  value=slhr_lnp;

add slhr-profile id=slhr_lnp;
add slhr id=slhr_lnp; gtt-req=Y; tt=11; GTT_ADDR_TYPE=CDPN; GTT_ADDR=3; opc-id=opc1;
dpc-id=stp_cap_pc; ssn_id=SSN_LNP1;
add sccp-route opc-id=opc1; dpc-id=stp_cap_pc; rk-id=itp-grp-rk2; ssn-id=SSN_LNP1;
description=LNP for opc1;

add pop ID=50901; STATE=tx; COUNTRY=US; TIMEZONE=CDT; LOCAL_7D_DIALING=Y; ITP=N;
ZERO_MINUS=LEC; BLOCK_EAWOPIC=Y; CNAM_OPTION=EXT_LIDB; PIC2_REQD=N; MY_LRN=4692559999;
TREAT_IMS_ANONYMOUS=N; OPC_ID=opc1; ZERO_PLUS_LOCAL=N
```

```
############################################################
#   Additional TCAP/SUA Provisioning for the SS7 Network 2
############################################################

add subsystem id=SSN_LNP2; OPC-ID=opc2; LOCAL-SSN=247; REMOTE_SSN=247; sccp-nw-id=1;
SCCP_VERSION=ANS92; TCAP_VERSION=ANS92; APPLICATION_VERSION=AIN01;

add routing-key id=itp-grp-rk3; opc-id=opc2; sg-grp-id=sg-grp2; si=sccp; ssn-id=SSN_LNP2;
platform-id=FSAIN205; rc=5; description=Routing Key for SUA User Adaptation layer;

add dpc id=stp_cap_pc_net2; point-code=2-1-22; point-code-type=ANSI_CHINA;
description=Capability Point Code of STPs in SS7 Network 2

add slhr id=slhr_lnp; gtt-req=Y; tt=11; GTT_ADDR_TYPE=CDPN; GTT_ADDR=3; opc-id=opc2;
dpc-id=stp_cap_pc_net2; ssn_id=SSN_LNP2;

add sccp-route opc-id=opc2; dpc-id=stp_cap_pc_net2; rk-id=itp-grp-rk3; ssn-id=SSN_LNP2;
description=LNP for opc2;

add pop ID=50901; STATE=tx; COUNTRY=US; TIMEZONE=CDT; LOCAL_7D_DIALING=Y; ITP=N;
ZERO_MINUS=LEC; BLOCK_EAWOPIC=Y; CNAM_OPTION=EXT_LIDB; PIC2_REQD=N; MY_LRN=4692559990;
TREAT_IMS_ANONYMOUS=N; OPC_ID=opc2; ZERO_PLUS_LOCAL=N
```

Geographically Distributed D-link Profile with SG Routing Priority

This profile fits the customer who operates two different geographically separated telephony networks using geographically separated Cisco BTS 10200 and Cisco ITP nodes. In Figure 5-10, BTS1 and ITP1 are in Dallas, Texas while BTS2 and ITP2 are in Washington D.C.

Figure 5-10 Geographically Separated D-Link Profile



Usage

The topology between ITPs and STPs forms an SS7 STP quad. The SG mated pair could be connected to an STP service provider's STP mated pair or the gateway STPs provided by any of the local service providers. The Cisco ITP pair can either be colocated with Cisco BTS 10200 in the customer's network or colocated with an STP pair in the service provider's network.

One key component of this profile is the use of SG priority routing (that is, having the ability to choose which SG in the SG-Group to give priority to when sending toward your destinations). In this profile, BTS1 primarily sends toward the DPCs (SSPs) in the Dallas network via ITP1 and it only routes through ITP2 for these endpoints at a lower priority. This is useful for cost reduction if, for instance, BTS1 has a POP in Dallas and BTS2 has a POP in Washington D.C. Note that Figure 5-10 only shows one STP in each of the respective cities. There would most likely be two network STPs for each of the two cities.

Alternate Base Profiles

There are no alternate profiles because A-link profiles use ITP-Groups instead of SG-Pairs and ITP-Groups cannot be geographically separated.

ITP Configuration Information

The Cisco ITP configuration here should be similar to the one in the "ITP Configuration Information" section on page 5-31, except for two points: 1) in Figure 5-10 only one STP is shown as a route toward each SSP (in reality, there would probably be two), 2) the routes through STP1 and STP2 lead toward different endpoints. The following is the configuration for the SS7 linksets and routes:

```
#
# SS7 Linkset definitions. Note: the number after 'link' represents SLC
#
cs7 linkset lset1chn 1.1.20
 link 0 Serial0/0:0
!
cs7 linkset lset2chn 2.1.20
 link 0 Serial0/1:0

#
# SS7 Route definitions
#
cs7 route-table system
 update route 1.1.30 255.255.255 linkset lset1chn priority 1
 update route 1.1.31 255.255.255 linkset lset1chn priority 1
 update route 2.1.30 255.255.255 linkset lset2chn priority 1
 update route 2.1.31 255.255.255 linkset lset2chn priority 1
```

Cisco BTS 10200 Provisioning Information

The key area that stands out in the Cisco BTS 10200 provisioning script is that each Cisco BTS 10200 will assign one of the SGs of the SG-Group as a priority 1 SG route while the other Cisco BTS 10200 will assign it as a priority 2 route. For instance, in the BTS1 provisioning script, SG1 will have a priority of 1 and SG2 will have a priority of 2. Likewise, in the BTS2 provisioning script, SG2 will have a priority of 1 and SG1 will have a priority of 2. The following is a provisioning example for configuring SG priorities.

BTS1 Provisioning

```
#
# SG configuration for BTS1. Note how the priority is provisioned opposite
# of what will be done on BTS2 (as shown in the next subsection).
#
add sg id=sg1; description=Signaling gateway 1 of SG GRP 1; priority 1
add sg id=sg2; description=Signaling gateway 2 of SG GRP 1; priority 2

#
# SG-GRP configuration for BTS1
#
add sg-grp id=sg-grp1; sg1-id=sg1; sg2-id=sg2 description=SG group 1;
```

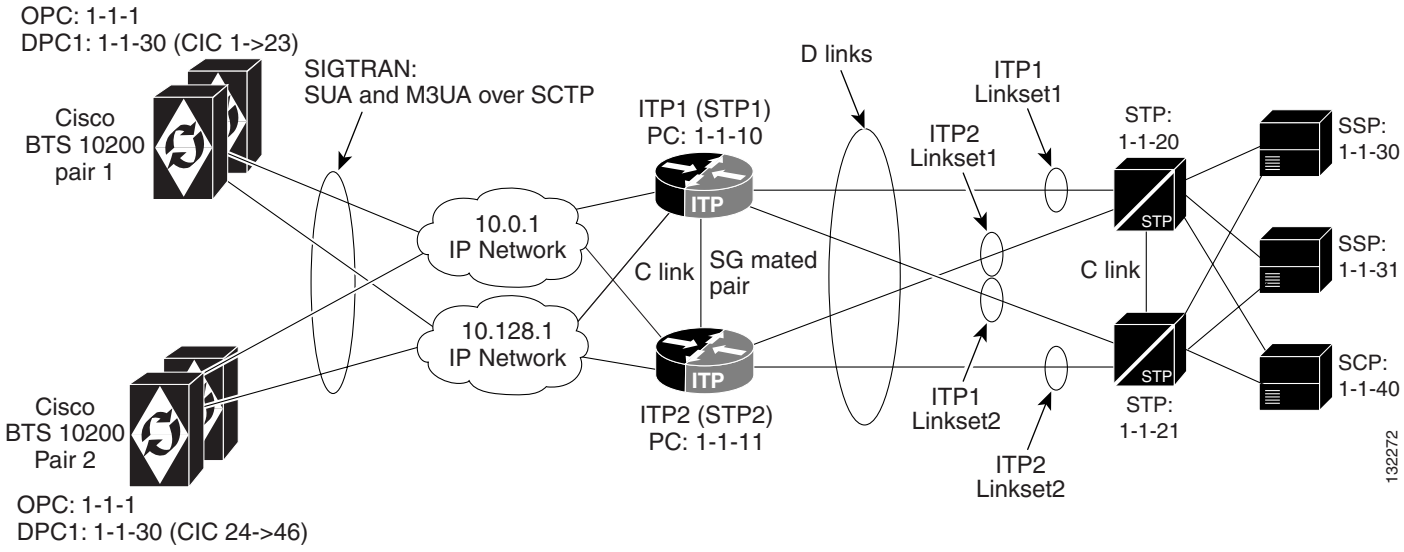
BTS2 Provisioning

```
#
# SG configuration for BTS2. Note how the priority is provisioned opposite
# of what it was for BTS1.
#
add sg id=sg1; description=Signaling gateway 1 of SG GRP 1; priority 2
add sg id=sg2; description=Signaling gateway 2 of SG GRP 1; priority 1

#
# SG-GRP configuration for BTS2
#
add sg-grp id=sg-grp1; sg1-id=sg1; sg2-id=sg2 description=SG group 1;
```

Multiple Cisco BTS 10200 Nodes Sharing the Same OPC

This profile is generally used whenever a customer wants to share a single OPC among multiple Cisco BTS 10200 nodes.

Figure 5-11 Multiple Cisco BTS 10200 Nodes Sharing One OPC (with CIC-Based Routing)



Usage

When this profile is used, traffic is divided in one of two ways:

- Traffic can be split between the Cisco BTS 10200 nodes based on a per Call Control Route basis. In this case, the Cisco BTS 10200 nodes will not be provisioned with the same DPC. This means that only one of the Cisco BTS 10200 nodes will send traffic to and receive traffic from the associated DPC in the service provider network.
- Traffic can also be split on a per Call Control Route/CIC range basis. In this case, the same DPC (and Call Control Route) can be provisioned on multiple Cisco BTS 10200 nodes, but the associated trunk group will be provisioned with a CIC range that differs on each Cisco BTS 10200 node.

Limitations

- Multiple Cisco BTS 10200 nodes sharing a single point code is only valid for ISUP. If TCAP queries are needed, then a separate TCAP OPC will be needed for each Cisco BTS 10200.
- If a provisioned DPC on one Cisco BTS 10200 is also provisioned on any other Cisco BTS 10200, then the load must be divided between the Cisco BTS 10200 nodes based on CIC range.
- When provisioning call control routes on the Cisco BTS 10200, it is not allowable to provision two different call control routes that have the same routing key and DPC information.

Alternate Profiles

This feature is valid for D-link, A-link, F-link and E-link topologies. For the A/F/E link topologies, the point code of the ITP-Group is shared by the Cisco BTS 10200.

ITP Configuration Information

The Cisco ITP configuration information is essentially the same as the basic D-link configuration provided in the "ITP Configuration Information" section on page 5-10; however, this section provides an example AS and ASP configuration given only for M3UA. For a default D-link configuration that includes SUA, see the "ITP Configuration Information" section on page 5-10.

The main difference is there is extra ASP configuration information for communicating to the second CA (BTS2). Also, there is extra information in the AS configuration section for routing to each of the Call Agents (based on CIC range).

The following example shows the ASP and AS configuration elements for ITP1. Note that ITP2 will have the same ASP and AS configuration information that is shown below for ITP1.

For additional Cisco ITP configuration information, see the *Cisco ITP Configuration Guide and Command Reference* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/wireless/moblwrls/itp/25sw/itp25swi.pdf

ITP1 Information

```
## ASP configuration for BTS1

cs7 asp PRI_ISUP_BTS1 11146 2905 m3ua
 remote-ip 10.0.1.5
 remote-ip 10.128.1.2

cs7 asp SEC_ISUP_BTS1 11146 2905 m3ua
 remote-ip 10.0.1.6
 remote-ip 10.128.1.3
```

```
## ASP configuration for BTS2

cs7 asp PRI_ISUP_BTS2 11146 2905 m3ua
 remote-ip 10.0.1.7
 remote-ip 10.128.1.4

cs7 asp SEC_ISUP_BTS2 11146 2905 m3ua
 remote-ip 10.0.1.8
 remote-ip 10.128.1.5

## AS configuration for BTS1
#
# Note: In the following configuration the routing context entries are as follows:
# routing context = 1, DPC(BTS OPC)=1.1.1, opc=1.1.30, mask is 255.255.255,
# service indicator=ISUP, CIC range=1->23
#
# Configuring network-appearance 1 is required for release 4.4, but will not be required
# in release 4.5 and beyond.

cs7 as ISUP_BTS1 m3ua
 routing-key 1 1.1.1 opc 1.1.30 255.255.255 si isup cic 1 23
 asp PRI_ISUP_BTS1
 asp SEC_ISUP_BTS1
 traffic-mode override
 network-appearance 1

## AS configuration for BTS2
# Note that the CIC range changes to 24->46 for sending messages to BTS2
cs7 as ISUP_BTS1 m3ua
 routing-key 2 1.1.1 opc 1.1.30 255.255.255 si isup cic 24 46
 asp PRI_ISUP_BTS2
 asp SEC_ISUP_BTS2
 traffic-mode override
 network-appearance 1

## Note that additional AS configurations will be needed for other DPCs (such as 1-1-31).
```

BTS1 Provisioning for Routing Key/CIC-Based Routing

Unlike the Cisco ITP, the Cisco BTS 10200 does not configure CIC ranges within the routing key. Instead, the CIC ranges on the Cisco BTS 10200 are provisioned as part of the trunk object.

```
add opc id=opc1; point-code=1-1-1; point-code-type=ANSI_CHINA;
add dpc id=dpc1; point-code=1-1-30; point-code-type=ANSI_CHINA;
add dpc id=dpc2; point-code=1-1-31; point-code-type=ANSI_CHINA;
add sg id=sg1; priority=1;
add sg id=sg2; priority=1;
add sg-grp id=sg-grp1; sg1-id=sg1; sg2-id=sg2;
add sgp id=sg1-sgp1; sg-id=sg1;
add sgp id=sg2-sgp2; sg-id=sg2;
add sctp-assoc-profile id=sctp-prof1;

add sctp-assoc id=sg1-sgp1-sctp; sgp-id=sgp1; sctp-assoc-profile-id=sctp-prof1;
platform-id=CA146; remote-port=2905; remote-tsap-addr1=10.89.225.235;
remote-tsap-addr2=10.89.226.235; dscp=AF11; ip-tos-precedence=ROUTINE;

add sctp-assoc id=sg2-sgp2-sctp; sgp-id=sgp2; sctp-assoc-profile-id=sctp-prof1;
platform-id=CA146; remote-port=2905; remote-tsap-addr1=10.89.225.236;
remote-tsap-addr2=10.89.226.236; dscp=AF11; ip-tos-precedence=ROUTINE;

add user-part-variant id=ANSISS7_GR317;
```

```
#-------------------------------------------------------------------------------------
# NOTE THAT RC VALUE IN BTS CONFIG MATCHES RC VALUE IN ITP CONFIG
#-------------------------------------------------------------------------------------
add routing-key id=rk1; opc-id=opc1; sg-grp-id=sg-grp1; si=ISUP; rc=1; platform-id=CA146;

add call-ctrl-route id=dpc1-route; dpc-id=dpc1; routing-key-id=rk1; si=ISUP;
user-part-variant-id=ANSISS7_GR317;
add call-ctrl-route id=dpc2-route; dpc-id=dpc2; routing-key-id=rk2; si=ISUP;
user-part-variant-id=ANSISS7_GR317;
add mgw-profile id=as5300-prof; mgw-type=AS5300; mgcp-version=MGCP_1_0;
add mgw id=as5300-1; mgw-profile-id=as5300-prof; call-agent-id=CA146;
tsap-addr=as5300-1.cisco.com; type=TGW;
add termination prefix=S1/DS1-0/; port-start=1; port-end=23 or 31; type=trunk;
mgw-id=as5300-1;

add ss7-ansi-tg-profile id=ss7-prof1;
add trunk-grp id=1; call-agent-id=CA146; tg-type=SS7; tg-profile=ss7-prof1;
call-ctrl-route-id=dpc1-route;

#-------------------------------------------------------------------------------------
# NOTE THAT THE CIC RANGE IN THE BTS TRUNK MATCHES THE ONE IN THE ITP AS
# RKEY CONFIGURATION.
#
# Also note that the CIC range is not defined in the routing-key for the BTS.
# It is defined as part of the trunk object. It is however possible to define
# the DPC in this routing key, but it is not necessary (it was not done here).
#-------------------------------------------------------------------------------------
add trunk cic-start=1; cic-end=23; type=trunk; mgw-id=as5300-1;
termination-prefix=S1/DS1-0/; tgn-id=1; termination-port-start=1; termination-port-end=23;

add route id=dpc1-route; tg-selection=RR; tgn1-id=1;
add route-guide id=dpc1-rg; policy-type=ROUTE; policy-id=dpc1-route;
add destination id=dpc1-dest; route-type=ROUTE; route-guide-id=dpc1-rg;
```

BTS2 Provisioning for Routing Key/CIC-Based Routing

```
add opc id=opc1; point-code=3-10-3; point-code-type=ANSI_CHINA;
add dpc id=dpc1; point-code=3-50-3; point-code-type=ANSI_CHINA;
add dpc id=dpc2; point-code=3-51-3; point-code-type=ANSI_CHINA;
add sg id=sg1; priority=1;
add sg id=sg2; priority=1;
add sg-grp id=sg-grp1; sg1-id=sg1; sg2-id=sg2;
add sgp id=sgp1; sg-id=sg1;
add sgp id=sgp2; sg-id=sg2;
add sctp-assoc-profile id=sctp-prof1;

add sctp-assoc id=ca-sgp1-sctp; sgp-id=sgp1; sctp-assoc-profile-id=sctp-prof1;
platform-id=CA147; remote-port=2905; remote-tsap-addr1=10.89.225.235;
remote-tsap-addr2=10.89.226.235; dscp=AF11; ip-tos-precedence=ROUTINE;

 add sctp-assoc id=ca-sgp2-sctp; sgp-id=sgp2; sctp-assoc-profile-id=sctp-prof1;
platform-id=CA147; remote-port=2905; remote-tsap-addr1=10.89.225.236;
remote-tsap-addr2=10.89.226.236; dscp=AF11; ip-tos-precedence=ROUTINE;

add user-part-variant id=ANSISS7_GR317;

#-------------------------------------------------------------------------------------
# NOTE THAT RC VALUE IN BTS CONFIG MATCHES RC VALUE IN ITP CONFIG
#
# Also note that the CIC range is not defined in the routing-key for the BTS.
# It is defined as part of the trunk object. It is however possible to define
# the DPC in this routing key, but it is not necessary (it was not done here).
#-------------------------------------------------------------------------------------
```

```
add routing-key id=rk3; opc-id=opc1; sg-grp-id=sg-grp1; si=ISUP; rc=2; platform-id=CA146;

add call-ctrl-route id=dpc1-route; dpc-id=dpc1; routing-key-id=rk3; si=ISUP;
user-part-variant-id=ANSISS7_GR317;
add call-ctrl-route id=dpc2-route; dpc-id=dpc2; routing-key-id=rk4; si=ISUP;
user-part-variant-id=ANSISS7_GR317;
add mgw-profile id=as5300-prof; mgw-type=AS5300; mgcp-version=MGCP_1_0;
add mgw id=as5300-1; mgw-profile-id=as5300-prof; call-agent-id=CA146;
tsap-addr=as5300-1.cisco.com; type=TGW;
add termination prefix=S1/DS1-0/; port-start=1; port-end=23 ; type=trunk; mgw-id=as5300-2;
add ss7-ansi-tg-profile id=ss7-prof1;

add trunk-grp id=1; call-agent-id=CA147; tg-type=SS7; tg-profile=ss7-prof1;
call-ctrl-route-id=dpc1-route;

#-------------------------------------------------------------------------------------
# NOTE THAT THE CIC RANGE IN THE BTS TRUNK MATCHES THE ONE IN THE
# ITP AS RKEY CONFIGURATION
#-------------------------------------------------------------------------------------

add trunk cic-start=24; cic-end=46; type=trunk; mgw-id=as5300-2;
termination-prefix=S1/DS1-0/; tgn-id=1; termination-port-start=1; termination-port-end=23;

add route id=dpc1-route; tg-selection=RR; tgn1-id=1;
add route-guide id=dpc1-rg; policy-type=ROUTE; policy-id=dpc1-route;
add destination id=dpc1-dest; route-type=ROUTE; route-guide-id=dpc1-rg;
```

Configuring the Cisco 10000 ESR

Configuring the Cisco 10000 ESR is like configuring any other Cisco IOS router with the exception of QoS. QoS must be used on all voice and data egress interfaces on this router. Because voice and data travel across the same interfaces, the MQC must be used to define service policies on those interfaces. Refer to the configuration below for examples on how to define the service policies.

The class map example in this section defines two traffic classes for voice signaling, voice bearer, and telnet traffic. There are a couple of approaches that can be used: one is to trust incoming traffic that has been marked at the edge and use the TOS/DSCP values to queue traffic that traverses the network and classify it according to that value. If the network is private, marking the traffic at the edge of the network and trusting the DSCP value in the distribution and the core is the most straightforward way to manage QoS in the network.

However, in this example the DSCP value of the incoming traffic is not trusted. TCP or UDP port numbers are used to identify the traffic and classify it accordingly.

```
class-map match-all voice-signaling
description Match MGCP Signaling and Backhaul
!< Access list identifying signaling traffic. For ACL example refer to 6509 configuration
section >
  match access-group 122
class-map match-all voice-rtp
description Match Voice Real-Time Transport Protocol
!< Access list identifying RTP bearer traffic. For ACL example refer to 6509 configuration
section >
  match access-group 121
class-map match-all gold-data
!< Access list identifying telnet traffic. For ACL example refer to 6509 configuration
section >
  match access-group 123
```

Depending on the service offering of the carrier, a policy map or a group of policy maps will have to be designed. In the following example, the carrier is offering service with a 16-port FXS IAD as well as a T1 IAD. Each will support up to 16 and 24 voice calls respectively. In addition, if we assume voice compression using the G.726-32k codec, each call will use ~51 kbps of bandwidth including L2 overhead. Connectivity between the 10k and each IAD is a full T1.

```
policy-map voice-16fxs
< RTP traffic>
  class voice-rtp
   set ip dscp 46
< This traffic is assigned to the strict priority queue (LLQ) >
priority
< The average kpbs assigned in the police statement is based on (51 kbps * 16). Given the
nature of voice traffic in that it is not bursty the bc and be values should not come into
play. They are specified here to maintain design consistency and are in accordance with
the formula (cir * 1byte / 8bits * 1 second). >
    police 816000 102000 102000 conform-action transmit exceed-action drop violate-action
drop
< Signaling traffic >
class voice-signaling
< 2500 bps is allocated for signaling traffic per call. >
    police 40000 5000 5000 conform-action transmit exceed-action drop violate-action drop
   set ip dscp 26
  class gold-data
   set ip dscp 10
< 32kbps is allocated for telnet traffic >
    police 32000 4000 4000 conform-action transmit exceed-action drop violate-action drop
< all other traffic is marked to DSCP 0 and can use available bandwidth. >
  class class-default
   set ip dscp 0
…
< This policy map is the same concept as the voice-16fxs policy map above, but configured
to accommodate 24 simultaneous voice calls. >
policy-map voice-customer-t1
  class voice-rtp
   set ip dscp 46
 priority
    police 1224000 153000 153000 conform-action transmit exceed-action drop violate-action
drop
  class voice-signaling
   set ip dscp 26
< Note that the cir value in the police statement can only be specified in 8,000 bps
increments therefore 2500 bps * 24 = 60000 bps get rounded to 64000. >
    police 64000 8000 8000 conform-action transmit exceed-action drop violate-action drop
  class gold-data
   set ip dscp 10
    police 32000 4000 4000 conform-action transmit exceed-action drop violate-action drop
  class class-default
    random-detect precedence-based
   set ip dscp 0

interface Serial1/0/0/7:0
 ip address 10.19.1.5 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip directed-broadcast
 no ip proxy-arp
 encapsulation ppp
 load-interval 30
< PPP authentication provides protection against customer connecting their own CPE to the
network. >
 ppp authentication chap
 ppp chap hostname cisco-10k
```

```
< The service policy defined above is applied to the T1 interface in the outbound
direction. >
 service-policy output voice-16fxs
```

For additional information on configuration of QoS on the Cisco 10000 router as well as other configuration topics, refer to the following links:

- *Cisco 10000 Series Router Quality of Service Configuration Guide*
  http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/config/qos/index.htm
- Cisco 10000 series routers http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/index.htm
- Cisco IOS Release 12.0
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/index.htm

Configuring the Cisco PIX Firewall

In the following configuration, the Cisco PIX Firewall is used as a control point for access from the untrusted network to the trusted network which contains the Cisco BTS 10200. The intent was to use the Cisco PIX Firewall protocol fixup features to open pinholes in the firewall for voice RTP traffic.

```
fixup protocol mgcp 2427
fixup protocol mgcp 2428
fixup protocol mgcp 2727
fixup protocol mgcp 2728
```

Due to limitations in the Cisco PIX Firewall software, the fixup feature did not work. Therefore, an access list was created to allow RTP traffic inbound through the firewall. Below are excerpts from the Cisco PIX Firewall configuration that identify the ports that need to be opened to allow communication between the Cisco BTS 10200, gateways, and IADs. Not all ports will be required depending on the design of the network. For example, if the announcement server and unified messaging platforms were located outside the firewall, there would be no need for RTP traffic to traverse the firewall.

```
< For subnets that contain IADs and gateways MGCP ports must be opened to allow
communications with the BTS. >
access-list from-outside permit udp 10.120.1.0 255.255.255.0 10.130.1.4 255.255.255.254
range 2727 2728
…
access-list from-outside permit udp 10.120.1.0 255.255.255.0 10.130.1.4 255.255.255.254
range 2427 2428
< For subnets that contain IADs and gateways that support PRI, singnaling ports for RUDP
must be opened up to allow the backhaul of ISDN signaling to the call agent. >
access-list from-outside permit udp 10.120.1.0 255.255.225.0 range 5555 5556 10.130.1.4
255.255.255.254 range 5555 5556
< For subnets that contain IADs and gateways RTP ports must be opened to allow
communications with the announcement server and unified messaging platform. >
access-list from-outside permit udp 10.120.1.0 255.255.255.0 range 16384 32767 any range
16384 32767
< Ports must be opened for DNS >
access-list from-outside permit udp 10.0.0.0 255.0.0.0 host 10.130.4.2 eq domain
< Ports must be opened for Syslog >
access-list from-outside permit udp 10.0.0.0 255.0.0.0 10.130.7.0 255.255.255.0 eq syslog
< Ports must be opened for Syslog >
access-list from-outside permit udp 10.0.0.0 255.0.0.0 any eq tftp
< Ports must be opened for Ping >
access-list from-outside permit icmp any any echo
access-list from-outside permit icmp any any echo-reply
 < Ports must be opened for NTP >
access-list from-outside permit udp 10.0.0.0 255.0.0.0 10.130.7.18 255.255.255.0 eq ntp
< Ports must be opened for SNMP >
```

```
access-list from-outside permit tcp 10.0.0.0 255.0.0.0 10.130.7.0 255.255.255.0 range 161
162
access-list from-outside permit udp 10.0.0.0 255.0.0.0 10.130.7.0 255.255.255.0 range snmp
snmptrap
< If using the CNS Configuration Engine for automated provisioning, port must be opened to
allow the agent that resides on the IOS device to communicate with the configuration
server. >
access-list from-outside permit tcp 10.120.1.0 255.255.225.0 host 10.130.7.13 eq 11011
access-list from-outside permit tcp 10.120.1.0 255.255.225.0 host 10.130.7.13 eq www
```

For additional information on configuring the Cisco PIX Firewall, see the Cisco PIX Firewall Version 6.3 documentation at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/v_63/index.htm.

Configuring the Trunking Gateway

The Cisco BLISS for T1 Solution Release 4.0 provides two options for the trunking gateway component. One option is to use the Cisco MGX 8880 with the VISM-PR voice card; the other option is to use the Cisco AS5850. This section does not cover the configuration of the MGX/VISM—it is well documented in the *Cisco VoIP Switching Configuration Guide* at the following URL:

http://wwwin.cisco.com/rtg/ccmsbu/products/vism_pr/index.shtml#white.

When configuring the MGX, each VISM is essentially a standalone gateway and must be configured individually. Also, we recommend using the active-active configuration with the RPM-XF to provide faster failover if one of the RPM-XF line cards fails.

For additional information on configuring the Cisco MGX media gateway, see the following documentation:

- Release 5 Software Documentation for the MGX
  http://www.cisco.com/univercd/cc/td/doc/product/wanbu/mgx8880/rel5/index.htm
- Voice Interworking Service Module Release 3.2
  http://www.cisco.com/univercd/cc/td/doc/product/wanbu/mgx8850/vism32/index.htm
- RPM-XF Documentation
  http://www.cisco.com/univercd/cc/td/doc/product/wanbu/8850px45/rel5/rpm/index.htm

Configuring the Cisco AS5850

The Cisco AS5850 is a Cisco IOS gateway which is configured the same way as an IOS-based router in terms of IP addressing and QoS parmeters. The "Cisco AS5850 BTS Configuration" section on page 5-56 provides configuration parameters that allow the Cisco AS5850 to communitcate with the Cisco BTS 10200 Call Agent.

```
< define domain name and domain name server for BLISS solution. Note that the hostname
defined for the MGW must match the hostname used in the BTS configuration >
hostname c-58-240
ip domain name site1.cactus2.cisco.com
ip name-server 10.16.66.22

controller T3 12/0
 framing m23
 clock source line
 cablelength 100
 t1 1-28 controller
```

```
!
controller T1 12/0:1
 framing esf
 ds0-group 0 timeslots 1-24 type none service mgcp
…
controller T1 12/0:28
 framing esf
 ds0-group 0 timeslots 1-24 type none service mgcp
…
voice-port 12/0:1:0
…
voice-port 12/0:28:0
!
< This section enables MGCP gateway functionality. In this section we specify the Call
Agent, MGCP version and the MGCP packages that the gateway will have to support. Since
this is a trunking gateway it will support features for CAS and SS7 trunks. >
mgcp
mgcp call-agent mga-sysCA146.site1.cactus2.cisco.com service-type mgcp version 1.0
mgcp modem passthrough voip mode nse
mgcp sgcp disconnect notify
mgcp quarantine mode process loop
mgcp package-capability dtmf-package
mgcp package-capability mf-package
mgcp package-capability rtp-package
mgcp default-package ms-package
mgcp tse payload 105
no mgcp timer receive-rtcp
mgcp fax t38 nsf 000000
mgcp fax t38 gateway force
mgcp rtp payload cisco-pcm-switch-over-ulaw 126
!
mgcp profile default
 description This is an mgcp profile
 timeout tsmax 100
 max2 retries 5
 endpoint naming t3
!
< For each voice port that will be under MGCP control you specify the application as
mgcpapp and specify the voice port. >
dial-peer voice 1201 pots
 application mgcpapp
 port 12/0:1:0
…
dial-peer voice 1228 pots
 application mgcpapp
 port 12/0:28:0
```

Cisco AS5850 BTS Configuration

This configuration assumes you have already configured the Cisco ITPs and SS7 components associated with the Cisco BTS 10200. If not, then see the "ITP Configuration Information" section on page 5-49."

```
< Defines the call control route between the OPC and DPC >
add call-ctrl-route ID=inet3-ccroute2; DPC_ID=inet-callgen3-1;
USER_PART_VARIANT_ID=ANSISS7_GR317; SI=ISUP; ROUTING_KEY_ID=rk-itp

< Defines a template that specifies common characteristics of the media gateway >
add mgw_profile ID=Cisco5850; VENDOR=Cisco; PORT_START=1; MGCP_VERSION=MGCP_1_0;
mgw_type=5850;

< Defines information that is unique to each MGW managed by the call agent. The MGW can be
uniquely addressed by domain name , an IP address, or the TSAP address. >
```

```
add mgw  ID=d-58-240; TSAP_ADDR=d-58-240.site1.cactus2.cisco.com; CALL_AGENT_ID=CA146;
MGW_PROFILE_ID=Cisco5850; STATUS=INS; CALL_AGENT_CONTROL_PORT=2427; type=TGW;

< Define the trunk group and terminations for the SS7 trunk group. >
add ss7_ansi_tg_profile id=ss7-ansi; cfn_supp=N; cot_duration=1; cot_freq=0; cot_orig=N;
cot_tone=4W_TO_4W; fast_answer_supp=N; hop_counter=20; inband_info=N; send_atp=Y;
send_cip=N; send_cpn=Y; send_gap=Y; send_gn=N; send_jip=Y; send_ocn=Y; send_redir_num=Y;
t_8=15; t_blo=6; t_ccr_r=12; t_cgb=15; t_cot_l=300; t_cot_r=20; t_grs=15; t_iam=30;
t_rel=6; t_rsc=15;
add trunk-grp
ID=2401201;CALL_AGENT_ID=CA146;TG_TYPE=SS7;TG_PROFILE_ID=ss7-ansi;POP_ID=ny;QOS_ID=G729B;c
all-ctrl-route-id=inet3-1-ccroute1;MGCP_PKG_TYPE=T;dial-plan-id=ny;
add termination mgw_id=c-58-240; type=TRUNK; oper_status=NF; prefix=S12/DS1-1/;
port_start=1; port_end=24;
add trunk tgn_id=2401201; mgw_id=c-58-240; cic_start=4001; cic_end=4024;
termination_prefix=S12/DS1-1/; termination_port_start=1; termination_port_end=24;

< Define the routing for the trunk group. Note the dial-plan entry that defines the digits
that when matched will direct the call to the trunk group defined above. >
add route id=rt_2401201; tgn1_id=2401201;
add route_guide id=rg_2401201; policy_type=ROUTE; policy_id=rt_2401201;
add destination dest_id=dest_2401201; call_type=LOCAL;
route_type=ROUTE;route_guide_id=rg_2401201;
add dial_plan id=ny; digit_string=2402201; dest_id=dest_2401201;

< Put the trunks and media gateway in service >
equip trunk-termination tgn_id=2401201; cic=all;
control mgw id= d-58-240;mode=forced; target-state=ins
control  trunk-grp id=2401201; mode=forced; target-state=ins;
control  tt tgn_id=2401201; cic=all; mode=forced; target-state=ins;
```

Configuring the Cisco IAD2431

The configuration of the Cisco IAD is a combination of a router and a media gateway. The main difference between the Cisco IAD and the trunking gateway is the line packages required. Because the Cisco IAD provides customer-facing services, it must be able to provide features like three-way calling, call waiting, and so on. Depending on customer requirements, features like NAT and security ACLs may also need to be configured.

```
< DNS configuration for the IAD. >
ip domain round-robin
ip domain name bts
ip name-server 10.152.136.32

< Define the T1 for connectivity to the Cisco 10000 router. >
controller T1 1/0
 framing esf
 fdl both
 linecode b8zs
 cablelength short 133
 channel-group 0 timeslots 1-24 speed 64
!
< Define the class map for voice bearer, voice signaling and telnet traffic. >
class-map match-all voice-signaling
match access-group 122
class-map match-all ztel-telnet
match access-group 123
class-map match-all voice-rtp
 match access-group 121
…
```

```
< Define the polices that will be applied to the traffic classified above. Note that since
the IAD is the ingress to the network we mark the traffic with the appropriate DSCP value
so that is can be queued appropriately. >
policy-map voice
class voice-rtp
  set ip dscp ef
  priority percent 60
 class voice-signaling
  set ip dscp af31
  bandwidth percent 3
 class telnet
  bandwidth percent 2
  set ip dscp af11
 class class-default
  set ip dscp default
  fair-queue
  random-detect
!
< This is a customer facing Ethernet interface. Note that PAT is being used to translate
customer IP addresses to the public IP address for this customer.
interface FastEthernet0/0
 ip address 192.168.220.5 255.255.255.0
 no ip redirects
 no ip proxy-arp
 ip nat inside
 load-interval 30
 duplex auto
 speed auto
 no cdp enable
…
interface Serial1/0:0
 bandwidth 1536
 ip address 10.148.0.18 255.255.255.252
 ip nat outside
 max-reserved-bandwidth 90
< Apply the policy defined above the the egresson the serial interface. >
 service-policy output voice
 encapsulation ppp
 load-interval 30
 ppp authentication chap
 ppp chap hostname iad-chap
…
< Access list to identify RTP traffic >
access-list 121 permit udp any any range 16384 32767
< Access list to identify MGCP signaling traffic ?
access-list 122 permit udp any any range 2427 2428
access-list 122 permit udp any any range 2727 2728
< port for RUDP backhaul of ISDN signaling >
access-list 122 permit udp any any range 5555 5556
< port for MGCP ping from call agent >
access-list 122 permit udp any any eq 12100
< Access list to identify telnet traffic >
access-list 123 permit tcp any eq telnet 10.0.0.0 0.255.255.255
!
voice-port 2/0
 timeouts interdigit 5
…
voice-port 2/15
 timeouts interdigit 5
!
mgcp
mgcp call-agent mgcp-tpapss01ca.bts 2427 service-type mgcp version 1.0
mgcp dtmf-relay voip codec all mode nte-gw
mgcp restart-delay 300
```

```
mgcp codec g726r32 packetization-period 20
mgcp package-capability rtp-package
mgcp default-package rtp-package
no mgcp timer receive-rtcp
< The next two lines define the source interface for signaling and media packets >
mgcp bind control source-interface Serial1/0:0
mgcp bind media source-interface Serial1/0:0
!
mgcp profile default
< The mgw will try to contact the ip addresses defined as a result of the dns query of the
call agent host name. Each IP address will be retried per the max1 retry value and for the
last IP address it will be retried per the max2 retry value. >
 max1 retries 3
 max2 retries 3
!
!
dial-peer voice 20 pots
< defines MGCP as the signaling protocol that will control the voice port >
 application mgcpapp
 port 2/0
…
dial-peer voice 215 pots
< defines MGCP as the signaling protocol that will control the voice port >
 application mgcpapp
 port 2/15
```

For more information on configuration of the IAD, see the following documentation:

- Cisco IAD2430 Series IADs
  http://www.cisco.com/univercd/cc/td/doc/product/access/iad/iad2430/index.htm
- Cisco IOS Release 12.3
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/index.htm