Cisco Bandwidth Manager
User Guide to Applications
Software Release 1.5
April 20, 2006

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
THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)

Cisco Edge Admission Control User Guide to Applications
© 2006 Cisco Systems, Inc. All rights reserved.
Contents

11 Topology Information Model

Examples

ATM

Session Information Model

Layout

Resiliency

Director BPM

3 Functionality

Overview

Director BPM

Resource Controller BPM

Relationships to Functional Interfaces

Director BPM

Resource Controller BPM

Architecture

Topology Awareness Function

Topology Store Function

Path Computation Function

Admission Control Function

Signaling Interface Function

Session Awareness Function

Session Store Function

Context Store Function

Context Timer Function

Accounting Log Function

Response Cache Function

Statistics Function

4 Deployment

Overview

Director BPM

Resource Controller BPM

Terminology
Overview

This document discusses the Cisco Edge Admission Control (EAC) offering that runs on the Broadband Policy Manager (BPM) system. It discusses the EAC topology, functionality, deployment, and its applications and their position in the BPM architecture. The document gives an overview of the BPM system and EAC components and explains the benefits they provide for service providers and their customers.

Before you use the information in this document, complete the installation of the hardware and software that came with your BPM system according to the instructions in the documentation.

Audience

This guide is for the network professional who handles the EAC capability.

Organization

This document contains six chapters:

- Chapter 1 - Introduction
- Chapter 2 - Topology
- Chapter 3 - Functionality
- Chapter 4 - Deployment
- Chapter 5 - Applications in Action
- Chapter 6 - Agents

BPM Documentation Set

In addition to this book, the documentation for your BPM system includes the following documents:

- Broadband Policy Design Studio User Guide
Preface

- Broadband Policy Manager Operations Guide
- Broadband Policy Manager Release Notes
- Broadband Policy Manager Installation and Configuration Guide

**Cisco Broadband Policy Design Studio User Guide**

This guide provides instructions for installing the BPDS and using it to create, deploy, and manage network services, and to manage subscribers.

**Cisco Broadband Policy Manager Operations Guide**

This guide describes the use of the BPDS to obtain information, conduct day-to-day operations, perform maintenance tasks, and troubleshoot problems with the BPM system.

**Cisco Broadband Policy Manager Release Notes**

This document describes new features, known limitations, and other important information about the BPM system.

**Cisco Broadband Policy Manager Installation and Configuration Guide**

This guide describes how to install the software for the Broadband Policy Manager (BPM). It describes how to install and configure the Solaris operating system for use by the BPM system. It also includes procedures to install and configure the BPM software and the procedures to install and log into the Broadband Policy Studio (BPS) graphical user interface (GUI).

**Cisco Bandwidth Manager User Guide to Applications**

This guide discusses the Bandwidth Manager (BWM) offering that runs on the Broadband Policy Manager (BPM). It discusses the BWM applications and their position in the BPM architecture, BPM and BWM components, possible deployment scenarios and supported platforms.
Overview

The Edge Admission Control (EAC) solution targets Capacity Admission Control (CAC) for the access network connected via a core network in which only the access network contains tracked capacity resources. The solution coexists in a network with other services and may interact with other traffic types.

The EAC providesCapacity Admission Control to IP networks. The BPM provides the basis for a variety of applications. Its architecture allows service providers to build additional dynamic, subscriber-based, IP services. It delivers the following CAC applications, which deliver carrier-class scalability, manageability, performance, and reliability:

- Voice CAC
- Video CAC

Each application builds on the Broadband Policy Manager (BPM). The solution combines these applications with the BPM and integrates with the relevant application servers, such as Session Initiated Protocol (SIP) servers or video middleware.

Voice CAC supplies management of multivendor call managers.
Introduction

The key features target the Internet Engineering Task Force (IETF) SIP-based Broadband Voice and Video. CAC bases CAC decisions on calculated link capacity values that are stored from the topology management functions. When signaled with changes that have occurred in the network configurations, the database is updated.

VoIP Architecture

The architecture works with broadband Voice over Internet Protocol (VoIP) architectures. Refer to RFC 3665 for details on call setup examples associated with this architecture. Figure 1-1 provides an architecture outline.

Figure 1-1. VoIP Architecture Outline

The architecture supports multimedia devices in the home network that support SIP signaling. This includes multimedia conferencing software on the PC; an IP Phone; IP Voice software on a PDA, a television, or a set-top-box (STB); a video conferencing system, or any variety of SIP-based communication clients.
Video-on-Demand

Video-on-Demand provides support for IP-based video-on-demand distribution. A subscriber can interactively start, stop, and resume videos. He can download content onto a personal video recorder, where he can view content from a local cache or a dedicated unicast stream from a video server with play, stop, and resume controls. Figure 1-2 presents Video-on-Demand details.

Figure 1-2. Video-On-Demand Detail.

A video client is a STB attached directly to a subscriber television. It can also be a software-based client on a PC, PDAc, or cellular phone. The video client interacts with a video middleware component that provides available stream information and processes remote control commands, for example, play, pause, and stop. The video middleware also interacts with the VODS, which streams content to the subscriber.
Standards Body Requirements

Although standards are under development by the European Telecommunications Standards Institute (ETSI)/Telecommunications and Internet Services and Protocol for Advanced Networking (TISPAN) standards bodies, the Cisco solution adheres to the RACS framework vision.

ETSI/TISPAN

ETSI/TISPAN provides an open, unified layer for controlling network resources for NGN applications. See the design in Figure 1-3.

Figure 1-3. Cisco Mapping to ETSI/TISPAN

RACS evolves the 3GPP R6 PDF to support wireline and wireless networks. It separates the PDF into a Service Policy Decision Function (Director BPM) that handles access technology independent aspects of policy and admission control from the Access-Resource Admission Control Function (Resource Controller BPM) that handles access technology specific policy functions.
• RACS architecture is limited because it defines only a few policy enforcement points.
• Many PEPs are employed as part of a service delivery architecture.
• Cisco supports generic concept of PEP topologies and allows any PEP to be controlled.

Figure 1-3 demonstrates the alignment of the Cisco solution to the ETSI/TISPAN architecture.

**Director BPM**

• BPM Director BPM plus Director BPM Resource Controller BPM
• Implementation of Gq when standard is finalized
• SIF-TRPC or SIF-SOAP Rq
• Ia vendor-specific in the short term (i.e., SCE API)

**Resource Controller BPM**

• Multiple RC handling Edge Functions
  • MGW, DSLAM, BRAS, MPLS-PE (for MLPS-based Admission Control)
  • DSL Forum active in assisting definitions for Re
  • NASS interface through XML/HTTP, RADIUS, and others.

The Cisco solution provides a fully compliant RACS implementation and can extend support to non-RACS compliant policy enforcement points and complex service delivery networks that are not supported by the RACS architecture (e.g., Deep Packet Inspection devices, MPLS PE routers, and DSLAMs).
Overview

The Cisco solution is multitechnology and supports both ATM and Ethernet access networks. In the sample network layout, shown in Figure 2-1, each DSLAM-derived ATM Virtual Path (VP) transports 100 subscriber Virtual Circuits (VCs).

Figure 2-1. Sample Network Layout
Each VP has a 6 Mbps peak cell rate (PCR) and a priority queue (PQ) of 512 Kbps. Each VC transported within the VP is 640 K or 1280 K downstream and 256 K upstream with a PQ of 128 Kbps.

Reference Interface Architecture

Figure 2-2 examines the preferred reference interface architecture.

The Edge Admission Control (EAC) offering maintains five separate interfaces:
- SESS interface to the SIP server
- DBASE interface to the user/session control database
- WEB interface to the Content Portal
- POOL interface over which dynamic pool addresses are learned from the BRAS
Static IP Topology

Figure 2-3 presents the static IP topology model, which provides support for edge networks utilizing dedicated links as bandwidth resources. Here, IP hosts (or subnets) are interconnected by a dedicated link of known bandwidth. This provides a simple admission control solution, based on the concept of a link that connects two points on the network. Each link is associated with an IP host or an IP subnet on one side, and a border node (a special IP host) of the core network on the other. Each link has an associated capacity.

Figure 2-3. Static Edge IP Topology
In this network topology, bandwidth capacity exists at both the VP and the VC levels. Because of this, oversubscription is possible. For example, a 100 mbps VP may contain 100x 2mbps VCs (2:1 oversubscription factor). The system takes this into account when the admission control decision is made.

The VC is checked for its available capacity. If the CAC request indicates a larger quantity than the capacity the VC can handle, the request is rejected. If the VC can handle the quantity, the system checks the VP capacity. The system determines the capacity of the VP and the existing reservations on other VCs in the VP to determine if the request should be admitted.

Weighted scheduling classes further complicate the decision. With a weighted scheduler, the weight of the VC within the VP affects the bandwidth available for a reservation.
Ethernet Edge Topology

Figure 2-5 presents the Ethernet Edge network topology model. Here, each subscriber receives an IP address per service. At the Ethernet DSLAM, all traffic from the subscriber is grouped into an 802.1q VLAN. Traffic is aggregated by an Ethernet switch. At the Ethernet switch, services are grouped into common service classes using an additional VLAN tag.

Figure 2-5. Ethernet Edge Topology

Topology Information Model

TSF maintains the Topology Information Model (TIM), which stores connectivity information and provides a flexible resource attachment scheme. Arbitrary resources are assigned to nodes and links. The information model encapsulates the basic graph characteristics of links and nodes, added to the ability to create resource types, and assigns them to those nodes and links. This model accommodates various network topology models, both physical and virtual.

Examples

This section contains the topology examples.
ATM

In an ATM example topology, a BRAS contains multiple ports, each port contains multiple VPs, and each VP contains multiple VCs. The VC represents a hard line into a customer premises. Thus, the Customer Premises Equipment (CPE) is uniquely identified by BRAS-Port-VPI-VCI.

In the example (Figure 2-6), admission criteria is based on IP PQs associated with IP traffic classes. There exists a PQ for both the VP and the VC, and in both upstream and downstream directions. Since, in the topology, the VP contains multiple VCs, those VCs share a single VP PQ resource.

Figure 2-6. ATM Circuit Hierarchy

Physically, the VP is typically terminated at a DSLAM, which aggregates a VC from each CPE into a VP (or multiple VPs) back to the BRAS (each VP on a BRAS port) (Figure 2-7).

Figure 2-7. Simplified ATM Physical Topology
A DSLAM is not a real node, in that inherently, data traveling into a DSLAM over a VP cannot go to an arbitrary CPE. Each VC is inside a particular VP. If multiple VPs exist between the BRAS and DSLAM, they refer to a CPE subset. There is a virtual node per VP, if a node is needed. The following examples show only the links and interfaces carrying traffic from the core to the CPE.

A hypothetical BRAS (Figure 2-8) has a single northbound interface (purple), while it has multiple nested southbound interfaces (red/yellow). This figure represents the northbound interface restriction (untracked) in purple, the ATM port interface in red, and the VP interface in yellow. In this example, the BRAS also terminates the VC directly, rather than the VC being terminated by a DSLAM. A level of interface nesting exists, and, therefore, resource nesting.

**Figure 2-8. Hypothetical BRAS, DLSAM, and CPE Nodes**

The entire BRAS, which encompasses multiple incoming and outgoing interfaces is considered as one node (B). (Only ingress north and egress south are shown.) The resources consumed by traffic through the BRAS are associated with the interfaces shown. Each line into, or out of, the circle represents an interface ability to communicate with another node in the topology.

The DSLAM (nodes J and K) represents an ATM transport cloud and has a similar set of ingress and egress interfaces. These are shown as simple non-nested interfaces. The model can accommodate more complex nodes at the DSLAM location. Its interfaces shown in orange represent the termination of the VP to the BRAS. Those in blue represent a VC that terminates at a CPE.

The CPE (nodes C, D, E) is shown as a simple non-nested interface. It is the topology termination, so has no southbound interfaces. Its interface is shown in magenta and represents the VC termination.
The first example shows the inclusion of two virtual DSLAM nodes in the topology. The link into the BRAS (B) comes from an inner part of the topology. In this example, that is the core on which resources are not tracked. A resource representing the northbound BRAS interface constraints (purple B1) is associated with the ingress link to Node B.

The links from BRAS to DSLAM (L-BJ, L-BK) are associated with resources representing the nested interfaces of the BRAS (Port, VP), and the ingress interface of the DSLAM that terminates the VP.

In figure Figure 2-9, the link to each CPE (L-JC, L-KD, L-KE) has resources corresponding to the appropriate interface constraints: the VC and the CPE ingress that terminates the VC. This example attaches numerous resources to the links. The ingress interfaces of a virtualized DSLAM, and a CPE may not be tracked if it is inherently handled via the ATM protocol.

Figure 2-9. ATM TIM Example with DSLAM
The second example (Figure 2-10) shows links directly from the BRAS to each CPE. Each link is associated with the port, VP, DSLAM ingress, VC, and CPE ingress resource. The node representing the DSLAM need not be present to account for the resource constraint it may incur by its physical presence.

**Figure 2-10. ATM TIM Example without DSLAM Nodes**

For a two-tier VP/VC Capacity check, these diagrams clearly represent an over abundance of tracked resources. The resources tracked and attached to links are the VP (yellow) and VC (blue), plus the core-to-BRAS interface resource constraint. The figure shows that the VCs from the BRAS B to CPEs D and E share a common VP, while the VC to C is in a different VP.
The last diagram (Figure 2-11) represents the approach that expedites the path calculation for the access network, and fully meets hierarchical resource utilization needs.

**Figure 2-11. ATM TIM Example for VP/VC CAC**

**Director BPM**

To accomplish the Edge Admission Control (EAC) goals, the Director BPM requires the following from the TIM:

- IP address pool assignments to each BRAS
- Resource Controller BPM component (primary and secondary address) assigned to each BRAS

This is accomplished by defining a resource of type POOL with an attribute representing the subnet pool definition. Associating the pool resources to the appropriate BRAS nodes in the topology completes the requirement. For the Resource Controller BPM component, it is accomplished by defining a resource of type ARACF with attributes representing primary and secondary, with values identifying an IP address and port (contact point) for a Resource Controller BPM.

Other attributes of BRAS nodes or even the introduction of Media Gateways (bridges to the PSTN) is accomplished by adding appropriate resources to those nodes. Following conventions for creating the identifiers of nodes can expedite node recognition, but additional information about the device are more appropriately accomplished by assigning rich resources to the node and examining within the application framework.
**Resource Controller BPM**

At the Resource Controller BPM, resource layers for the network such as VP and VC PQs are used to track resources. The deployed product is (or can be configured to be) cognizant of the resource types. Additionally, the EAC must understand the contexts existing over any link in its topology. This information is used clean up resources appropriately when a link fails, or when a (PPP) session ends. The EAC accomplishes this by automatically creating a resource type called CONTEXTS and assigning one to each link. This resource tracks all active contexts over a link on the local topology.

**Session Information Model**

The SSF maintains the SIM, which connects dynamic sessions within the topology. An IP address is typically an assigned IP address. Subsequently, it can belong to a different CPE. For IP pool reassignment, it may be shifted to a CPE attached to a different BRAS associated with a different Resource Controller BPM.

The Resource Controller BPM components use the dynamic mapping of the IP address to the session to determine the CPE and BRAS associated with a particular IP address when it is in use. This determines the topology elements terminating the context, so that the PCF can compute a path between them in the local topology. Also, since this information determines the links and resources in the TIM that are used to evaluate the Admission Control Decision, it must be consistent with the other external elements. It causes incorrect behavior for an IP address assignment from DHCP to occur, and for the AF to request a call for that specific address before the external system has informed the EAC.

Since the edge cases involved can cause information to resolve to entirely different Resource Controller BPM elements, it is important to achieve the session information notification in the correct manner. However, the soft-state model eventually corrects aberrant behavior. The model maintains eventual consistency, but it does not solve the issue of incorrect admission results due to non-synchronous delivery of presence information.

Director BPMs are unconcerned with the dynamic nature of each individual IP address assigned for each session. Of primary importance is the ability to resolve an IP address to a Resource Controller BPM. This occurs with a best first match against all assigned IP address pools. The Director BPM forwards the request to the determined Resource Controller BPM component, for localized information.
Layout

Figure 2-12 presents a general view of the layered architecture and depicts the following layers:

- Layer 1 - Application Function
- Layer 2 - Policy Control
- Layer 3 - Network Device

The requesting applications are received at the Application Function Layer and abstracted from the network by the Policy Control Layer. The Policy Control Layer handles the northbound abstraction, hybrid southbound control, and the implementation of business rules. The Network Device Layer, containing the multivendor equipment base, provides information about sessions and users and provides the mechanisms for control, for example, Quality of Service (QoS) and firewall mechanisms.

Figure 2-12. Technology Deployment
Figure 2-13 explains the functions of the following devices:

- Director BPM
- Policy Repository BPM
- Resource Controller BPM

The Director BPM maps application function requests to the appropriate Resource Controller BPM. It hides the topology from the application function, executes global policy (for example, global CAC), and handles gate control functions.

The Policy Repository BPM holds persistent global data relative to the following:

- Topology
- Network Devices
- Subscriber Profiles

The Resource Controller BPM executes policy rules associated with network resources, performs network adaptation and admission control decision functions, and supports subscriber applications (quota-based control).
The functional layout of machines and roles for the EAC primarily involves Director BPMs and Resource Controller BPMs (Figure 2-14). Each Resource Controller BPM has responsibility for a portion of the access network. Resource Controller BPMs are deployed redundantly, with a secondary for every primary. The Director BPM determines the access networks in use, queries the appropriate Resource Controller BPMs, and determines the unified result. The Topology-DB houses the global TIM. Changes to this information base are infrequent, but the information is resilient.

Figure 2-14. Deployment Layout

Resiliency

The EAC delivers a highly available capacity reservation service by employing a variety of resiliency mechanisms in various EAC functional areas. The Director BPMs are designed to be stateless, and can achieve high availability by being deployed in an N + 1 active/active manner. An essential part of the EAC solution design is load-balancing across the N+1 set of Director BPMs.
The Resource Controller BPMs handle a specific access network section, and are highly stateful. Resource Controller BPMs are paired in a 1:1 primary/secondary manner. Both the primary and secondary Director BPMs are responsible for an access network section, and they switch to the secondary when the primary does not respond. Other elements, such as the Topology-DB, provide independent resiliency.

**Director BPM**

Failover of a Director BPM does not cause a lasting problem for system performance or availability. Since Director BPMs are stateless and they are deployed in N + 1 active/active configuration, they are load-balanced to allow provision for adequate availability and performance scaling characteristics by adding more Director BPMs. Requests in progress at the specific Director BPM are lost, but are retransmitted to another Director BPM, through the load balancer (repeating message identifiers, etc.), and the EAC services them correctly (Figure 2-15).

**Figure 2-15. Director BPM Failure**
When a failed Director BPM restarts, it synchronizes its TIM with the topology database. It re-establishes connections with the Resource Controller BPMs. It is ready to receive requests from AFs, and signals its ability to rejoin the load balance set.

Director BPMs must know the state of primary and secondary Resource Controller BPMs responsible for access networks. The Director BPM can decide that failover criteria are met. This is due to delayed response times or dropped requests, or a notification from the Resource Controller BPM or other Director BPMs.
Overview

This chapter discusses the following functional elements of the market trial version of the Edge Admission Control (EAC) key application:

- Installation
- Manual Provisioning Interfaces
- Programmatic Interface to the EAC
- Alarms and Statistics
- Configuration and Log Files

The Cisco alignment with the European Telecommunications Standards Institute (ETSI)/Telecommunications and Internet Services and Protocol for Advanced Networking (TISPAN) (ETSI/TISPAN) bodies includes the solution-specific high level functional elements:

- Director BPM
- Resource Controller BPM
- Presence-Director BPM
- Topology-DB
**Functionality**

**Director BPM**

The Director BPM determines the Resource Controller BPM component responsible for a particular QoS request, coordinates the decisions returned by the Resource Controller BPM component, and formulates a unified response.

**Resource Controller BPM**

The Resource Controller BPM handles QoS requests for a Topology Information Model sections, for example, a particular access network or node.

**Relationships to Functional Interfaces**

**Director BPM**

The Director BPM encapsulates a specific type of ACF that uses Address Pool Information to determine the responsible Resource Controller BPM components. It augments the request with local context (the path segment for which the Resource Controller BPM is responsible). The Director BPM forwards it to the Resource Controller BPM components. The ACF collects the responses and aggregates the results into a unified response for the QoS request. For differing responses from the Resource Controller BPM, the ACF restores appropriate state to the Resource Controller BPM components.

The Director BPM represents:

- SIF to interface with the external Application Function (AF)
- ACF to perform a unified Admission Control Decision (ACD)
- TSF to store the Director BPM TIM, which holds pool and Resource Controller BPM entries for each Aggregating Access Node (BRAS)
- TAF to react to external updates to the TIM, and to filter them into the internal TSF.
- SSF to determine the BRAS node that is associated with a particular IP address via IP pool matching.
- RCF for handling retransmission of messages
- ALF for recording accounting information
- SF for recording statistics
Functionality

Resource Controller BPM

The Resource Controller BPM encapsulates an ACF that performs the access network-level Admission Control Decision (ACD), based on resource utilization. The Resource Controller BPM represents:

- SIF to interface with the external AF, which is the Director BPM. Since this is internal, the SIF is transparent.
- TSF to maintain the TIM that the Resource Controller BPM is responsible for and that resource consumption is checked against
- TAF to interact with the TSF to react to topology changes (link or node activate/deactivate) by correctly cleaning up internal state and resource utilization
- SSF to maintain the SIM that the Resource Controller BPM is responsible for the sessions through the topology that the Resource Controller BPM is responsible for SAF to interact with the SSF and TSF and react to session changes by correctly cleaning up internal state and resource utilization
- PCF to determine the path through the local topology that the call transits
- CSF to maintain the context (or call) information for media flows
- CTF to enact the soft-state reservation model to automatically remove orphaned or stale contexts and the resources they consume
- ACF to perform local ACD, based on TIM resource utilization
- RCF for handling retransmission of messages
- ALF for recording accounting information
- SF for recording statistics

Architecture

The delivery of Telephony CAC utilizes generalized internal Cisco components.

- Topology Awareness Function
- Topology Interaction Function
- Topology Store Function
- Path Computation Function
- Admission Control Function
- Signaling Interface Function
- Session Awareness Function
- Session Store Function
Functionality

- Context Store Function
- Context Timer Function
- Accounting Log Function
- Response Cache Function
- Statistics Function

The functional components are connected through well-defined interfaces to comprise the Director BPMs and Resource Controller BPMs.

Figure 3-1. Director BPM / Director BPM
The Topology Awareness Function (TAF) extracts changes in the node and underlying network details by various methods. It stores the information and maintains the information model in a data store. Node and link failures detected by a TAF (possibly a different TAF) are used to dynamically update and maintain the information model.

The TAF has two discrete interface functions:

- Interface to the network over which network discovery detail is extracted
- Interface to the Topology Store Function (TSF) over which topology data is recorded within the Topology Store information model
Functionality

Topology Store Function

The Topology Store Function (TSF) maintains the Topology Information Model (TIM). This is populated by clients acting as TAFs. The database stores the entire network node and link detail, or the needed local subset of this information, depending on deployment configuration. Information is stored against nodes that describe their capabilities. Each node has a unique identifier (deployment dependent). Each link is stored as a directed association between two (or more) nodes. Other elements using the TSF, such as the PCF or ACF, may use the stored Topology Information Model to determine the path between two end points, or update resources in the TIM.

Depending on the deployment, links and nodes need not describe the physical network topology. For tunnels use (for example, MPLS), the description may depict the tunnel head end and remote nodes and ignore the core topology underlying this path. This virtualization allows the admission control criteria to dictate the requirements on the TIM. The TAF in use understands the same virtualization to populate and maintain the TIM appropriately.

The TSF has three separate interfaces to the other system functional components (ACF, PCF, and TAF). The same interface is utilized to support the requirements of this interconnectivity.

Path Computation Function

The Path Computation Function (PCF) determines the path taken through the topology for any given end-to-end session for which the ACF requires information. The PCF determines the nodes and links used for session interconnectivity, according to the request. The result may return both symmetrical and asymmetrical paths for certain topology sections. The PCF is synchronized with the TIM so that it computes valid paths. It must model the underlying network behavior to ensure that its results accurately reflect the path that traffic takes across the network. The ACF utilizes the PCF to subdivide the underlying network into the discrete segments required for any given admission control decision. The PCF provides the information necessary to permit the ACF to subdivide the admission control tasks across a number of underlying admission control functions, though this information comes from the TIM.

The PCF has two discrete, internal interfaces:

- An interface to the ACF through which the ACF requests path details on a given session request
- An interface to the TIM via the TSF through which the PCF can extract raw topology data and over which to determine path calculations. This interface is the same for ACF, TSF, PCF, TSF.
Admission Control Function

The Admission Control Function (ACF) receives and responds to session set-up requests from the Signaling Interface Function (SIF). Based on specific requests from the SIF, the ACF initiates the appropriate measures to determine the capability within the TIM to satisfy the requirements of any given session request. Using classical event condition mode, the ACF can support sophisticated policy decision rules. When the network (and network device) capability permits dynamic resizing of link bandwidth and queue capacity, the ACF can attempt to dynamically resize links for a positive admission control decision. This is handled through the TIF. The ACF relies on the PCF to determine the specific path to be taken through the topology. When a session is accepted, the ACF updates the Topology Information Model to reflect the available capacity left after accepting this session.

The ACF has several (internal) interfaces:
- An interface over which call set-up requests are delivered
- An interface to the PCF to calculate a path through the topology
- An interface to the TSF to allow the capacity of links in the TIM to be updated (when capacity is a resource attached to a link). This can utilize the same interface methods as the PCF TSF and TAF TSF interface functions
- An interface to the TIF to enable requests for dynamic resizing to be handled

Signaling Interface Function

The Signaling Interface Function (SIF) handles messages to and from the requesting application. It provides the ACF (ACF) with the session parameters that allow the ACF to accept or deny the call request. The SIF supports signaling protocols at its northbound interface into the requesting application. The interface specifications closely follows the standardization efforts across all appropriate standards organizations. Its southbound interface into the ACF provides an abstraction layer from the choice of actual application signaling method.

The SIF has two discrete interfaces:
- An interface to the requesting application
- An interface into the ACF that provides an abstracted messaging model to the ACF
Functionality

Session Awareness Function

The Session Awareness Function (SAF) obtains dynamic session information. This relates to individual subscriber sessions (IP) and subscriber network sessions (such as PPP). Subscriber sessions are controlled at the edge of the service provider network and can provide elements that are utilized within the overall admission control framework. The information supplied by the SAF is leveraged for mapping subscribers to physical network elements (devices and ports) and can therefore provide valuable information to the overall Topology Information Model.

The SAF has two discrete interfaces:

- An interface to the network over which session awareness is gleaned (i.e., RADIUS, DHCP, e4 ETSI/TISPAN protocol)
- An interface to the Session Store Function (SSF) to permit session state to be stored within the session database

Session Store Function

The Session Store Function (SSF) enables subscriber session state information in the Session Information Model (SIM) to be maintained. Various Cisco functional components can interrogate the SSF. Data from the SSF populates dynamic topology element attributes in the Topology Information Model, or associates subscribers with particular topology elements. The SSF communicates with the other Cisco functional components through its interface.

Context Store Function

The Context Store Function (CSF) determines how media contexts are stored. A media context is a collection of media flows, each of which describes an IP stream via its endpoints, direction, capacity, and various other attributes. The CSF stores information about the TIM resources in use by each flow and the flow characteristics. This information releases the appropriate capacity from the TIM when handling a QoS release message. The CSF communicates with the other Cisco functional components through its interface.

Context Timer Function

The Context Timer Function (CTF) is the mechanism that accomplishes the soft-state semantics for contexts and the resources they consume. Its responsibility is to periodically release expired contexts, and recoup their resources. It does this by interfacing with the ACF (for QoS release capability) and with the CSF (to retrieve and remove contexts).
The CTF has two interfaces and interacts with other components.

- An interface to allow timeouts to be registered with the CTF, or initiate an immediate timeout check
- An interface to handle or initiate a timeout interval
- The CTF interfaces with the ACF to initiate a QoS release action for expired contexts. It uses a reserved Application Function Identifier to differentiate itself from an external QoS release.
- The CTF interfaces with the CSF to retrieve contexts to validate their expiration and retrieve necessary inputs to QoS release.

**Accounting Log Function**

The Accounting Log Function (ALF) records entrance parameters, internal decisions, and exit responses. The subscriber provides accounting pertinent information and a correlation identifier, and the ALF stores the information in an appropriate manner. The ALF receives accounting information through its defined interface.

**Response Cache Function**

The Response Cache Function (RCF) facilitates message replay. It stores a LRU cache of responses for particular message identifiers. This allows it to recognize repeated message identifiers within a message window. This allows the system to immediately respond with the previously given response rather than duplicating the action. Also, it provides the ability to detect and respond with an error when presented with concurrent use of a message identifier. The RCF adds and retrieves responses over its defined interface.
Statistics Function

The Statistics Function (SF) records and queries system statistics. It provides a location for various components to store statistics concerning their runtime state and for other clients to inspect those statistics.

The system provides the following statistics:

- `<AF>.qos.<action>.count`
- `<AF>.qos.<action>.accept.count`
- `<AF>.qos.<action>.deny.count`
- `<AF>.qos.<action>.error.count`
- `<AF>.qos.<action>.replay.count`

where,

- `<AF>` is the Application Function ID (also, a reserved key for the sum total of statistics for all the AFs)
- `<action>` is the request name (i.e., reserve, modify, refresh, release)

Certain statistics, such as release deny, do not increment. The SF interacts with its clients over its defined interface.
Overview

The devices below are the high-level functional elements from the Broadband Policy Manager (BPM). The BPM aligns with the European Telecommunications Standards Institute (ETSI)/Telecommunications and Internet Services and Protocol for Advanced Networking (TISPAN) standards bodies.

- **Director BPM**
- **Resource Controller BPM**

**Director BPM**

The Director BPM functional element determines which Resource Controller BPM (RC) BPM components are responsible for specific QoS requests, coordinates the decisions returned by the Resource Controller BPMs, and formulates a global response.

The Director BPM encapsulates a very specific ACF type that determines the responsible Resource Controller BPMs, inserts the local context into the request (which segment of the path is the Resource Controller BPM responsible for), and forwards to the Resource Controller BPM. The ACF collects the responses and aggregates the results into a global response for the QoS request.

The Director BPM represents the following:
Deployment

- SIF, to interface with the external application function (AF)
- ACF, to perform a global Admission Control Decision (ACD)
- TSF, to store the Director BPM TIM, which holds pool and Resource Controller BPM entries for each access aode

The Director BPM functional element directs session awareness information to the appropriate Resource Controller BPM. The Director BPM encapsulates a SAF that interacts with the SSF of appropriate Resource Controller BPM. The responsible Resource Controller BPMs are determined via the Director BPM methodology, using the association between access node and pool, and Resource Controller BPM. The Director BPM represents the following:

- TSF to store the Director BPM TIM, which holds pool and Resource Controller BPM entries for each access node (as in the Director BPM)
- SAF to interact with the SSF on the appropriate Resource Controller BPM, to create or destroy session information in the correct localized SIM.

The Director BPM encapsulates a TAF that is responsible for interacting with the TSF the Director BPMs and Director BPMs. The Director BPM element updates the association between access node and address pool. This is topology information in the Director BPM and Director BPM TIM.

The Director BPM element holds and distributes (to the Director BPM and Director BPM) the association between network address pools and specific topology elements (access nodes).

The Director BPM represents TAF to interact with the TSF of the Director BPMs and Director BPMs.

Resource Controller BPM

The Resource Controller BPM element is responsible for QoS requests for a specific part of the Topology Information Mode, for example, for a particular access node. The Resource Controller BPM encapsulates an ACF that is responsible for performing the low-level Admission Control Decision (ACD), based on resource utilization. The Resource Controller BPM represents:

- SIF to interface with the external AF, which is a Director BPM here. Since this is internal, the SIF may be transparent.
- TSF to maintain the TIM that the Resource Controller BPM is responsible for
- SSF to maintain the SIM that the Resource Controller BPM is responsible for (sessions through its TIM)
- PCF to determine the call path through the local topology
Deployment

- CSF to maintain the context information for media flows
- ACF to perform local ACD, based on TIM resource utilization

The Director BPM holds the global Topology Information Model (TIM), from which the Resource Controller BPM retrieves relevant portions.

The Resource Controller BPM element holds and distributes (to the Director BPM) the mapping between topology elements (access nodes) and the Resource Controller BPM element.

The Resource Controller BPM encapsulates a TAF that is responsible for interacting with the TSF of the Director BPMs and Director BPMs. The Resource Controller BPM element updates the association between access node and Resource Controller BPM. This is topology information in the Director BPM and Director BPM TIM.

Terminology

Application ID

This identifier differentiates various application function implementations to the EAC.

Transaction ID

This uniquely identifies a message sent to an interface. This identifier provides correlation capability for failure management and mediation. It also allows the client of the interface to retransmit identical messages if the response is lost, and the EAC element can maintain transactional consistency. The uniqueness of a transaction ID is possibly different per interface.

Transaction Token

This identifies the transaction begin created / maintained / committed / etc. by one of the store functions for actions taken through this interface. This token is unique within the connection and existing open transaction tokens. This is different from the Transaction ID, which is for message level correlation.

Context ID

This parameter uniquely identifies a context containing the media streams. This identifier should be globally unique.

Result

This is a 4-byte integer encapsulating the following elements:
Deployment

- **Status**
- **Reason**

**Status**

This is one of Success = 0, Deny = 1, or Error = 2

Accept and deny do not always make literal sense for an operation. Some analogous possibilities are OK, NOT-OK, and ERROR. In some cases the system does not use the Deny / NOT-OK value. This is a 2-byte integer.

**Reason**

If the result status is Deny or Error, the reply include a reason. If the Status is Success, ignore the Reason. The reason codes are specific to the message type and interface returning a Result. This is 2-byte unsigned integer.

**Resource**

A Success may be referenced by multiple links or nodes. Each Success belongs to a class (Resource Name, for example, VP) and is uniquely defined within that class, by its resource identifier (Resource ID). The properties of a specific type of resource identifier (all identified with the same Resource Name) are the same. However, each resource type may have different attributes.

**Resource Identifier**

**Resource Name**

This is the name of the resource identifier layer, such as VP or VC. An ACF can use this name to determine the correct policy to evaluate against the resource identifier.

**Resource ID**

This is the unique identifier for the resource identifier within the scope of the resource name. The two, together, are unique to all resources.

**Resource Properties**

A set of properties for the resource, the attributes present are consistent for all resources of the same name. When a resource is attached to a topological element such as a node or link for insert, it may omit the properties and simply reference an existing resource via the resource identifier.

**Resource ID**

A node may have multiple resources associated with it.
Link

Resource ID

A link may have multiple resources associated with it.

Flow Descriptor

A flow descriptor is a set of attributes describing a unidirectional media flow from defined source to defined destination.

Flow ID

This identifier uniquely identifies the flow within the context.

Direction

This specifies the direction of the media flow with respect to the Source and Destination of the Context. The possible values are FORWARD = 0, REVERSE = 1, BI-DIRECTIONAL = 2. In the case of REVERSE, the source of the unidirectional media flow is the destination address. This is a 1-byte value.

Source Port

This is the port for the media flow at the source address. The meaning of this parameter changes with the Direction attribute, as do the Source and Destination of the Context. This is 2-byte unsigned integer.

Destination Port

This is the port for the media flow at the destination address (the meaning of this parameter changes with the Direction attribute, just as do the Source/Destination of the Context). This is 2-byte unsigned integer.

Flow Capacity Descriptor

This describes the capacity requirements of the media flow. This encapsulates capacity information that is application-domain specific and endpoint descriptions that may provide context for admission control.

FCD-Type

This is a 2-byte unsigned integer indicating the type of Descriptor. The expected initial FCD type is 0, indicating that the payload is a 4-byte unsigned integer describing Kbps.

FCD-Length

This is a 2-byte unsigned integer indicating the length of the FCD, where the length of the header (type, length) is included.
**FCD-Content**

This specifies the capacity characteristics. For Type 0, it is an integer specifying Kbps. For other types, it may be a more complex traffic descriptor.

**Flow DSCP Descriptor**

This optionally indicates the Type of Service (TOS) or DSCP for this flow (corresponds to IP header). The system may use this to determine the specific resource to resolve the reservation against. This is a 1-byte unsigned integer.

**Flow Application ID Descriptor**

This optionally indicates the application identifier (Protocol Identifier) for this flow (corresponds to IP header). The system may use this to determine the specific resource to resolve the reservation against. This is a 1-byte unsigned integer.

**Lease Length**

This is a request for a minimum lease length for the requested capacity. This is a number of milliseconds for which the capacity lease remains valid, without the receipt of a QoS refresh message. The value 0 is reserved to indicate request for infinite lease (which may not be supported). If the application function wishes the default value for the parameter, it may opt not to specify a Lease Length.

This value is a minimum value only, there is no guarantee that the system recoup the capacity at the exact expiration of the lease, but only that it not do so before. This is a 4-byte unsigned integer.

**Session Descriptor**

The session descriptor is a collection of attributes about sessions:

- End point identities
- Session presence location on the topology

<table>
<thead>
<tr>
<th>Name</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access-Point-Address</td>
<td>The IP address of the CPE.</td>
</tr>
<tr>
<td>Access-Point-ID</td>
<td>The Technical Key (TK) that identifies the CPE in the TIM.</td>
</tr>
<tr>
<td>Entry-Point-ID</td>
<td>The BRAS IP address, the ID for the BRAS in the TIM.</td>
</tr>
<tr>
<td>Properties</td>
<td>Collection of additional flexible properties.</td>
</tr>
</tbody>
</table>
Context

Source VPN
This is the identifier of the source VPN. This provides localized uniqueness to the source address if needed. This is a 4-byte identifier.

Destination VPN
This is the identifier of the destination VPN. This provides localized uniqueness to the destination address if needed. This is a 4-byte identifier.

Source Address
This is the address of the source of the media. The flows are forward/reverse/bidirectional with respect to this address. This is an IP address (IPv4).

Destination Address
This is the address of the destination of the media. The flows are forward/reverse/bidirectional with respect to this address. This is an IP address (IPv4).

Timestamp Create
The time at which the context was created.

Timestamp Expiration
The timestamp at which the context expires, if not refreshed.

Interfaces

Topology Awareness Function
The Topology Awareness Function (TAF) encapsulates the interaction with an external system.

Director BPM TAF
The solution is a manual provisioning interface. The TIM model is represented externally in a file format that captures BRAS-ID, IP-Pool definitions, and Resource Controller BPM element (RC) assignment.

Resource Controller BPM TAF
The solution is a manual provisioning interface. The TIM model is externally in a file format. This format captures BRAS-ID, Port-ID, VPI, VP-PQ, VCI, VC-PQ. This model is flexible enough to recognize that there is encapsulating VP level OQ resource for certain VCs.
Format Description

The format allows the "vp" tag to omit capacity and identification information. This is because in certain ATM topologies there may not be a VP pipe that the VC pipe resides in. There is no VPI and the VP tag is an empty container to keep the file format uniform. Initially, a VP always contains the VC. The port may be the NLC and may have a different format.

Interaction with TSF

The TAF converts the TIM as defined for external interface into a well defined interaction with the TSF. Each BRAS-ID is an element in the TIM, as is each Technical Key (TK) (the BRAS-ID/PORT-ID/VPI/VCI tuple). On the implicit links between these two elements is VP level capacity information (if present), and VC level capacity information. These may have separate upstream and downstream capacities that are applied to the upstream and downstream links between the two elements.

Topology Store Function

The Topology Store Function (TSF) encompasses some storage metaphors for generalized directed graph terminology and some concepts that are specific to the idea that links and nodes in networks become temporarily disabled without disappearing. It allows for flexible resource assignment that models both hierarchical and flat resource models. It also supports transactional semantics.

Path Computation Function

The Path Computation Function (PCF) encapsulates the ability to compute a path through the TIM, based on a flow descriptor, provided by a component, such as the ACF. The initial interface for the PCF may import notifications of TIM updates into the PCF so that it is possible for the PCF to compute and cache intermediate information to speed path computation (for example, Dijkstra Shortest Path Trees). In this intermediate information model, it is necessary to receive updates to know when to recompute.

Get-Path

This operation computes the path from the source to the destination of the flow descriptor, or as much of such a path as exists in the TIM. The client determines if this is sufficient for its purposes.
**Admission Control Function**

The Admission Control Function (ACF) encapsulates a client server message channel for reservation, modification, and release of topology resources for various media contexts. In a possible back communication channel, the EAC may indicate out-of-band occurrences, such as timer expirations. This is not supported initially.

**QoS-Reserve**

The *QoS-Reserve* message reserves a specific resource from the TIM, based upon the provided parameters. The QoS reserve function specifies only media flows that are new reservations in the message. Thus, repeated existing flow descriptors (duplicated flow IDs with pre-existing ones) are ignored (if not an error). If the parameters of flow descriptor changes, this is not detected or persisted. This allows a reservation to indicate emergency preference, for instance.

**QoS-Reserve-Answer**

This reply to the *QoS-Reserve* message contains accept, deny, or error status and any reason for deny or error. It also contain the used lease length that are at least as large as the provided value.

**QoS-Modify**

The *QoS-Modify* message alters the media context reservation information and contains only the flow descriptors to be modified. Any flow descriptor not to be changed, is omitted. Any included descriptor is resolved against the existing flow descriptor, even if they are identical.

**QoS-Modify-Answer**

This reply to the *QoS-Modify* message contains the accept, deny, or error status and the reason for deny or error. It also contain the used lease length that is at least as large as the provided value.

**QoS-Release**

The *QoS-Release* message causes the EAC to release the capacity that is reserved from the TIM.

**QoS-Release-Answer**

This reply to the *QoS-Release* message contains accept, or error status and the reason for an error.
Deployment

QoS-Refresh
The QoS-Refresh message causes the EAC to refresh the lease on the context and its reserved capacity. If this message is not received before the lease expires, the EAC possibly recoup the capacity from the TIM. Any subsequent message referencing the context are responded to with an error status.

QoS-Refresh-Answer
This is the reply to the QoS-Refresh message. It contains accept, deny, or error status as well as any reason for deny or error.

Signaling Interface Function
The Signaling Interface Function (SIF) interacts with a deployment specific signaling protocol and converts it into the messages appropriate to the ACF.

Session Awareness Function
The Session Awareness Function (SAF) interacts with a deployment specific external interface to gain session awareness capability and convert this into interaction with the other interfaces, specifically the SSF. Currently, this is a manual provisioning step.

Session Store Function
The Session Store Function (SSF) encompasses some simple storage concepts, such as the ability to create, update, remove, and obtain session information.

Context Store Function
The Context Store Function (CSF) encompasses some simple storage concepts, including, the ability to create, update, remove, and obtain context and media flow information.

Context Timer Function
The Context Timer Function (CTF) is responsible for performing soft-state maintenance.
Applications

Overview

The Edge Admission Control (EAC) allows service providers to deliver dynamic, Capacity Admission Control (CAC) applications, including the following:

- Edge Voice for Broadband (IETF SIP VOIP CAC)
- Video-on-Demand (Video CAC)

The Broadband Policy Manager (BPM) integrates the applications with relevant application servers, such as Session Initiated Protocol (SIP) servers or video middleware. CAC bases decisions on calculated link capacity values that are stored in a database. When signaled with changes that have occurred in the access or core configurations, the database is updated.

The EAC solution targets Telephony Capacity Admission Control (CAC) for the access network connected via a core network in which only the access network contains tracked capacity resources.

Edge Voice for Broadband

This section depicts a brief edge voice scenario.
How It Works

1. Voice over Internet Protocol (VoIP) calls are signaled to the SoftSwitch component.

2. The SoftSwitch requests that the Quality of Service (QoS) server reserve the bandwidth within the underlying network to accept the call request.

3. The EAC inspects the call source and destination addresses and performs an admission control function. When one, or both, addresses are served through the broadband network, the QoS sever determines if sufficient bandwidth is available within the virtual circuit (VC) and virtual path (VP) assigned priority queue (PQ).

4. If both conditions are positive, the admission request is successful. When both addresses are connected to the broadband infrastructure, both ends of the call are checked before the call request is accepted.

5. The EAC signals the SoftSwitch to permit the call setup.

Access Methods

Telephony CAC uses the access network connected via a core network in which only the access network contains tracked capacity resources. In the sample topology, a BRAS contains multiple ports, and each port contains multiple VPs, each of which contains multiple VCs. The VC represents a hard line into a customer premises. The Customer Premises Equipment (CPE) is uniquely identified by BRAS-Port-VPI-VCI.
Video on Demand

This section depicts a video-on-demand scenario.

How It Works

1. A subscriber has a high-speed Internet (HSI) session, which uses his available bandwidth (six megabits).
2. The subscriber requests a VoD session that requires two megabits.
3. The VoD request travels from the subscriber set-top-box (STB) to VoD middleware.
4. VoD middleware issues a request to the policy control layer.
5. The policy control layer performs an admission control decision.
6. The system checks the number of active sessions of the subscriber.
7. The system determines whether the transport network has enough bandwidth available to support the request.
8. If the subscriber has the capacity to open another session and the network has the appropriate bandwidth available, the system dynamically reallocates network resources to allow the video session.
9. The system reduces the HSI session bandwidth to four megabits
10. The system allocates two megabits of bandwidth for the video session.
11. The system sends an acceptance message to the VoD middleware server to initiate the session.
12. When the session is complete, the system sends an updated accounting record to the appropriate devices.

Access Methods

The core bandwidth management application is integrated with Cisco GSR and CRS-1 products and competitive router products. CAC supplies management of multivendor metro and core NGN network components.
Figure 5-1 provides an outline of the architecture. The architecture supports a variety of multimedia devices in the home network that support SIP signaling. This can include multimedia conferencing software on the PC; an IP Phone; IP Voice software on a PDA, a television or STB; a video conferencing system, or any variety of SIP-based communication clients.

Figure 5-1. Architecture Outline

IP-based video-on-demand allows a subscriber to start, stop, and resume videos interactively. He can download content onto a personal video recorder, where he can view the content from a local cache or from a dedicated unicast stream from a video server with play, stop, and resume controls.
The video client STB is attached directly to the subscriber television. The video client can also a software-based client on a PC, PDAc, or cellular phone. The client interacts with a video middleware component that provides stream information and processes the remote control commands: play, pause, and stop. The middleware also interacts with the defined VODS, which streams the content to the subscriber.

**Figure 5-2. Client Interacting with Middleware**

Voice services are no longer the sole domain of incumbent telecommunication carriers; video services, the eminent rule of cable providers; or mobility, the stronghold of wireless providers. IP networks are the catalyst for a new world of communications and entertainment services. To succeed, service providers are moving from the network transport-focused business model, where the bandwidth is the service, to an application- and solution-provider business model that offers secure, easy, access to quality-assured applications and services that are available anywhere, anytime.

Next-generation IP networks focus on converging voice, video, and data applications onto one, unified, IP service-delivery platform that provides next-generation network services, such as VoIP, Internet Protocol Television (IPTV), video-on-demand (VoD), and other collaborative applications.
## Appendix A - Glossary

### A

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>In a pair of BPMs, this is the BPM actively processing requests.</td>
</tr>
<tr>
<td>AE</td>
<td>Application Environment.</td>
</tr>
<tr>
<td>Agent</td>
<td>An internal PCS component that interacts with a device. The user creates</td>
</tr>
<tr>
<td></td>
<td>and configures it to interact with a specific device by indicating the</td>
</tr>
<tr>
<td></td>
<td>device type, IP address, and port number. The user then assigns the agent</td>
</tr>
<tr>
<td></td>
<td>to perform service functions.</td>
</tr>
<tr>
<td>Agent Configuration</td>
<td>Agent information that comprises a specific agent type instance. For</td>
</tr>
<tr>
<td></td>
<td>example, a RADIUS agent configuration contains appropriate IP address,</td>
</tr>
<tr>
<td></td>
<td>port, and shared secret values for a RADIUS agent type.</td>
</tr>
<tr>
<td>Agent Function</td>
<td>See Function.</td>
</tr>
<tr>
<td>Agent Instance</td>
<td>A running instance of an agent type.</td>
</tr>
<tr>
<td>Agent Package</td>
<td>Software that allows agents to interact with a particular device type.</td>
</tr>
<tr>
<td></td>
<td>For example, a RADIUS agent package contains software that allows the PCS</td>
</tr>
<tr>
<td></td>
<td>user to create agents that interact with specific RADIUS devices.</td>
</tr>
<tr>
<td>Agent Type</td>
<td>The agent type describes a particular type of agent that you can load onto</td>
</tr>
<tr>
<td></td>
<td>the system. You select the agent type when you create the agent instance.</td>
</tr>
<tr>
<td>API</td>
<td>Application Program Interface.</td>
</tr>
<tr>
<td>Application</td>
<td>A service that maps business models and operational procedures directly</td>
</tr>
<tr>
<td></td>
<td>into IP services, executable by their customers, for example, video on</td>
</tr>
<tr>
<td></td>
<td>demand or automatic backup. See also Service.</td>
</tr>
<tr>
<td>Application Program</td>
<td>API.</td>
</tr>
<tr>
<td>Interface</td>
<td>Application Service Provider.</td>
</tr>
<tr>
<td>ASP</td>
<td></td>
</tr>
<tr>
<td>Glossary</td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td></td>
</tr>
<tr>
<td>ASP</td>
<td>Application Service Provider.</td>
</tr>
<tr>
<td>Asynchronous Transfer Mode</td>
<td>ATM.</td>
</tr>
<tr>
<td>ATM</td>
<td>Asynchronous Transfer Mode.</td>
</tr>
<tr>
<td>Attribute</td>
<td>In the BPDS Object manager tool, a simple type with a default value. An object can have several attributes.</td>
</tr>
</tbody>
</table>

**B**

| Backend | Software that runs on the BPM. It comprises the controller, engine, agent host, activation daemon, and scheduler processes; synonymous with BPM. |
| BGP     | Border Gateway Protocol. |
| Border Gateway Protocol | BGP. An exterior gateway routing protocol that enables groups of routers to share routing information to establish efficient, loop-free routes. BGP is commonly used within and between Internet Service Providers (ISPs). |
| BPDS    | Broadband Policy Design Studio. |
| BRAS    | Broadband Remote Access Server. |

**C**

<p>| CAC      | Call Admission Control |
| Call Admission Control | CAC |</p>
<table>
<thead>
<tr>
<th><strong>Class of Service</strong></th>
<th>CoS. A traffic prioritization scheme that enables more predictable traffic delivery, based on application requirements.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Client</strong></td>
<td>Generic term that denotes the BPM BPDS application.</td>
</tr>
<tr>
<td><strong>CoS</strong></td>
<td>Class of Service.</td>
</tr>
<tr>
<td><strong>CPE</strong></td>
<td>Customer premises equipment.</td>
</tr>
<tr>
<td><strong>CLI</strong></td>
<td>Command line interface.</td>
</tr>
<tr>
<td><strong>Cluster</strong></td>
<td>A pair of cooperating and redundant BPMs.</td>
</tr>
<tr>
<td><strong>Component</strong></td>
<td>An object comprising data and code. A component provides a well-specified set of publicly available services. All devices, services, and applications on a network are components.</td>
</tr>
<tr>
<td><strong>Configuration</strong></td>
<td>Information necessary to construct an instance of a type (agent, service).</td>
</tr>
<tr>
<td><strong>Controller</strong></td>
<td>A software element that runs on the BPM and controls various elements of the backend. Usually only one controller exists per backend; therefore, from the BPDS perspective, the controller is the backend.</td>
</tr>
<tr>
<td><strong>Customer Premises Equipment</strong></td>
<td>CPE.</td>
</tr>
<tr>
<td><strong>D</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Deep Packet Inspection Protocol</strong></td>
<td>DPI.</td>
</tr>
<tr>
<td><strong>Device</strong></td>
<td>Any piece of software or hardware connected to a network. RADIUS servers, routers, billing systems, accounting systems, and video servers are devices. An agent communicates with a device.</td>
</tr>
<tr>
<td><strong>Device Rule</strong></td>
<td>A generic task that can be applied to a device that supports the device rule functionality to carry out a network action. Device rules can retrieve information from connected devices. See also Device Type and Policy Rule.</td>
</tr>
<tr>
<td><strong>Device Type</strong></td>
<td>A classification of actual devices, based on device attributes, such as vendor, model, hardware version, and software version. See also Device Rule.</td>
</tr>
<tr>
<td><strong>Domain</strong></td>
<td>One or more cooperating Policy Control System (PCS)s managed by a single domain repository.</td>
</tr>
<tr>
<td><strong>Glossary</strong></td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td></td>
</tr>
<tr>
<td><strong>Domain Controller</strong></td>
<td>The software that stores and manages agents, agent types, agent instances, service types, services instances packages, service engines, policy engines, and clusters; also known as the Cisco database.</td>
</tr>
<tr>
<td><strong>Domain Data</strong></td>
<td>Data maintained about the elements in a domain; for example, controller host and port configuration, database host and port information, agent and service configuration and deployment information.</td>
</tr>
<tr>
<td><strong>Domain Repository</strong></td>
<td>The master database that contains configuration information for each domain element.</td>
</tr>
<tr>
<td><strong>DPI</strong></td>
<td>Deep Packet Inspection Protocol.</td>
</tr>
<tr>
<td><strong>DSLAM</strong></td>
<td>Digital Subscriber Line Access Multiplexer.</td>
</tr>
<tr>
<td><strong>Element</strong></td>
<td>An object with the BPM: Cisco package; agent configuration; service instance; shared object.</td>
</tr>
<tr>
<td><strong>Enumeration</strong></td>
<td>In the BPDS Object manager tool, enumeration is contained within a simple type.</td>
</tr>
<tr>
<td><strong>Field Replaceable Unit</strong></td>
<td>FRU. An FRU represents an element (e.g., entire system, BPDS client software, agent) within the Policy Control System (PCS) that can have a version associated with it. A FRU is a subset of an element.</td>
</tr>
<tr>
<td><strong>Flow</strong></td>
<td>The movement of data or control between agents. It is a collection of one or more operators and zero or more routes. The designer uses flows to define services and applications.</td>
</tr>
<tr>
<td><strong>FRU</strong></td>
<td>Field Replaceable Unit.</td>
</tr>
<tr>
<td><strong>Function</strong></td>
<td>The element that performs an operation, based on inputs and returns the results of the operation via its outputs. The user drags and drops a function into a flow in the BPDS. An agent, which interacts with a device, performs the actual operation.</td>
</tr>
<tr>
<td><strong>GUI</strong></td>
<td>Graphical User Interface (BPDS).</td>
</tr>
<tr>
<td><strong>Head Version</strong></td>
<td>The latest version of an element.</td>
</tr>
</tbody>
</table>
Hot Backup | A backup system, identical in configuration to the primary BPM system. The hot backup is ready to resume request execution immediately if the primary BPM system fails. See Primary BPM, Secondary BPM.

ILC | Appium SOAP load balancer.

Implementation | An instruction set for executing a specification.

Install Rule |  

Instance | An executing type (agent, service), created from a specification, implementation, and configuration. An agent instance is a specific implementation of that agent type.

Interface | A collection of functions.

Internet Subscriber Gateway | ISG

IP address | The address that identifies a computer. The IP address format is a 32-bit numeric address written as four numbers (0 to 255) separated by periods.

ISG | Internet Subscriber Gateway

ISP | Internet Service Provider.

JDBC™ | Java Database Connectivity (TM of Sun Microsystems; not an acronym).

L2TP | Layer Two (2) Tunneling Protocol.

Management Protocol | A set of protocols for managing devices and networks, for example SNMP, SSH.

Master | In a pair of BPMs, the BPM that actively processes requests. Also known as the primary BPM.

Metadata | In the BPDS Object Manager tool, the data structure. Cisco customers can import metadata to invoke a structure for their database.

MPLS | Multiprotocol Label Switching.
<table>
<thead>
<tr>
<th>Glossary Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiprotocol Label Switching</td>
<td>An IETF initiative that integrates Layer 2 information about network links (bandwidth, latency, utilization) into Layer 3 (IP) within a particular autonomous system or ISP. It simplifies and improves IP-packet exchange and gives network operators the flexibility to divert and route traffic around link failures, congestion, and bottlenecks.</td>
</tr>
<tr>
<td>N</td>
<td>The ability for service engines to use one service engine as a backup.</td>
</tr>
<tr>
<td>NAS</td>
<td>Network Attached Storage.</td>
</tr>
<tr>
<td>NAV</td>
<td>The Network Admin view of the PCS VDS.</td>
</tr>
<tr>
<td>Network</td>
<td>Loosely coupled set of components.</td>
</tr>
<tr>
<td>Network Attached Storage</td>
<td>NAS.</td>
</tr>
<tr>
<td>Network Device Library Entry</td>
<td>An entry that properly configures a network device for applying a network policy.</td>
</tr>
<tr>
<td>Network Event</td>
<td>Contained within a profile, a set of install and uninstall rules performed in sequence.</td>
</tr>
<tr>
<td>Network Policy</td>
<td>A device rule entry, where the device rule contains commands to configure a network device to apply a network policy. See also Device Rule, Policy Rule.</td>
</tr>
<tr>
<td>Network Provisioner</td>
<td>A Cisco system on the wholesale side of a wholesale/retail network.</td>
</tr>
<tr>
<td>NP</td>
<td>Network Provider.</td>
</tr>
<tr>
<td>O</td>
<td></td>
</tr>
<tr>
<td>Object</td>
<td>An agent, controller, function, service, switch, or service within the Policy Control System (PCS).</td>
</tr>
<tr>
<td>Object Dependency</td>
<td>An exact object type, for example a Cisco 2500 router agent, that a service depends on. The user adds the object type to the dependency list of the service. All Interfaces supported by the object type are then available for use with the service.</td>
</tr>
<tr>
<td>Object Type</td>
<td>In the BPDS Object manager tool, object type is defined with attributes. It can own contain, and associate with other object types.</td>
</tr>
<tr>
<td>OC</td>
<td>Orchestration Controller. That portion of the Policy Control System (PCS) that controls processes such as username and password authentication,</td>
</tr>
<tr>
<td>Operation and Support Systems</td>
<td>OSS.</td>
</tr>
<tr>
<td>Operator</td>
<td>A representation of actions to be undertaken on a system networked to a Policy Control System (PCS).</td>
</tr>
<tr>
<td>----------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Orchestrated Controller</td>
<td>Orchestration Controller (OC). See Domain Controller.</td>
</tr>
<tr>
<td>Orchestrated Network</td>
<td>The process for handling service calls over a network. It defines the flow of control and information between work units.</td>
</tr>
<tr>
<td>OSS</td>
<td>Operation and Support Systems.</td>
</tr>
<tr>
<td>P</td>
<td></td>
</tr>
<tr>
<td>Pad</td>
<td>A collection of pins on an operator. This appears as a box along the edge of an operator.</td>
</tr>
<tr>
<td>BPM</td>
<td>Broadband Policy Manager.</td>
</tr>
<tr>
<td>PDP</td>
<td>Policy Decision Point.</td>
</tr>
<tr>
<td>PE</td>
<td>Policy Engine. The software that stores and manages user profile information, subscriber access records, policy rules; also known as the policy database.</td>
</tr>
<tr>
<td>PEP</td>
<td>Policy Enforcement Point.</td>
</tr>
<tr>
<td>Pin</td>
<td>An input or output from an operator. The pin serves as a route endpoint and holds a single input or output value. For example, an operator that needs a username and password as input has two input pins; one for the username; the other, the password.</td>
</tr>
<tr>
<td>PM</td>
<td>Policy Manager.</td>
</tr>
<tr>
<td>Point-to-Point Protocol Over ATM</td>
<td>PPPoA</td>
</tr>
<tr>
<td>Point-to-Point Protocol Over Ethernet</td>
<td>PPPoE</td>
</tr>
<tr>
<td>Point-to-Point Protocol Over Ethernet Over ATM</td>
<td>PPPoEoA</td>
</tr>
<tr>
<td>Point-to-Point Termination Aggregation</td>
<td>PTA</td>
</tr>
</tbody>
</table>

Version 1.5 | Broadband Policy Manager User Guide to Applications | 57 of 63
## Glossary

**Policy**  
A flow comprising a rule or set of rules that take a specific action provided by an ISP for its subscribers. For example, a policy for subscriber access directs how the system identifies a user via User ID, access type, and log in location. A policy performs an operation, based on input and returns the results of its action as output.

**Policy Database**  
The database of policy objects that services access to make policy decisions.

**Policy Decision Point**  
PDP.

**Policy Enforcement Point**  
PEP.

**Policy Engine**  
PE. The software that stores and manages user profile information, subscriber access records, policy rules; also known as the policy database.

**Policy Function**  
Policy rules encapsulated in a Tcl agent `execute` function.

**PPPoA**  
Point-to-Point Protocol Over Asynchronous Transfer Mode.

**PPPoE**  
Point-to-Point Protocol Over Ethernet Over Asynchronous Transfer Mode.

**PPPoEoA**  
Point-to-Point Protocol Over Ethernet Over Asynchronous Transfer Mode.

**PR**  
Policy Repository.

**Primary BPM**  
In a pair of BPMs, the primary BPM is processing requests. If the primary fails, the secondary becomes the primary.

**Profile**  
A sequence of network events involved in creating and taking down a network session for a subscriber.

**Property**  
The parameter or characteristic of an agent or device.

**PTA**  
Point-to-Point Termination Aggregation.

**R**  
Remote Authentication Dial-In User Service.

**Raw Data Record**  
RDR.

**RDR**  
Raw Data Record.
| **Remote Authentication Dial-in User Service** | RADIUS. A client/server protocol enabling remote access server communication with a central server to authenticate dial-in subscribers and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. |
| **Remote Method Invocation** | (RMI) |
| **RMI** | Remote Method Invocation |
| **Role-based Dependency** | A dependency in which a user indicates that multiple service elements support the same interface. The user defines different roles and assigns the required service interfaces to each. The different roles are added to the dependency list for the service and operators are clearly marked to indicate their assigned role. |
| **Route** | A path between operators. |
| **RS** | Remote Server. |
| **Rule** | Criteria applied to the objects and methods of a business system to determine how objects and methods are used by, or for, a given system user. A flow comprises a rule or set of rules. Rules prescribe terms and conditions for a specific action provided by an ISP for its subscribers. One rule can call another rule. |
| **S** | |
| **SAV** | The Service Admin view of the BPM BPDS. |
| **Schema** | A set of rules and syntax for storing data. |
| **SDV** | The Service Design view of the BPM BPDS. |
| **SE** | Service Engine. |
| **Secondary BPM** | In a pair of BPMs, the secondary BPM does not process requests. Instead, it monitors the health of the primary to assess its ability to process requests. If the primary is not viable, the secondary becomes the primary. |
| **Service** | An application, created by the PCS user, that maps business models and operational procedures directly into IP services, executable by their customers, for example, video on demand or automatic backup. A service comprises objects (agent, controller, function, switch, or other service). A service comprises one or more flows. |
| **Service Configuration** | The information needed to construct a service. The service configuration specifies agent configurations for each function in the service type. The BPM user creates the service configuration. |
### Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Dependency</td>
<td>The user-defined dependencies of a service. The user builds a service by defining data-flows that use operators from multiple objects, including agents and other services. The user builds a service upon a concrete set of agents and services. If a service is portable across different agents and services, the user specifies any constraints on the concrete instances and specifies the interfaces that those concrete instances must support.</td>
</tr>
<tr>
<td>Service Engine</td>
<td>SE. The software that runs services; also known as the backend.</td>
</tr>
<tr>
<td>Service Interface Dependency</td>
<td>If a service uses a particular service interface, but does not require that a specific object provide the service interface, the user can add the service interface as a dependency. Here, the service interface operators are available for use in the current service, but the object that provides the interface is determined later.</td>
</tr>
<tr>
<td>Service Instance</td>
<td>The running of a service type created by the end user.</td>
</tr>
<tr>
<td>Service Palette</td>
<td>The agent types available to a service.</td>
</tr>
<tr>
<td>Service Profile</td>
<td>A collection of services and information about service execution.</td>
</tr>
<tr>
<td>Service Provisioner</td>
<td>SP. A Cisco appliance on the retail side of a wholesale/retail network.</td>
</tr>
<tr>
<td>Service Type</td>
<td>The definition of what agent types are required for a service; the defined flow of data between functions of agent types. The end user or PCS staff creates the service type.</td>
</tr>
<tr>
<td>Servlet</td>
<td>An applet that runs on a server. Usually refers to a Java applet that runs within a Web server environment. Analogous to a Java applet that runs within a Web browser environment.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>An authentication string that ensures security between devices. KERBEROS is an instance of a shared-secret authentication protocol.</td>
</tr>
<tr>
<td>Simple Type</td>
<td>In the BPDS Object manager tool, a simple type is similar to data type, except it can express with enumerations.</td>
</tr>
<tr>
<td>Simple Network Management Protocol</td>
<td>SNMP. An IETF protocol by which networked devices can be periodically polled for information as part of a network management system.</td>
</tr>
<tr>
<td>SLA</td>
<td>Service Level Agreement.</td>
</tr>
<tr>
<td>SP</td>
<td>Service Provider.</td>
</tr>
<tr>
<td><strong>SPACE-P</strong></td>
<td>Space Provisioning.</td>
</tr>
<tr>
<td><strong>Specification</strong></td>
<td>A type definition that includes interface definitions, configuration schemas, and binding information.</td>
</tr>
<tr>
<td><strong>SQL</strong></td>
<td>Structured Query Language.</td>
</tr>
<tr>
<td><strong>Structured Query Language</strong></td>
<td>SQL.</td>
</tr>
<tr>
<td><strong>Subscriber</strong></td>
<td>A customer of a business that provides a wide variety of online services, including e-mail, stock quotes, news, and online forums.</td>
</tr>
<tr>
<td><strong>Subscriber Profile</strong></td>
<td>A table entry containing information, such as authentication, authorization, and location on a specific subscriber.</td>
</tr>
<tr>
<td><strong>Super Operator</strong></td>
<td>A reusable flow that other flows can call. To the other flows, the super operator appears as an operator that they can call and insert on any route.</td>
</tr>
<tr>
<td><strong>Switch</strong></td>
<td>A device that filters and forwards packets between LAN segments. Switches operate at the data link layer and the network layer of the OSI Reference Model.</td>
</tr>
</tbody>
</table>

**T**

| **TER** | Transaction Event Record. |
| **TM** | Traffic Management (TM). |
| **TOS** | Type of Service. |
| **Traffic Management** | TM. |
| **TRPC** | Transaction Remote Procedure Call. |
| **Type** | A PCS component group that has a unique specification. It may have an implementation, and it may have one or more configurations and instances. |

**U**

| **UML** | Unified Modeling Language. UML is the industry standard notation for representing software architecture and design models. |

**V**

<p>| <strong>VC</strong> | Virtual Circuit. |</p>
<table>
<thead>
<tr>
<th><strong>Glossary</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BPDS</strong></td>
</tr>
<tr>
<td><strong>VLAN</strong></td>
</tr>
<tr>
<td><strong>Voice-over-Internet Protocol</strong></td>
</tr>
<tr>
<td><strong>VoIP</strong></td>
</tr>
<tr>
<td><strong>VP</strong></td>
</tr>
<tr>
<td><strong>VPN</strong></td>
</tr>
<tr>
<td><strong>W</strong></td>
</tr>
<tr>
<td><strong>Workspace</strong></td>
</tr>
<tr>
<td><strong>WSA</strong></td>
</tr>
</tbody>
</table>
Index

A
access 45
accounting
   log 31
   record 47
Accounting Log Function 31
ACF 29
Admission Control Function 29
ALF 31
architecture 8
   ETSI/TISPAN 5
   outline 2
   preferred 8
   RACS 5
   service delivery 5
   VOIP 2
ATM 12

B
BPM 1
BRAS 5, 8, 12, 13, 15
Broadband Policy Manager 1

C
CAC 1, 25, 45, 47
Capacity Admission Control 1
Context Timer Function 30
CTF 25, 30, 31, 42

D
DSLAM 5, 7, 12, 13, 14, 15

E
Edge 23
ETSI 4, 23, 30
European Telecommunications Standards Institute 23
European Telecommunications Standards Institute (ETSI)/Telecommunications 4
Index

G
glossary 51

I
Internet Services and Protocol for Advanced Networking (TISPAN) 4
IP services
  subscriber-based 1

N
NGN 4, 47

P
Path 40
  Path Computation Function 28
  PCF 17, 25, 28, 29, 34, 40
  PCR 8
  peak cell rate 8
  PQ 8, 12, 46
  priority queue 8, 46

Q
Quality of Service 8

R
RACS framework 4
  RCF 31
  Response Cache Function 31
  RFC 3665 2

S
SAF 30
  Session Awareness Function 30
  Session Store Function 30
  SF 32
  SIF 29
  Signaling Interface Function 29
  SIP signaling 2
  SSF 30
  Statistics Function 32
  subscriber-based 1
  subscriber-based IP services 1

T
TAF 27
  Telecommunications and Internet Services and Protocol for Advanced Networking 23
  TIM 11, 28
  TISPAN 4, 5, 23, 30
Index

Topology Awareness Function 27
Topology Information Model 11, 28
Topology Store Function 28
TSF 28

V
VC 7, 12, 15
Video 1
Video-on-Demand 2, 3
Virtual Circuit 7
virtual node 13
Virtual Path 7
Voice 1, 2
VP 7, 12, 15