Cisco Broadband IP Service Module User Guide

Software Release 1.6
December 22, 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

Customer Order Number:
Text Part Number:

Cisco Broadband IP Service Module User Guide

Contents

Preface

Overview

This document discusses the Broadband IP Service Module offering. It discusses its components and architecture.

Audience

This guide is for the network professional who handles the IP Service Module.

Organization

This document contains three chapters and one appendix:

- Chapter 1 - Introduction
- Chapter 2 - Session Manager
- Chapter 3 - Network Manager
- Chapter 4 - Deployment
- Appendix A - Glossary

Documentation Set

The documentation for your Broadband Policy Manager (BPM) system includes the following documents:

- Cisco Broadband IP Service Module User Guide
- Cisco Broadband Policy Design Studio User Guide
- Cisco Broadband Policy Manager Installation and Configuration Guide
- Cisco Broadband Policy Manager Operations Guide
- Cisco Broadband Policy Manager Release Notes
- Cisco Capacity Admission Control Manager User Guide

Cisco Broadband IP Service Module User Guide

This document discusses the Broadband IP Service Module for session management and network adaptation. It discusses its architecture, components, access methods, and functions.

Cisco Broadband Policy Design Studio User Guide

This guide provides instructions for installing the Broadband Policy Design Studio (BPDS). It discusses how to use the BPDS to create, deploy, and manage network services and topologies.

Cisco Broadband Policy Manager Installation and Configuration Guide

This guide describes how to install the software for the BPM. It describes how to install and configure the Solaris operating system for use by the BPM. It also includes procedures to install and configure the BPM software and the procedures to install and log into the BPDS.

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. These tasks include use of the Log Messages addendum, the Application Log Messages addendum, and the Statistics addendum.

Cisco Broadband Policy Manager Release Notes

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

Cisco Capacity Admission Control Manager User Guide

This document discusses the architecture and components for the Capacity Admission Control Manager product.

Conventions

This guide may use the text and icon conventions described in this section.

Text

The table below contains documentation text conventions.

Table 1. Text Conventions

Convention	Explanation	Example
alternate mouse button	Usually indicates the right mouse button.	Click the agent with the alternate mouse button.
arrow **-->**	Indicates the selection order of menu items.	**File --> Save** This indicates go to the File menu and choose the Save function.
bar brackets [ ]	Indicate the default.	Choose your Name Service type [2]: This indicates the default is *2*.
bold	Indicates user input or button selection.	**poweron**
bold italic	Indicates objects, attributes, pin names, and service flows.	Right-click the ***request*** function.
Ctrl+X	Indicates the quick access key for a menu option.	Ctrl+M This indicates open the Object Manager.
default mouse button	Usually indicates the left mouse button.	Click the agent with the default mouse button.
italic	Indicates an application, chapter, directory, document, header, section, or title names.	For more information, refer to the section entitled *Creating Services*.
<KEYNAME>	Indicates press the named key.	Supply the required information, then press the <ENTER> key.
`screen display`	Represents system output.	`This agent does not have any agent-specific properties.`

Icons

The following icon conventions provide additional information to indicate special conditions or possible risks:

Note: *A note is an informational message containing a tip or suggestion.*

Caution: *A caution indicates a risk of damage to equipment or a loss of data.*

1

Introduction

Overview

The IP Service Module comprises the Session Manager (SM) and the Network Manager (NM) packages. The SM and the NM products run on the Resource Controller Broadband Policy Manager (BPM) system. The Resource Controller tracks resource utilization for the system. Each Resource Controller tracks the resources of a subset of the network topology.

Session Manager

The Session Manager (SM) product tracks user sessions connecting to the broadband access network. The SM product allows the addition of per-subscriber session management storage capability to a policy control solution. It also mapping of subscribers to physical network devices and ports and provides valuable information to the topology information model. The SM product can be integrated with the NM product.

Network Manager

The Network Manager (NM) product provides facilities for controlling and querying network elements. The NM product offers a variety of interfaces, including Netconf, SNMP, and RADIUS COA. It can be deployed with the SM product. Its processes systematically modify the properties of the underlying network elements as part of the execution of policies from a policy control system perspective. The system offers a variety of interfaces for this including Netconf (CLI) and RADIUS COA. The Network Manager product also provides an Application Programming Interface (API). The API allows applications to apply stateful profiles to sessions in the network.

BPM

The Broadband Policy Manager (BPM) consists of visual development, deployment manager, and execution environments that provide an architecture for service-oriented systems. The BPM simplifies the repeated production of related solutions for real-time network policy management.

BPDS

In the BPM architecture, dataflow programming promotes the data movement and transformation in program execution. The Broadband Policy Design Studio (BPDS), graphical user interface (GUI) facilitates these tasks for the service designer and network administrator. Using the BPDS, the service designer develops programs interactively using drag-and-drop visual programming. The programs move data between operators that are exposed by software agents. The agents encapsulate specific implementations protocols, network devices, data sources, or logic capabilities. The designer can combine the programs into collections of services, referred to as applications, which provide complete solutions. The network administrator publishes these applications in the execution environment.

Execution Environment

The execution environment is a distributed domain of networked processing nodes. A node is a computer, or other device or system on a network with a unique network address. A link is a line or channel between the nodes, over which data is transmitted. Information resources can be attached to a node to describe its capabilities.

A resource is any device or other item that can be used. Devices such as printers and disk drives are resources. Memory is also a resource. In many operating systems, a resource is specifically data or routines that are available to programs. These are also called system resources. Resources (information) can also be attached to a link to describe, for example, its bandwidth capabilities or delay properties.

Each node runs a highly concurrent graph-traversal engine, coupled with a fast data switching fabric. Once published to an execution environment on a node, application services are available for execution and monitoring. The execution environment also provides resiliency and failover capabilities.

BRAS Resiliency

A resiliency mechanism on the Resource Controller system ensures that both the *active* system and the *standby* system of a clustered Resource Controller pair can receive and process messages from external sources. The *standby* of the clustered pair establishes a connection with the database on the *active* system, allowing all of its agents and services to function. However, it uses the database on the *active* system.

System Startup Sequence

On startup, the system determines if it is a member of a cluster. If it is, it determines the role it is fulfilling, *standby* or *active*. If it is the *standby* system in the cluster pair, its agents, the Topology Store Function (TSF) and Session Store Function (SSF) agents, open connections to the policy database on the *active* system. This enables the *standby* system to remain a functioning member of the cluster, servicing requests on behalf of the *active* system, should a loss of connectivity occur between the BRAS device and the *active* system. Database communication between the standby and active systems occurs over the heartbeat link to reduce network congestion on the management, primary, and secondary network interfaces.

Join Cluster Sequence

When two systems are clustered, the *active* system remains unchanged. The *standby* system, however, is reset. This means that the agents and services of the *standby* system are undeployed. New agent and service configurations are deployed to mirror the *active* system. During this process, the agents and services start. The. *standby* system detects that it is now a member of a cluster. The sequence outlined in System Startup Sequence, above is performed.

Dissolve Cluster Sequence

During a Dissolve Cluster sequence, agents and services are also undeployed from the *standby* system. When an agent is redeployed to the former *standby* system, this sequence is identical to the System Startup sequence.

Failover Detection Sequence

The database agents (TSF, SSF) maintain a pool of persistent connections to the *active* policy database. If the standby agent detects a connection failure, it attempts to reconnect to the database. If the reconnection attempt is successful, the system writes an entry to *tazz.log*. If the reconnection attempt is not successful, the agent assumes a critical storage error exists and initiates the *connectionError* operator.

Failover Sequence

If a *connectionError* is initiated, a new flow invokes the *initiate failover* operator of the controller agent to cause the system to fail over. Additionally, the flow informs the Topology Database Server that a failover operation occurred.

System Administration

Service provider employees, the service designer and the system administrator, use the BPM product suite to create and deploy advanced services on broadband networks. The service designer develops the programs or services. The network administrator performs routine operational, maintenance, and troubleshooting tasks, including starting or stopping the BPM, monitoring status, obtaining statistics or other information, managing user access, configuring components, solving problems, and deploying the programs and services. The service designer and the network administrator can be the same employee of the service provider.

The designer and administrator use various tools to perform their tasks. These include the BPDS and a command line interface. The BPDS includes the following views:

- Network Administration screen, which shows network BPM data, including service engines, agents, and services
- Subscriber Access screen, which shows subscriber access BPM data, including access groups, access lines, administrators, network devices, policies, servers, and subscribers
- Service Design screen, which shows the structure of existing services and allows the creation of new services.

In addition, the administrator can use the *tash*, a command line interface (CLI), to directly enter certain commands. (Refer to the *Cisco Broadband Policy Manager Command Line Interface Guide*, for further details on using the CLI.)

Figure 1 presents the overall system architecture.

Figure 1. System Architecture

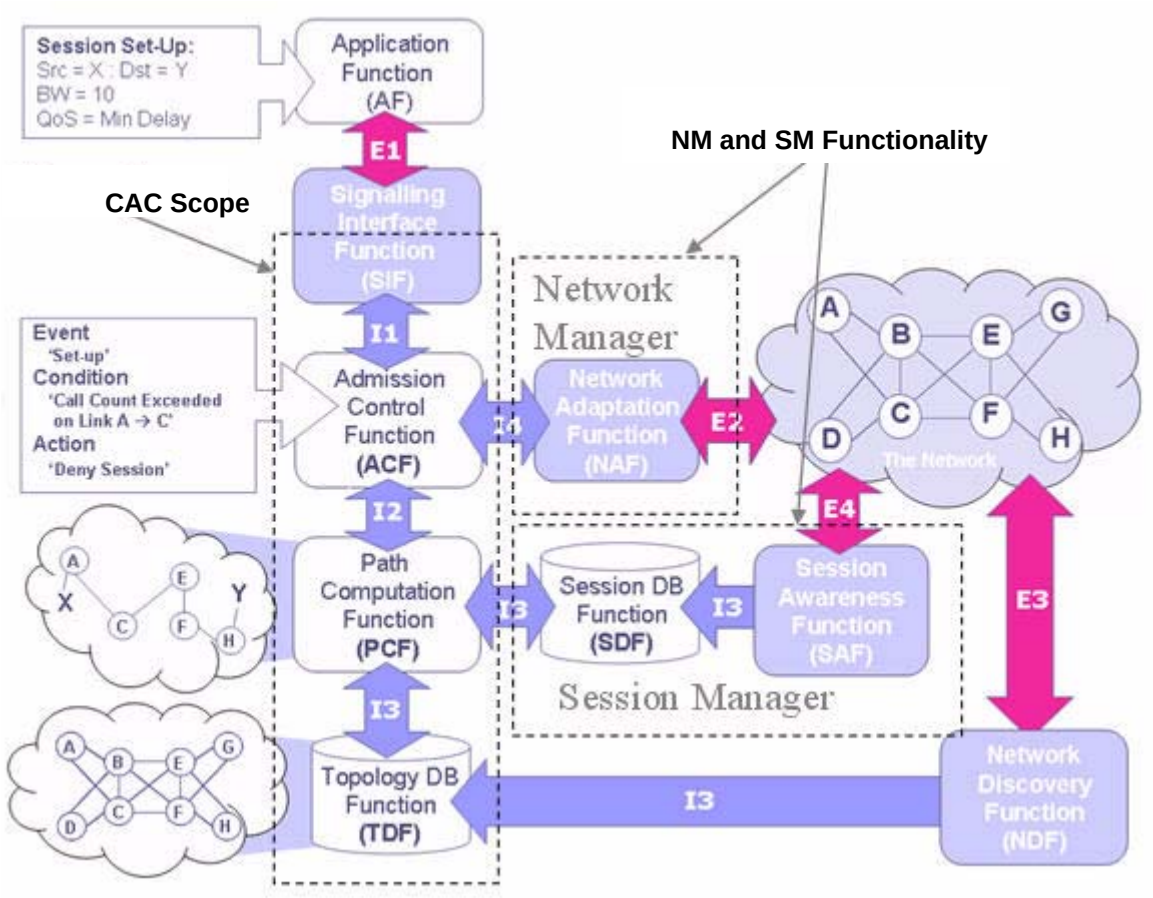
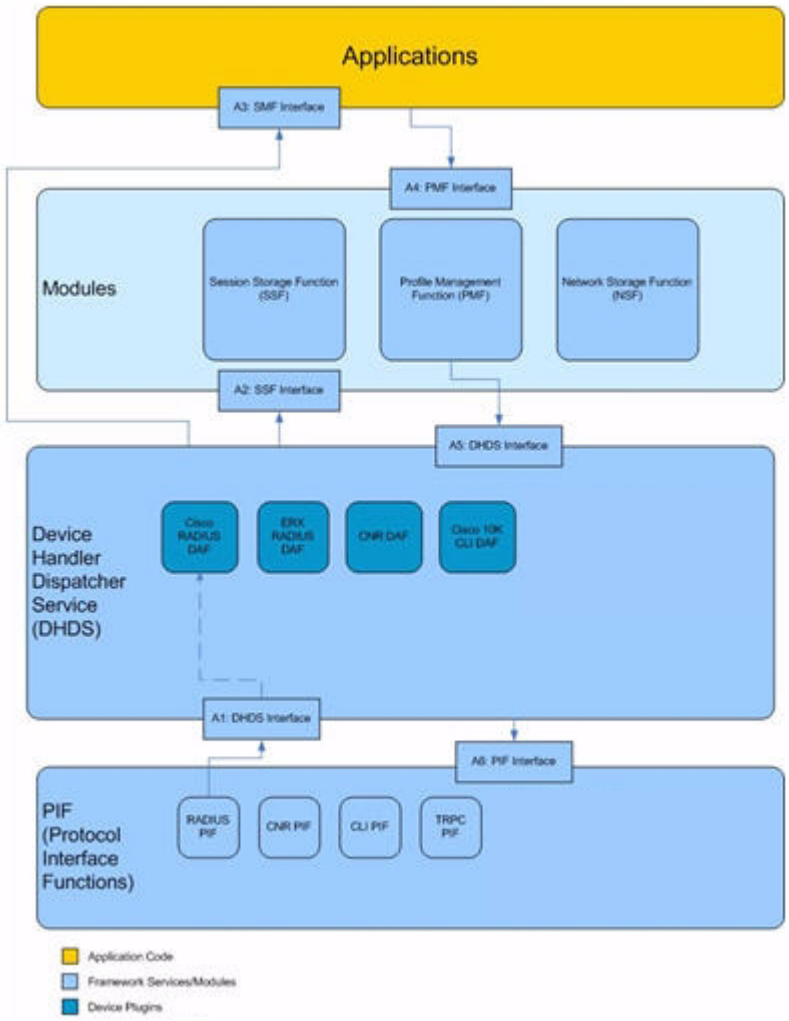


Figure 2 presents the SM and NM architecture.

Figure 2. SM/NM Architecture



2

Session Manager

Overview

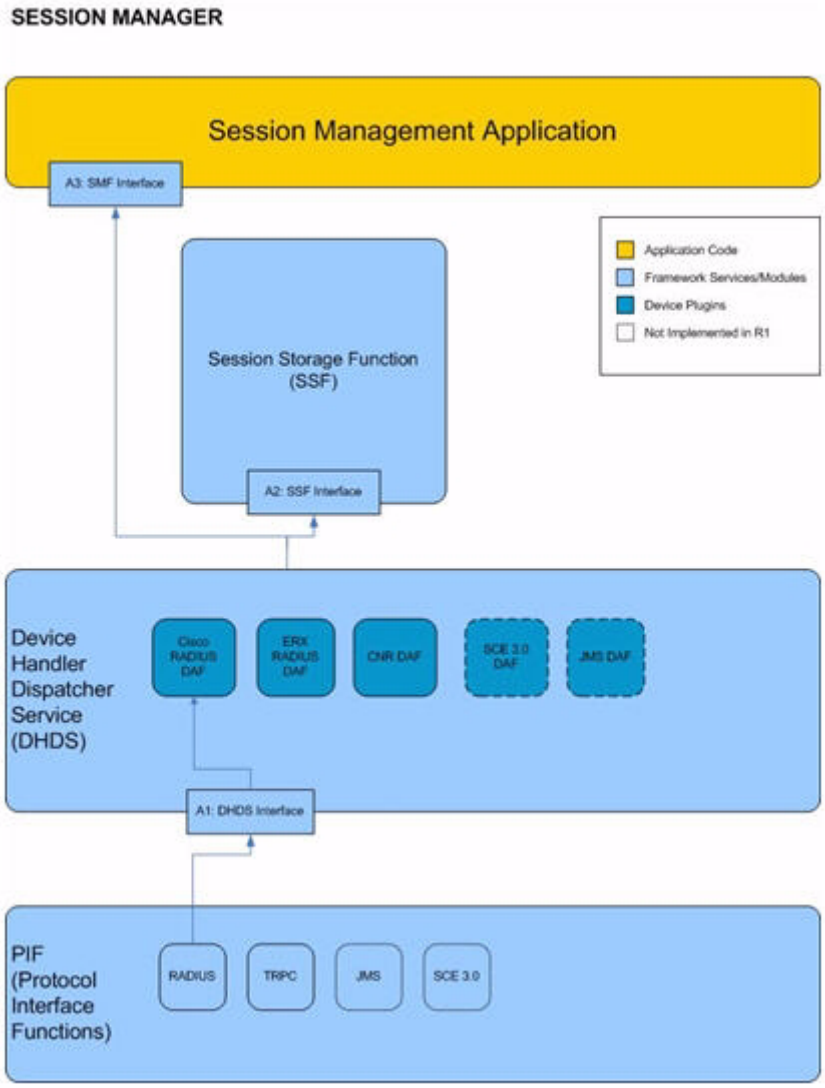
This chapter discusses the Session Manager (SM) product. It describes SM components and its architecture. The SM product uses one component specific to its functionality, a number of system module component, and a series of components shared with the Network Manager (NM) product. (See Chapter 3 for a discussion of NM components.)

The SM product controls subscriber sessions at the edge of the service provider network and can provide elements for use within the overall admission control or subscriber management framework. The SM offers allows the addition of per-subscriber session management storage capability to a policy control solution. It also allows mapping of subscribers to physical network devices and ports and provides valuable information to the topology information model.

How It Works

The SM product tracks the set of user sessions on a broadband access network. It can be deployed with the NM product. The SM product provides facilities for controlling and querying elements in the network. Figure 2-3 depicts the SM architecture.

Figure 2-3 SM Architecture



SM Components

The SM product uses the following function, which is specific to its functionality:

- Session Management Function

Session Management Function

The Session Management Function (SMF) encapsulates customer-specific business logic applied to network sessions. An SMF is abstracted from specific protocols and devices used in the network through the Device Adapter Function (DAF) and Protocol Interface Function (PIF) layers. The SMF notifies applications of session state changes.

Shared Components

The SM product uses the following components, which it shares with the NM product:

- Protocol Interface Function
- Device Adapter Function
- Device Handler Dispatch Service
- Accounting Log Function
- Statistics Function
- Alarm Notification Function

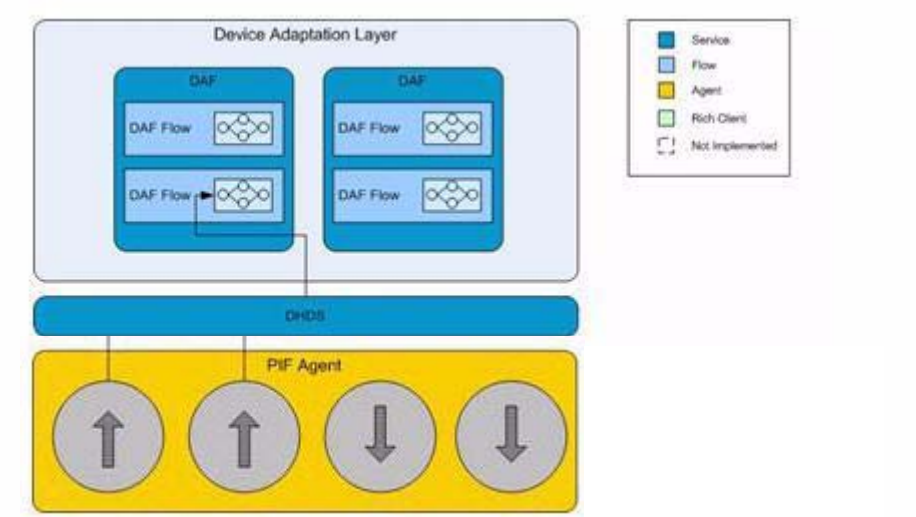
Protocol Interface Function

The Protocol Interface Function (PIF) encapsulates a protocol interface towards external systems and allows the BPM system to communicate with those systems. A PIF can act as a client, server, or peer with respect to those external systems. It standardizes the method by which new protocol interfaces are added to the system and the method by which they are managed.

Multiple PIFs can be in use at one time, and any device can have one or more associated PIFs. Multiple PIFs can be associated with a single external system. External systems use the PIF to deliver requests, queries, and notifications to the BPM. Applications within the BPM use the PIF to deliver requests, queries, and notifications to external systems. PIFs pass requests between DAF and the external systems represented by the DAFs.

Figure 2-4 presents the generic PIF architecture.

Figure 2-4 PIF Architecture



A PIF is a component that handles reading and writing of protocol messages. The interface exposed by a PIF agent is specific to the device or protocol it encapsulates. A PIF also contains a PIF service that maps triggers from the PIF agent onto the appropriate DAF for processing. The PIF Service extracts the details from the message that are required to invoke the Device Handler Dispatch Service (DHDS).

PIF Data Management

You can manage Protocol Interface Functions (PIFs) as collections of agents and flows using the Service Administration View and Network Administration View tools from the Broadband Policy Design Studio (BPDS). For further information about these administrative tools, see the *Broadband Policy Design Studio User Guide*.

PIF properties define local configuration variables that apply to a given PIF instance.

The following PIFs are available:

- Cisco Network Registrar (CNR)/TRPC Plugin PIF - This PIF receives lease statements from the Cisco CNR DHCP server.
- Telnet CLI PIF - this PIF executes Telnet CLI commands against the Cisco 10K.

Each PIF implementation has the following qualities:

- Agent required by the PIF
- Service that handles agent triggers
- Configuration properties associated with a PIF instance

Interfaces

PIF interfaces exist according to the requirements of the specific PIF.

Device Adapter Function

The Device Adapter Function (DAF) defines how events to and from PIFs are to be handled, based on the device sending or receiving the event. The DAF standardizes the modeling and management of device-specific behavior within the BPM. The DAF encapsulates a device-specific behavior. A DAF can be associated with multiple network devices. Multiple DAFs can be associated with a single network device instance. A PIF can invoke DAFs to handle an event received from an external system. Application functions can also invoke DAFs to request that actions be invoked on PIFs.

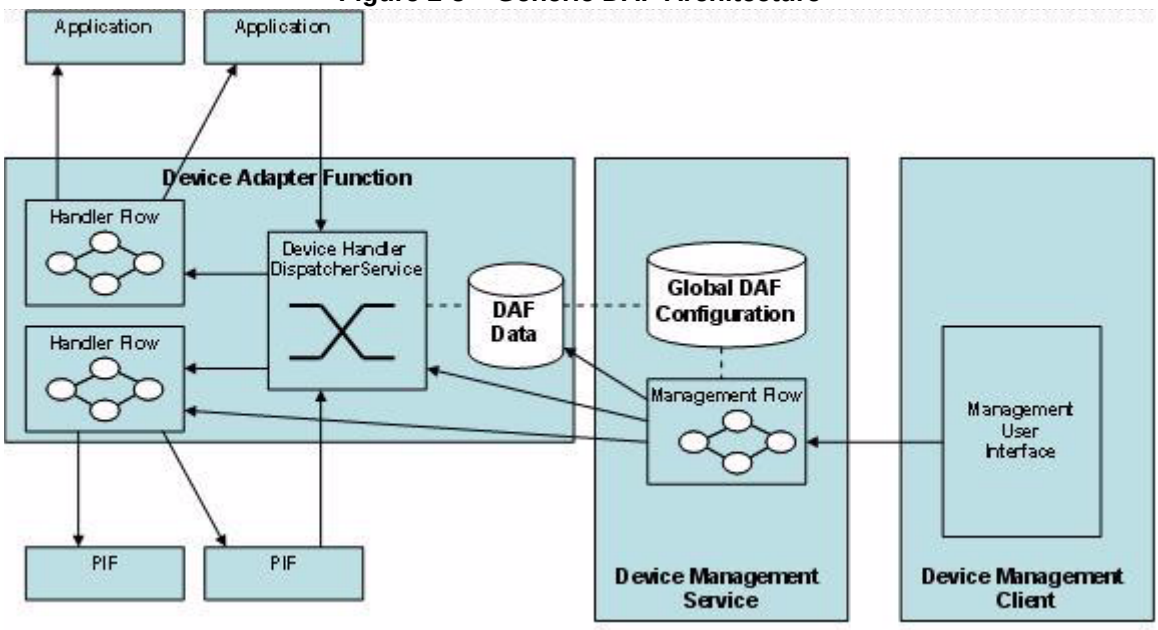
PIF events are dispatched to the appropriate DAF based on the request origin. Application events are dispatched to the appropriate DAF based on the event target.

The following list contains DAF implementations. The phrase *policy push adapter* indicates a capability to push a policy down to a specific external device, such as a Broadband Remote Access Server (BRAS).

- Generic CLI Policy Push Adapter
- Cisco ISG Policy Push Adapter
- Cisco IOS RADIUS Adapter
- Cisco CNR/DHCP Adapter

Figure 2-5 depicts the generic DAF architecture.

Figure 2-5 Generic DAF Architecture



The DAF has several associated, discrete installable components. The DHDS is an independent file package containing the DHDS service implementation. The DHDS must be deployed before any DAFs, as it is the service interface through which all requests are routed.

DAF Management

A DAF contains a single service and one or more flows. After you install it, you can associate the DAF with a device instance in the DAF data configuration. You can interact with the DAF to configure the set of adapters to be associated with each network device instance. The DHDS uses this data to determine the appropriate DAF instance for a given message.

The following DAFs are available:

- Cisco 10000 Adapter - This allows CLI command to run against a Cisco 10K device.

DAF Handler Interface

Handlers are service flows, grouped in adapters corresponding to the protocol they handle. They are device-, protocol-, and event-specific. The DHDS invokes DAF handlers, based on the configured handler records that are stored in the system. A set of handlers comprises a DAF. It is implemented as a service.

A device can have zero or more adapters associated with it, depending on the protocols it supports. For example, a Cisco 7600 device can have a Cisco CNR/DHCP adapter associations and a Telnet CLI adapter association. A handler varies in its specific behavior, which depends on the unique qualities of each device and protocol combination.

DAF Data Management

Adapters are services that are packaged as files. The file name contains the .tzz extension. The Network Storage Function (NSF) assigns adapters to devices.

The DAF encapsulates a device-specific behavior. A DAF can be associated with multiple network devices. Multiple DAFs can associate with a single network device instance. PIF events are dispatched to the appropriate DAF, based on the origin of the request. Application events are dispatched to the appropriate DAF, based on the event target.

How It Works

The DHDS is the service interface through which the system routes all requests. You must deploy the DHDS before any DAFs can be invoked. After installation, you can associate the DAF package with a network device instance. The system creates an association in the DAF data store.

When the DHDS receives a request, it searches for a network device instance to DAF association in the DAF datastore. If it finds the association, it invokes the DAF. If it does not find the association, it returns an error message.

The DHDS invokes DAF handlers, based on the configured handler records stored in the system. All handlers have the same Application Programming Interface (API).

Device Handler Dispatch Service

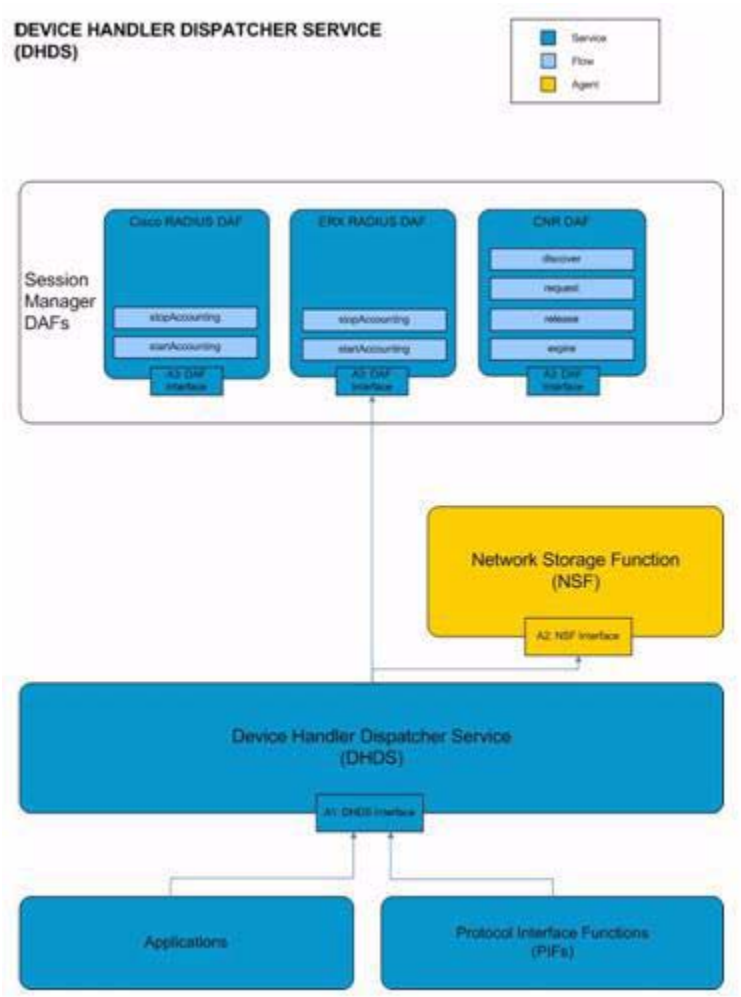
The Device Handler Dispatch Service (DHDS) determines the appropriate handler, based on a request from an upper layer, for example, a Profile Management Function (PMF) or direct application request; or from lower layers, for example, a RADIUS Start-Accounting message or a CNR Plugin Request. The system implements the DHDS as a BPM service with a single flow, *Dispatch*.

When the DHDS is invoked, it uses the *controlPoint*, *protocol*, and *action* attributes to determine the appropriate Device Handler flow to call.

- *controlPoint* - This identifies the device. For events originating from the PIF, it indicates the device sending the message. For events from upper applications, it indicates the device that is to run the command.
- *protocol* - This identifies the event protocol. For events received from the PIF, it indicates the protocol through which this event was received (for example, RADIUS, CNR/DHCP). For events from upper applications, it indicates the component that sent the request (for example, PMF, Session Management Application).
- *action* - this identifies the specific action associated with this event. The DHDS finds the node referred to by the device, and determines a handler. The handler refers to a BPM service or flow that is to handle the event

Figure 2-6 illustrates the DHDS and its relation to other BPM components.

Figure 2-6 DHDS Architecture



The handler invoked by the DHDS can reside locally on the machine or on a remote system. The DHDS hides the handler function location from the caller by internally remoting the request, if necessary.

How It Works

The DHDS invokes DAF handlers, based on the configured handler records stored in the system. All handlers have the same API, and take the following input:

- *Device-IPAddress* = *Device-IPAddress* value passed into, or derived by, the DHDS
- *Device-Instance* = *Device-Instance* value passed into, or derived by, the DHDS
- Protocol = Protocol value passed into the DHDS
- Event = Event value passed into the DHDS
- Parameters = Parameter values passed into the DHDS

The *Parameters* input represents a list of arguments whose contents depend on the specific device and action.

The DHDS invokes the appropriate handler flow, based on a request from a PMF or direct application request, a RADIUS Start-Accounting message or CNR Plugin. The DHDS is a service that comprises the single flow, *Dispatch*.

The DHDS uses the following attributes to determine the appropriate device handler flow:

- Device Instance - This identifies the device. For events from the PIF, it indicates the sending device. For events from upper applications, it indicates the device to run the command.
- Protocol - For events received from the PIF, this indicates the protocol through which the event was received, for example RADIUS or CNR/DHCP. For events from upper applications, it indicates the component sending the request, for example PMF or Session Management Application.
- Action - This identifies the action associated with the event. The DHDS finds the node referred to by the device and determines the handler identified by this value. The handler refers to a service or flow to handle the event.

The handler invoked by the DHDS can reside on the local machine or a remote system. The DHDS hides the handler function location from the caller by internally remoting the request, if necessary.

Dispatcher Interface

External components invoke the *Dispatch* function when they execute an action against a device or when they receive a request from a device. The function determines and calls the appropriate handler. When an application calls the DHDS, it uses a *deviceInstanceID*. The PMF takes the network session and a profile and extracts the *deviceInstanceIds* from the *deviceSessions* attached to the *networkSession*. One flow takes *deviceInstanceId*, protocol, and event; another takes IP address, protocol, and event.

Accounting Log Function

The Accounting Log Function, used by Directors and Resource Controllers records entrance parameters, internal decisions, and exit responses. The caller provides accounting-pertinent information and a correlation identifier. The ALF appropriately stores the information. Applications that use the SM and the NM functionality handle the accounting log functionality.

Accounting log messages are generated for the SM and the NM products. The system logs them to the Resource Controller accounting log file. Each event has one or more standard details. Table 2 presents the Accounting Log Function (ALF) configurable properties.

Table 2. Accounting Log Function Properties

Setting	Type	Default	Required/ Optional	Description
port	Integer		Required	This is the port over which peer active/standby instances communicate to ensure resiliency.
timeout	Integer	30,000	Optional	This is the number of milliseconds after which an outstanding request is timed out. This should be performance tuned.
maxSize	Integer	100 MB	Optional	This is the maximum size of the Accounting Log file reaches, before rollover occurs.

Table 2. Accounting Log Function Properties

Setting	Type	Default	Required/ Optional	Description
maxRecords	Integer		Optional	This is the maximum number of accounting records the log file reaches, before rollover occurs. The default is 1,000,000 records if not otherwise specified. A value of 0 disables automatic rollover due to number of records logged.
logFile	Path	<TAZZ_install>/ logs/ qosServer.log	Optional	This is the location of the Accounting Log file.

Accounting Log File

The Accounting Log file records entrance parameters, internal decisions, and exit responses. The caller provides accounting-pertinent information and a correlation identifier, and the ALF stores the information in an appropriate manner. The network administrator should monitor the size of the Accounting Log file. The administrator can set the default maximum size for the accounting log file (in MB) before it is rolled over. The default is 100 MB. Setting the value of *maxSize* to 0 disables automatic rollover due to file size.

The administrator can also set the maximum number of accounting records before the log file is rolled over. The default is 1,000,000 records. Setting the value of *maxRecords* to 0 disables automatic rollover due to number of records logged.

When the Accounting Log file is rolled over, the existing file is compressed and renamed according to the following format:

<logFile>@yyyymmdd_hhmmss-yyyymmdd_hhmmss.gz

Two distinct timestamps, encapsulated within the rolled-over file name, indicate the range of accounting records in the file.

Table 3. Accounting Log File Settings

Property	Type	Default	Required/ Optional	Description
maxSize	Integer	100 MB	Optional	This is the maximum size of the Accounting Log file, before rollover.
maxRecords	Integer		Optional	This is the maximum number of accounting records before the log file is rolled over. The default is 1,000,000 records if not otherwise specified. A value of 0 disables automatic rollover due to number of records logged.
logFile	Path	<TAZZ_install>/ logs/qosServer.log	Optional	This is the location of the Accounting Log file.

Statistics Function

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

Alarm Notification Function

The Alarm Notification Function (ANF) issues SNMP traps to alert external systems of aberrant BPM behavior. The ANF allows various BPM components to consistently report unexpected conditions and behavior, as well as unexpected life cycle changes.

System Modules

The SM product also uses the following basic system modules:

- Session Storage Function
- Network Storage Function

Session Storage Function

The Session Storage Function (SSF) provides session storage local to a Resource Controller. The SM product creates sessions that reside in the SSF. The SSF stores and retrieves session data in the repository.

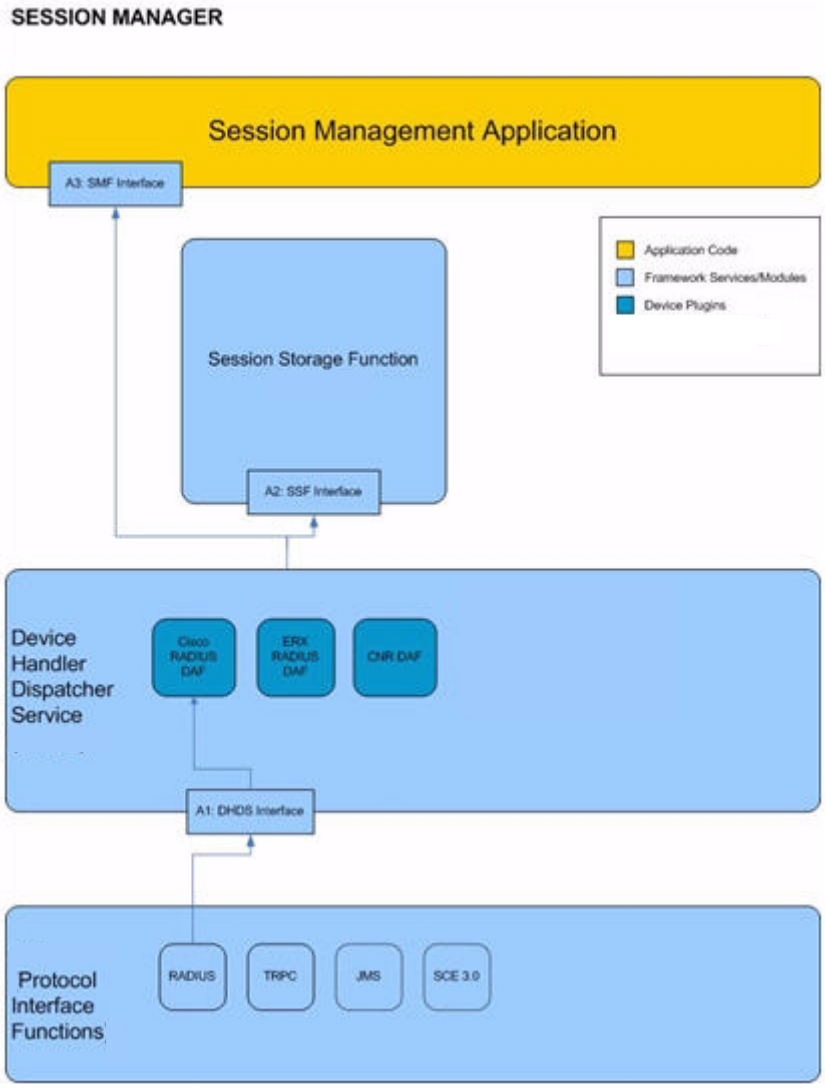
Network Storage Function

The Network Storage Function (NSF) assigns adapters to devices. It stores provisioned device and profile information and facilitates the SM and the NM operation. Data is provisioned on the Topology Database Server system and distributed to all Resource Controllers.

Architecture

Figure 2-7 depicts the SM architecture.

Figure 2-7 SM Architecture.



- A1: The DHDS takes an incoming network message from a PIF, and invokes the appropriate DAF.
- A2: The SSF stores and retrieves session data in the repository.
- A3: The SMF notifies applications of session state changes.

Subscriber Session Management

The SM product uses the following mechanisms to track and manage network access sessions on the broadband network:

- CNR Integration - The system processes DHCP sessions managed by the Cisco CNR.
- File-based Session Creation - The system loads a file that describes a set of network sessions.

Session State Storage

The SM product stores session state information for deployment scenarios via the following features:

- *PostgreSQL* storage of session state
- Database replication of session state between active/standby Resource Controllers
- SSF API used by all applications to access session state

The product delivers a standard API set. The system simplifies this process with the Session Management Application API that allows developers to create applications that are driven by the SM when sessions are started, modified, or stopped.

3

Network Manager

Overview

This chapter discusses the Network Manager (NM) product, its components, architecture, and operation. The NM product uses a series of components specific to its functionality, a number of system module components, and a series of components shared with the Session Manager (SM) product. (See Chapter 2 for a discussion of SM components.

NM Components

The NM product uses the following function, which is specific to its functionality:

- Profile Management Function

Profile Management Function

The Profile Management Function (PMF) activates and deactivates network profiles on subscriber sessions and provides stateful profile management for network sessions. A profile is an ordered set of actions that define how it is applied and removed from the network. Applications can request the activation and deactivation of generic profiles from the PMF. The PMF manages the application and removal of the profiles from the network.

The PMF is session-aware and stateful. Each profile request targets a specific network session, not the network elements that control the session. The PMF uses the DAF to control network elements. The DAF is unaware of specific network sessions, and actions target specific network elements. Applications use these APIs to invoke system capabilities.

Shared Components

The NM product uses the following shared components:

- Protocol Interface Function
- Device Adapter Function
- Device Handler Dispatch Service
- Accounting Log Function
- Statistics Function

- Alarm Notification Function

Protocol Interface Function

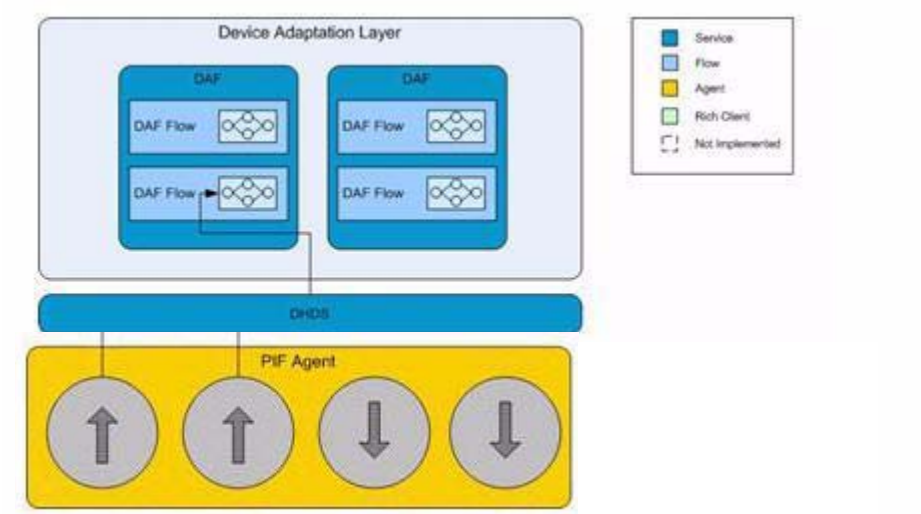
The Protocol Interface Function (PIF) encapsulates a protocol interface towards external systems and allows the BPM system to communicate with those systems. A PIF can act as a client, server, or peer with respect to those external systems. It standardizes the method by which new protocol interfaces are added to the system and the method by which they are managed.

Multiple PIFs can be in use at one time, and any device can have one or more associated PIFs. Multiple PIFs can be associated with a single external system. External systems use the PIF to deliver requests, queries, and notifications to the BPM. Applications within the BPM use the PIF to deliver requests, queries, and notifications to external systems. PIFs pass requests between Device Adapter Functions (DAFs) and the external systems represented by the DAFs.

A PIF is a component that handles reading and writing of protocol messages. The interface exposed by a PIF agent is specific to the device or protocol it encapsulates. A PIF also contains a PIF service that maps triggers from the PIF agent onto the appropriate DAF for processing. The PIF Service extracts the details from the message that are required to invoke the Device Handler Dispatch Service (DHDS).

Figure 3-8 presents the generic PIF architecture.

Figure 3-8 PIF Architecture



PIF Data Management

You can manage Protocol Interface Functions (PIFs) as collections of agents and flows using the Service Administration View and Network Administration View tools from the Broadband Policy Design Studio (BPDS). For further information about these administrative tools, see the *Broadband Policy Design Studio User Guide*.

PIF properties define local configuration variables that apply to a given PIF instance.

The following PIFs are available:

- Cisco Network Registrar (CNR)/TRPC Plugin PIF - This PIF receives lease statements from the Cisco CNR DHCP server.
- Telnet CLI PIF - this PIF executes Telnet CLI commands against the Cisco 10K.

Each PIF implementation has the following qualities:

- Agent required by the PIF
- Service that handles agent triggers
- Configuration properties associated with a PIF instance

Interfaces

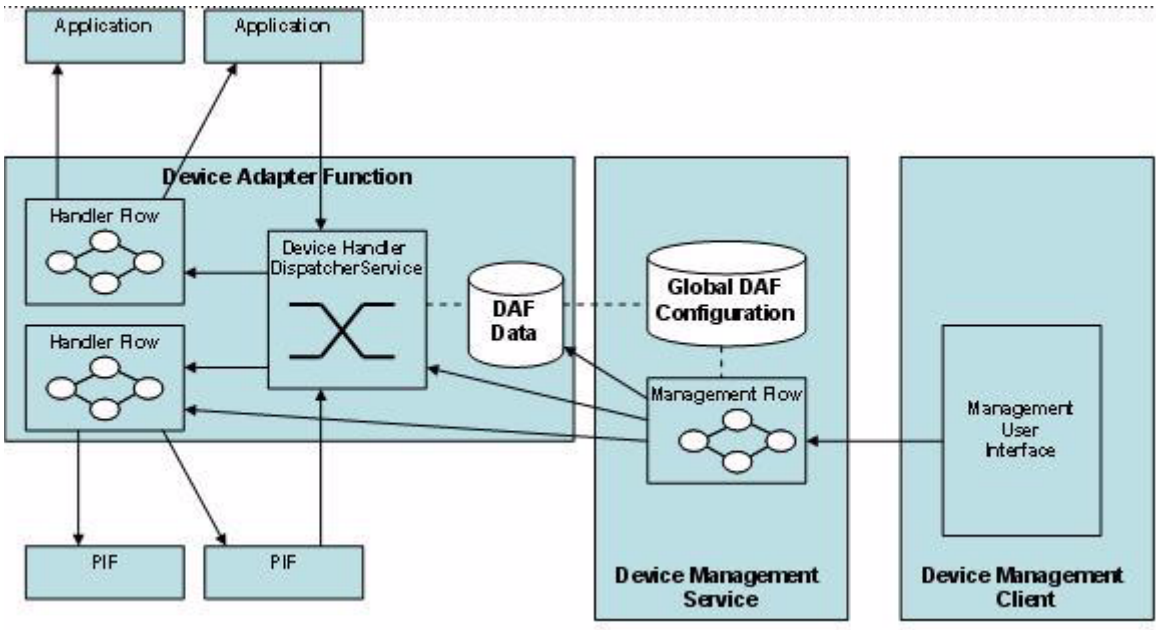
PIF interfaces exist according to the requirements of the specific PIF.

Device Adapter Function

The Device Adapter Function (DAF) defines how events to and from PIFs are to be handled, based on the device sending or receiving the event. The DAF standardizes the modeling and management of device-specific behavior within the BPM. The DAF encapsulates a device-specific behavior. A DAF can be associated with multiple network devices. Multiple DAFs can be associated with a single network device instance. A PIF can invoke DAFs to handle an event received from an external system. Application functions can also invoke DAFs to request that actions be invoked on PIFs.

Figure 3-9 depicts the generic DAF architecture.

Figure 3-9 Generic DAF Architecture



PIF events are dispatched to the appropriate DAF based on the request origin. Application events are dispatched to the appropriate DAF based on the event target.

The following list contains DAF implementations. The phrase *policy push adapter* indicates a capability to push a policy down to a specific external device, such as a Broadband Remote Access Server (BRAS).

- Generic CLI Policy Push Adapter
- Cisco ISG Policy Push Adapter
- Cisco IOS RADIUS Adapter
- Cisco CNR/DHCP Adapter

The DAF has several associated, discrete installable components. The DHDS is an independent file package containing the DHDS service implementation. The DHDS must be deployed before any DAFs, as it is the service interface through which all requests are routed.

DAF Management

A DAF contains a single service and one or more flows. After you install it, you can associate the DAF with a device instance in the DAF data configuration. You can interact with the DAF to configure the set of adapters to be associated with each network device instance. The DHDS uses this data to determine the appropriate DAF instance for a given message.

The following DAFs are available:

- Cisco 10000 Adapter - This allows CLI command to run against a Cisco 10K device.

DAF Handler Interface

Handlers are service flows, grouped in adapters corresponding to the protocol they handle. They are device-, protocol-, and event-specific. The DHDS invokes DAF handlers, based on the configured handler records that are stored in the system. A set of handlers comprises a DAF. It is implemented as a service.

A device can have zero or more adapters associated with it, depending on the protocols it supports. For example, a Cisco 7600 device can have a Cisco CNR/DHCP adapter associations and a Telnet CLI adapter association. A handler varies in its specific behavior, which depends on the unique qualities of each device and protocol combination.

DAF Data Management

Adapters are services that are packaged as files. The file name contains the .tzz extension. The Network Storage Function (NSF) assigns adapters to devices.

The DAF encapsulates a device-specific behavior. A DAF can be associated with multiple network devices. Multiple DAFs can associate with a single network device instance. PIF events are dispatched to the appropriate DAF, based on the origin of the request. Application events are dispatched to the appropriate DAF, based on the event target.

How It Works

Since the DHDS is the service interface through which the system routes all requests, you must deploy the DHDS before any DAFs can be invoked. After installation, you can associate the DAF package with a network device instance. The system creates an association in the DAF data store.

When the DHDS receives a request, it searches for a network device instance to DAF association in the DAF datastore. If it finds the association, it invokes the DAF. If it does not find the association, it returns an error message.

The DHDS invokes DAF handlers, based on the configured handler records stored in the system. All handlers have the same API, and take the following input:

- *Device-IPAddress* = *Device-IPAddress* value passed into, or derived by, the DHDS
- *Device-Instance* = *Device-Instance* value passed into, or derived by, the DHDS
- Protocol = Protocol value passed into the DHDS
- Event = Event value passed into the DHDS
- Parameters = Parameter values passed into the DHDS

The *Parameters* input represents a list of arguments whose contents depend on the specific device and action.

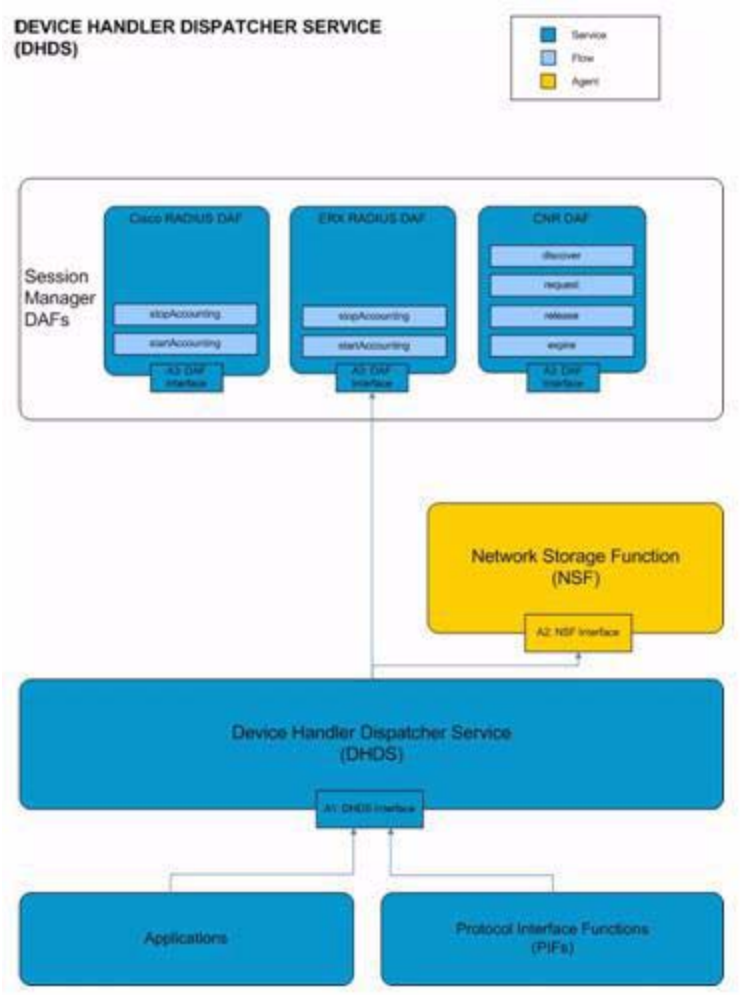
A DAF upgrade can occur at any time. This prompts you to update existing device instances to DAF associations with the new implementation.

Device Handler Dispatch Service

The Device Handler Dispatch Service (DHDS) determines the appropriate handler, based on a request from an upper layer, for example, a Profile Management Function (PMF) or direct application request; or from lower layers, for example, a RADIUS Start-Accounting message or a CNR Plugin Request. The system implements the DHDS as a BPM service with a single flow, *Dispatch*.

Figure 3-10 illustrates the DHDS and its relation to other BPM components.

Figure 3-10 DHDS Architecture



When the DHDS is invoked, it uses the *controlPoint*, *protocol*, and *action* attributes to determine the appropriate Device Handler flow to call.

- *controlPoint* - This identifies the device. For events originating from the PIF, it indicates the device sending the message. For events from upper applications, it indicates the device that is to run the command.

- *protocol* - This identifies the event protocol. For events received from the PIF, it indicates the protocol through which this event was received (for example, RADIUS, CNR/DHCP). For events from upper applications, it indicates the component that sent the request (for example, PMF, Session Management Application).
- *action* - this identifies the specific action associated with this event. The DHDS finds the node referred to by the device, and determines a handler. The handler refers to a BPM service or flow that handles the event.

The handler invoked by the DHDS can reside locally on the machine or on a remote system. The DHDS hides the handler function location from the caller by internally remoting the request, if necessary.

How It Works

The DHDS invokes DAF handlers, based on the configured handler records stored in the system. All handlers have the same API, and take the following input:

- *Device-IPAddress* = *Device-IPAddress* value passed into, or derived by, the DHDS
- *Device-Instance* = *Device-Instance* value passed into, or derived by, the DHDS
- Protocol = Protocol value passed into the DHDS
- Event = Event value passed into the DHDS
- Parameters = Parameter values passed into the DHDS

The *Parameters* input represents a list of arguments whose contents depend on the specific device and action.

The DHDS invokes the appropriate handler flow, based on a request from an upper layer, for example, a PMF or direct application request, or a lower layer, for example, a RADIUS Start-Accounting message or CNR Plugin request. The DHDS is a service that comprises the single flow, *Dispatch*.

Upon invocation, the DHDS uses the following attributes to determine the appropriate device handler flow:

- Device Instance - This identifies the device. For events from the PIF, it indicates the sending device. For events from upper applications, it indicates the device to run the command.
- Protocol - For events received from the PIF, this indicates the protocol through which the event was received, for example RADIUS or CNR/DHCP. For events from upper applications, it indicates the component sending the request, for example PMF or Session Management Application.
- Action - This identifies the action associated with the event. The DHDS finds the node referred to by the device and determines the handler identified by this value. The handler refers to a service or flow to handle the event.

The handler invoked by the DHDS can reside on the local machine or a remote system. The DHDS hides the handler function location from the caller by internally remoting the request, if necessary.

Dispatcher Interface

External components invoke the *Dispatch* function when they execute an action against a device or when they receive a request from a device. The function determines and calls the appropriate handler. When an application calls the DHDS, it uses a *deviceInstanceID*. The PMF takes the network session and a profile and extracts the *deviceInstanceIds* from the *deviceSessions* attached to the *networkSession*. One flow takes *deviceInstanceId*, protocol, and event; another takes (IP address), protocol, and event.

Accounting Log Function

The Accounting Log Function (ALF) records entrance parameters, internal decisions, and exit responses. The caller provides accounting-pertinent information and a correlation identifier. The ALF stores the information in an appropriate manner. Applications that use the NM functionality handle the accounting log functionality.

Accounting log messages are generated for the NM product. The system logs them to the Resource Controller accounting log file. Each event has standard details.

Statistics Function

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

Alarm Notification Function

The Alarm Notification Function (ANF) issues SNMP traps to alert external systems of aberrant behavior in the BPM. The ANF allows various components of the BPM to report unexpected conditions and behavior, as well as unexpected life cycle changes in a controlled and consistent manner.

System Modules

The NM product also uses the following basic system modules:

- Session Storage Function
- Network Storage Function

Session Storage Function

The Session Storage Function (SSF) provides session storage local to a Resource Controller. The SM product creates sessions that reside in the SSF. The SSF stores and retrieves session data in the repository.

Network Storage Function

The Network Storage Function (NSF) assigns adapters to devices. It stores provisioned device and profile information and facilitates the NM operation. Data is provisioned on the Topology Database Server system and distributed to all Resource Controllers

Architecture

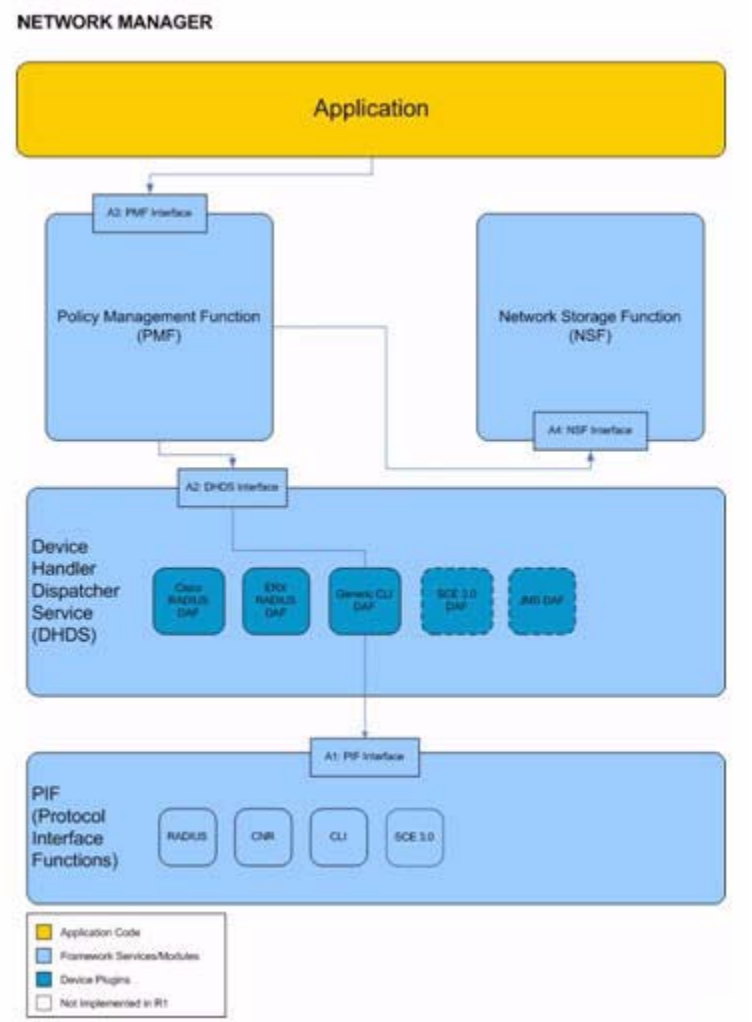
The Network Manager (NM) product provides facilities for controlling and querying elements in the network. It can be deployed with the SM product.

NM Product Features

Figure 3-11 depicts the NM architecture.

- A1: The PIF interface extensions for the NM - The Network Adaptation functions use the PIF interface extensions to invoke commands on network elements.
- A2: The DHDS takes a request from the PMF and invokes the appropriate NM DAF.
- A3: The PMF: The Session Management Applications use the PMF to manage stateful network profiles associated with a user session. Profiles are defined by groups of actions that are run against network elements to activate and deactivate the profile.
- A4: The Network SSF stores and retrieves device and profile data in the repository.

Figure 3-11 NM Architecture.



NM Operations

A set of processes systematically modify the properties of the underlying network elements as part of policy execution from a policy control perspective, for example, changing the size of an MPLS tunnel or pruning an IP Multicast branch. The system standardizes the following system interfaces:

1. The DHDS takes an incoming network message from a PIF, and invokes the appropriate DAF.
2. The SSF stores and retrieves session data in the repository.
3. The SMF notifies applications of session state changes.

4. The Session Management Applications use the PMF to manage stateful network profiles associated with a user session. Groups of actions define profiles that are run against network elements to activate and deactivate the profiles.
5. The DHDS takes a request from the PMF and invokes the appropriate NM DAF.
6. The Network Adaptation functions use PIF to invoke commands on network elements.

Device Adapters

The PMF calls the DAFs. Application events are dispatched to the appropriate DAF based on the event target.

The following list contains DAF implementations. The phrase *policy push adapter* indicates a capability to push a policy down to a specific external device, such as a BRAS.

- Generic CLI Policy Push Adapter
- Cisco ISG Policy Push Adapter
- Cisco IOS RADIUS Adapter
- Cisco CNR/DHCP Adapter

Network Manager API

The Network Manager (NM) provides an interface for applications to request services from the PMF or to invoke commands on the DAF. It offers the following mechanisms to control and configure network elements:

- Telnet CLI - The system executes CLI scripts against a network element including the ability to read information out from the CLI. This is used for configuring Cisco 10K devices.
- RADIUS CoA - The system uses Cisco ISG to configure Cisco ISG-enabled devices. The system sends unsolicited RADIUS CoA messages to control a network element.
- File-based Command Authoring - The system provides the ability to define network applications in a configuration file that can be loaded into the system for use by applications.

NM Application Implementation

The system delivers a single API for use by applications to control and query network elements. This interface harmonizes the configuration of diverse system configurations (for example, BRAS, DSLAM, DPI, SBC). It provides the PMF API, based on DHDS, with the ability to send action events to a device.

Policy Control for Subscriber Sessions

The NM provides an API that allows applications to apply stateful profiles to sessions in the network. When an application applies a profile, the NM remembers the profile. It allows the application to later release the profile without awareness of the specific steps required to perform the activation or release. The PMF allows the applications to apply and remove the profiles from a network session.

Command Execution

The NM provides an API that allows applications to execute logical commands against network elements. The PMF uses this API to control the configuration of individual network elements. Applications use this API directly (by passing the profile management API) to directly invoke commands on network elements.

4

Deployment

Overview

The BPM deployment consists of the Resource Controller Broadband Policy Manager (BPM).

This chapter discusses this device and the following topics:

- Resource Controller
- Realms

Resource Controller

The Resource Controller BPM tracks resource utilization for the system. You can configure Resource Controllers in resilient pairs, the *active* system and the *standby* system. Each Resource Controller (or resilient pair) tracks the resources of a subset of the network topology (logical and/or physical network entities, such as ATM Virtual Paths (VPs) and Virtual Circuits (VCs).

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

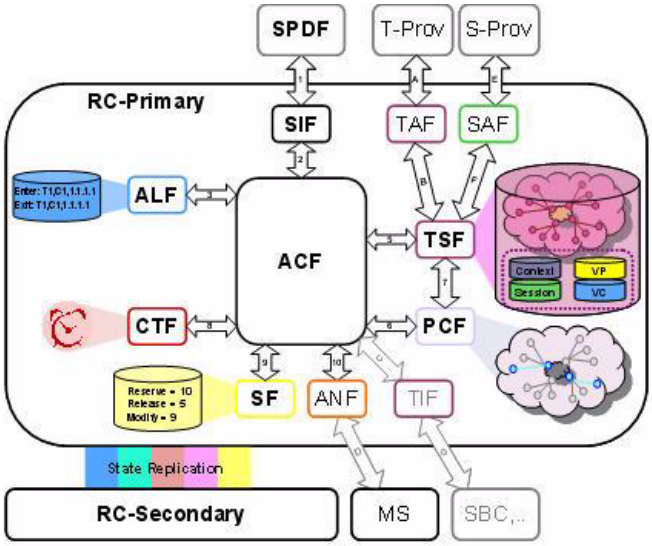
- Signaling Interface Function (SIF) - Interfaces with the external AF, which is the Director. Since this is internal, the SIF is transparent.
- Topology Store Function (TSF) - Maintains the Topology Information Model (TIM) that the Resource Controller is responsible for, against which resource consumption is checked.
- Topology Awareness Function (TAF) - Interacts with the TSF to react to topology changes (link or node activate/deactivate) by correctly resolving internal state and resource utilization.
- Path Computation Function (PCF) - Determines the path through the local topology that the call transits..
- Context Timer Function (CTF) - Enacts the soft-state reservation model to automatically remove orphaned or stale contexts and the resources they consume.
- Admission Control Function (ACF) - Performs local ACD, based on TIM resource utilization.
- Accounting Log Function (ALF) - Records accounting information.
- Statistics Function (SF) - Records statistics.

- Alarm Notification Function (ANF) - Handles alarm notification.

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, for example, Deep Packet Inspection devices, MPLS PE routers, and DSLAMs.

Resources are tracked at the Resource Controller. The deployed product knows the resource types. Resource Controllers are assigned to specific network resources (devices, links, etc.). The Resource Controller dynamically executes fine-grained configuration changes to the underlying network devices and tracks the availability of network resources. A Resource Controller receives messages from the Director indicating the policy actions required to fulfill an application or subscriber request.

Figure 12. Resource Controller Internal Structure



Session Information Model

The Session Information Model (SIM), internal to the TIM, connects dynamic sessions with the more static topology. For DHCP-derived addresses, it dynamically associates an IP address with a customer premises equipment (CPE) device, because the IP address association can change.

The next time the IP address is assigned, it can belong to a different CPE device. Usually, each address also belongs to a pool, which is often managed at the BRAS. The pools, in some cases, can be reassigned to different BRAS nodes. An IP address currently associated with a particular CPE device can occasionally shift to a CPE device attached to a different BRAS that is associated with a different Resource Controller.

The Resource Controller components use the dynamic mapping of IP address to the session to determine the CPE and BRAS devices 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.

Since this information determines the links and resources in the TIM that are used to evaluate the Admission Control Decision, the information must be consistent with other external elements.

It is incorrect if an IP address assignment from DHCP occurs, and the AF requests a call for that specific address before the external system has informed the BPM. This guarantee is not always possible, as the edge cases involved can cause information to resolve to different Resource Controller elements. It is important to achieve the notification of session information in the correct manner. However, the soft-state model eventually corrects for such aberrant behavior if it occurs. Though soft-state only maintains eventual consistency, it does not solve the issue of incorrect admission results due to non-synchronous delivery of presence information.

Directors are unconcerned with the highly dynamic nature of each individual IP address as assigned for each session (at least when they derive from pools managed by a BRAS). They resolve an IP address to a particular BRAS and, subsequently, the Resource Controller component responsible for that BRAS. They do this with a best *first match* against all assigned IP address pools, each of which is assigned to a particular BRAS. Each BRAS has an assigned Resource Controller component. The Director augments the request with the BRAS information for each side of the context (call). This information determines the *realm* for the Resource Controller. The Director forwards the request to the determined Resource Controller component, where more localized information exists.

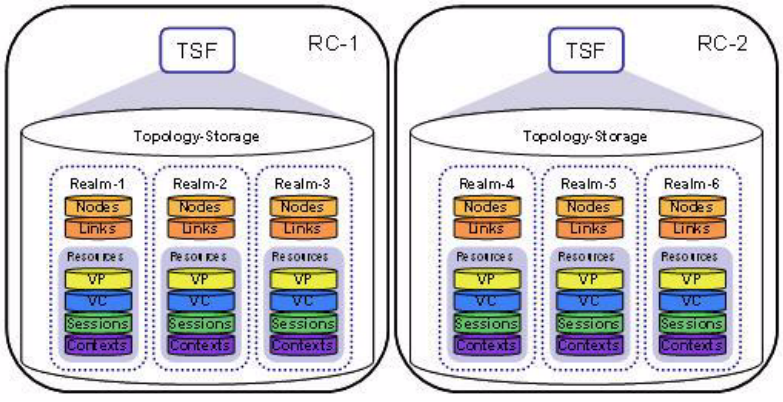
Realms

Topology, resources, active sessions, and active contexts exist in an information *realm*. The realm improves performance by restricting lookups and updates against smaller data sets, providing less lock contention and faster search times. It also allows a Resource Controller to comprehend the realms for which it is responsible. If a request involves a realm that the Resource Controller does not own, it may ignore the request (if that is the configured behavior). When introducing new Resource Controllers, BRAS responsibility is migrated from one Resource Controller to a new Resource Controller. The realm concept allows the information model to consider this a block movement of a realm. The migration affects only the realm that is moving. When scaling the BPM to accommodate more hardware and repartitioning the realms, only the realm/BRAS being moved is unavailable to QoS requests. Calls originating or terminating in other realms remain uninterrupted.

A BRAS defines a realm of self-contained information. The mapping of Resource Controllers to BRASs allows multiple BRASs and their access legs to be handled by a single Resource Controller. The state maintenance of various components is specified at the granularity of the Resource Controller. Thus, a single Topology Store Function (TSF) element handles more than one BRAS.

Figure 13 depicts the realms on a Resource Controller.

Figure 13. Realms on Resource Controllers



Network Realm

The Network Realm stores specific network adaptation information, (such as the devices active on a particular Resource Controller), profiles, devices, and handlers. The Network Realm is centrally provisioned on the Topology Database Server, and distributed to all Resource Controllers.

Session Realm

A Session Realm, unique to a Resource Controller, improves performance by restricting lookups and updates against smaller data sets.

Provisioning Format

Customized flows, for example, new handler flows and device adaptation flows, are centrally created on the data controller and provisioned to individual systems. Specific network adaptation data, such the active devices on a particular Resource Controller, are provisioned on the Topology Database Server and distributed to one or more Resource Controllers, as needed. The Network Realm database partition stores all this information. The Network Realm is centrally provisioned on the Topology Database Server, and distributed to all Resource Controllers.

Distribution of the Network Realm contents uses a Topology Database Server mechanism that copies realms to all Resource Controllers. It does not copy realms to Directors.

The Network Realm provisioning format uses elements, not attributes. All provisioning files have a root tag of global. For referential integrity, all network provisioning data must be in the same provisioning file. This provisioning format is used to add new information only into an installation. The mechanism runs on the Topology Database Server, where it converts the provisioning file into a series of SQL calls that populate the Topology Database Server database. The mechanism calls *CopyRealm* to distribute the data to one or more resource controllers as needed.

To remove or modify existing provisioned data, use the command line interface (CLI) on the Topology Database Server. The CLI applies changes and deletions to the Topology Database Server-local copies of realms, and distributes those updates to all applicable Resource Controllers. (Refer to the *Cisco Broadband Policy Manager Operations Guide*, for further details.)

Appendix A - Glossary

This appendix contains abbreviations, acronyms, terms, and their definitions.

Table A-1. Terms and Definitions.

Term	Definition
A	
Accounting Log Function	ALF. The Accounting Log Function records entrance parameters, internal decisions, and exit responses.
ACF	Admission Control Function. The ACF provides the core logic for performing admission control. It is programmed with a set of policies that define admission control behavior.
Action	An action is an operational category for changing, or inquiring about, a network element.
Active BPM	In a pair of BPMs, the active BPM processes requests. A standby BPM constantly monitors the health of the active BPM. If the active BPM is not viable, the standby BPM becomes the active BPM.
Admission Control Function	ACF. The ACF provides the core logic for performing admission control. It is programmed with a set of policies that define admission control behavior.
Agent	An internal BPM component that interacts with a device. The designer creates the agent and configures it to interact with a specific device by indicating the device type, IP address, and port number. The designer then assigns the agent to perform service functions.
Agent Configuration	Agent information that comprises a specific agent type instance. For example, a RADIUS agent configuration contains appropriate IP address, port, and shared secret values for a RADIUS agent type.
Agent Function	The service designer uses the BPDS to drag and drop an agent function into a flow in the BPDS. An agent, interacting with a device, performs the actual operation.
Agent Instance	A running instance of an agent type.
Agent Package	Software that allows agents to interact with a particular device type. For example, a RADIUS agent package contains software that allows the creation of agents that interact with specific RADIUS devices.
Agent Type	The agent type describes a particular type of agent that you can load onto the system. You select the agent type when you create the agent instance.
AI	Application Interface. The underlying frameworks use Application Interfaces to notify the Application of network events. The Cisco framework provides these interfaces.
Alarm Notification Function	ANF. The Alarm Notification Function issues SNMP traps to alert external systems of aberrant behavior in the BPM.
ALF	Accounting Log Function. The Accounting Log Function records entrance parameters, internal decisions, and exit responses.

Table A-1. Terms and Definitions.

Term	Definition
ANF	Alarm Notification Function. The Alarm Notification Function (ANF) issues SNMP traps to alert external systems of aberrant behavior in the BPM.
API	Application Program Interface. An API is a set of routines, protocols, and tools for building software applications. An API makes it easier to develop a program by providing the required building blocks. A programmer puts the blocks together.
Application	A service that maps business models and operational procedures directly into IP services, executable by their customers, for example, video on demand or automatic backup. See also Service.
Application Interface	AI. The underlying frameworks use Application Interfaces to notify the Application of network events. The Cisco framework provides these interfaces.
Application Program Interface	API. An API is a set of routines, protocols, and tools for building software applications. An API makes it easier to develop a program by providing the required building blocks. A programmer puts the blocks together.
Application Service Provider	ASP. An ASP is a business that provides computer-based services to customers over a network.
ASP	Application Service Provider. An ASP is a business that provides computer-based services to customers over a network.
Asynchronous Transfer Mode	ATM. Asynchronous Transfer Mode is a network technology based on transferring data in cells or packets of a fixed size.
ATM	Asynchronous Transfer Mode. ATM is a network technology based on transferring data in cells or packets of a fixed size.
Attribute	An attribute is a datum about a network session or a device session. Attributes contain a name and value and a distinguishing namespace. In the BPDS Object Manager tool, a simple type with a default value. An object can have several attributes.
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. 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 ISPs.
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 ISPs.
BPDS	Broadband Policy Design Studio. The BPDS is a graphical user interface to the BPM. The BPDS includes a service design feature.
BPM	Broadband Policy Manager. The BPM is a product suite used by service providers to create and deploy advanced services on broadband networks. A BPM system can be configured as a Director, Domain Controller, Resource Controller, or Topology Database Server.
BPS	Broadband Policy Studio. The BPS is a graphical user interface, similar to the BPDS. The BPS does not include the service design feature.

Table A-1. Terms and Definitions.

Term	Definition
BRAS	Broadband Remote Access Server. A BRAS device routes traffic to and from the digital subscriber line access multiplexers on an ISP network.
Broadband Policy Design Studio	BPDS. The BPDS is a graphical user interface, similar to the BPS. The BPDS includes a service design feature.
Broadband Policy Manager	BPM. The BPM is a product suite used by service providers to create and deploy advanced services on broadband networks.
Broadband Policy Studio	BPS. The BPS is a graphical user interface, similar to the BPDS. The BPS does not include the service design feature.
Broadband Remote Access Server	BRAS. A BRAS device routes traffic to and from the digital subscriber line access multiplexers (DSLAM) on an ISP network.
C	
CAC	Capacity Admission Control. CAC monitors, controls, and enforces the use of network resources and services with policy-based management over broadband access and MPLS core networks.
Capacity Admission Control	CAC. CAC monitors, controls, and enforces the use of network resources and services with policy-based management over broadband access and MPLS core networks.
Cisco Network Registrar	CNR. The CNR is a full-featured DNS/DHCP system that provides scalable naming and addressing services for service provider and enterprise networks.
Class of Service	CoS. This is a traffic prioritization scheme that enables more predictable traffic delivery, based on application requirements.
Classless Inter-Domain Routing	CIDR. This IP addressing scheme addresses the size of routing tables and makes more IP addresses available within organizations. CIDR is also called supernetting.
CIDR	Classless Inter-Domain Routing. This IP addressing scheme addresses the size of routing tables and makes more IP addresses available within organizations. CIDR is also called supernetting.
Client	This is a generic term that denotes the BPM BPDS application.
CoS	Class of Service. This is a traffic prioritization scheme that enables more predictable traffic delivery, based on application requirements.
CPE	customer premises equipment. This is communications equipment that resides on the customer premises. It is owned or leased by the customer.
CLI	command line interface. This is a user interface common to computers. The user enters a command. The computer acts on the command.
Cluster	A pair of cooperating and redundant BPMs.
CNR	Cisco Network Registrar. The CNR is a full-featured DNS/DHCP system that provides scalable naming and addressing services for service provider and enterprise networks.
Command Line Interface	CLI. This is a user interface common to computers. The user enters a command. The computer acts on the command.
Component	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.

Table A-1. Terms and Definitions.

Term	Definition
Configuration	Information necessary to construct an instance of a type (agent, service).
Controller	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.
Customer Premises Equipment	CPE. This is communications equipment that resides on the customer premises. It is owned or leased by the customer.
D	
DAF	Device Adapter Function. A DAF translates between the protocol and device type-specific events of at the PIF layer and the abstract application events at the Application layer. A DAF can be assigned to multiple device types and multiple DAFs can be assigned to one device.
Deep Packet Inspection Protocol	DPI. This is network packet filtering that examines packet *data*, searching for nonprotocol compliance or predefined criteria, to decide if the packet can pass. This is in contrast to shallow packet inspection (called packet inspection), which checks only the packet *header*.
Device	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.
Device Access	A device access is data about accessing a device instance. Most devices require authentication before any device action can occur. The device access contains this authentication data and other related data. Each device instance has one device access per management protocol.
Device Action	A device action is the implementation of an action for a given device type. That is, it is the actual set of instructions necessary to change the functioning of the device instance.
Device Adapter Function	DAF.A DAF translates between the protocol and device type-specific events of at the PIF layer and the abstract application events at the Application layer. A DAF can be assigned to multiple device types and multiple DAFs can be assigned to one device.
Device Adapter Function Flow	A Flow that handles a protocol event for a specific device type.
Device Handler Dispatch Service	DHDS. DHDS provides routing services for PIFs and Applications requesting invocation of DAF operations.
Device Instance	A device instance is a device type in use in the network. For example, a Cisco 10K device at IP address 128.148.176.10. Device instances are grouped according to roles.
Device Rule	A device rule is a provisioned list of steps that apply a policy to a device. A device rule consists of a set of instructions that the BPM sends to the device to apply the given policy. Device rules can retrieve information from connected devices. Preconfigured device rules are useful for configuring a new BPM system. See also Device Type and Policy Rule.

Table A-1. Terms and Definitions.

Term	Definition
Device Session	A device session contains data about a device instance used by a network session. For example, information about the bras would be encoded in a device session.
Device Type	A device type is a vendor's network element hardware. Device types are grouped according to roles and are based on device attributes, such as vendor, model, hardware version, and software version. See also Device Rule.
DHDS	Device Handler Dispatch Service. DHDS provides routing services for PIFs and applications requesting invocation of DAF operations.
Digital Subscriber Line	DSL. DSL technologies use sophisticated modulation schemes to pack data onto copper wires.
Digital Subscriber Line Access Multiplexer	DSLAM. This mechanism links customer DSL connections to a single high-speed ATM line.
Director	A Director is one or more stateless installations that takes requests and routes them to appropriate Resource Controllers, to handle the specific incoming requests.
Director Realm	The Director Realm stores information required by Director systems, including information about network devices (such as BRAS devices). The information specifies the Resource Controller responsible for each device and the IP address pools each device handles. A Director uses this information to forward an incoming request to the correct Resource Controller. The Topology Database Server maintains the Director Realm, and the server distributes its updates to each Director when updates occur.
Domain	One or more cooperating Broadband Policy Managers (BPMs) managed by a single domain repository.
Domain Controller	The Domain Controller is a standalone system responsible for domain management, including application deployment, configuration, and health for all systems in the domain. Only one Domain Controller exists per domain.
Domain Data	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.
Domain Realm	The Domain Realm maintains application level information about the physical network topology. The nodes in the topology represent Director and Resource Controller systems. The Topology Database Server uses the Domain Realm to understand the system topology. Links represent connectivity between cluster pairs. Resources represent interfaces on the component systems, system health, cluster information, and system configuration.
Domain Repository	The master database that contains configuration information for each domain element.
DPI	Deep Packet Inspection Protocol. This is network packet filtering that examines packet *data*, searching for nonprotocol compliance or predefined criteria, to decide if the packet can pass. This is in contrast to shallow packet inspection (called packet inspection), which checks only the packet *header*.

Table A-1. Terms and Definitions.

Term	Definition
DSL	Digital Subscriber Line. DSL technologies use sophisticated modulation schemes to pack data onto copper wires.
DSLAM	Digital Subscriber Line Access Multiplexer. This mechanism links customer DSL connections to a single high-speed ATM line.
E	
Element	An object with the BPM: package; agent configuration; service instance; shared object.
Enumeration	In the BPDS Object manager tool, enumeration is contained within a simple type.
Ethernet	The Ethernet is a large and diverse family of frame-based computer networking technologies for local area networks (LANs). It defines a number of wiring and signaling standards for the physical layer, two means of network access at the Media Access Control (MAC)/Data Link Layer, and a common addressing format. Ethernet has been standardized as IEEE 802.3.
ETSI	European Telecommunications Standards Institute. ETSI is an independent, non-profit organization, whose mission is to produce telecommunications standards for today and for the future.
European Telecommuni-cations Standards Institute	ETSI. ETSI is an independent, non-profit organization, whose mission is to produce telecommunications standards for today and for the future.
F	
Field Replaceable Unit	FRU. An FRU represents an element (e.g., entire system, BPDS client software, agent) within the Broadband Policy Managers (BPM) that has a version associated with it. A FRU is a subset of an element.
Flow	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.
FRU	Field Replaceable Unit. An FRU represents an element (e.g., entire system, BPDS client software, agent) within the Broadband Policy Managers (BPM) that has a version associated with it. A FRU is a subset of an element.
Function	The element that performs an operation, based on inputs and returns the results of the operation via its outputs. The designer drags and drops a function into a flow in the BPDS. An agent, interacting with a device, performs the actual operation.
G	
Graphical User Interface	GUI. A program interface that takes advantage of the computer's graphics capabilities to make the program easier to use. For the BPM, the GUI is the BPDS.
GUI	Graphical User Interface. A program interface that takes advantage of the computer's graphics capabilities to make the program easier to use. For the BPM, the GUI is the BPDS.
H	

Table A-1. Terms and Definitions.

Term	Definition
Handler	A handler enables flow of control between the PIF, DAF, and SMF interfaces. It includes details about the appropriate service flow to call under specific conditions.
Handler Flow	A Handler Flow normalizes protocol-specific parameters before forwarding them to an application. An application can indirectly invoke a Handler Flow using the DHDS.
Head Version	The latest version of an element.
Hypertext Preprocessor	PHP. PHP is an open source, server-side, HTML embedded scripting language used to create dynamic Web pages.
I	
Implementation	An instruction set for executing a specification.
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 Service Provider	ISP. An ISP is a company that provides access to the Internet. For a monthly fee, the company provides a software package, username, password and access phone number. In addition to serving individuals, ISPs also serve large companies, providing a direct connection from the company network to the Internet.
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.
ISP	Internet Service Provider. An ISP is a company that provides access to the Internet. For a monthly fee, the company provides a software package, username, password and access phone number. In addition to serving individuals, ISPs also serve large companies, providing a direct connection from the company network to the Internet.
J	
K	
Key	A key is an identifier used in conjunction with network sessions.
L	
LAN	Local Area Network. A LAN is computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings. A LAN connect workstations and personal computers. This allows users to share devices and data and communicate via email.
L2TP	Layer Two Tunneling Protocol. L2TP is an extension to the PPP protocol that enables ISPs to operate VPNs.
Layer Two Tunneling Protocol	L2TP. L2TP is an extension to the PPP protocol that enables ISPs to operate VPNs.
Link	A link is a line or channel over which data is transmitted.

Table A-1. Terms and Definitions.

Term	Definition
Local Area Network	LAN. A LAN is computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings. A LAN connect workstations and personal computers. This allows users to share devices and data and communicate via email.
M	
Management Protocol	A management protocol is the mechanism for managing a network element. Common management protocols are RADIUS and SNMP.
Metadata	In the BPDS, this is the data structure. A customer can import metadata to invoke a structure for his or her database.
MPLS	Multiprotocol Label Switching. MPLS integrates Layer 2 network link information into Layer 3 within an autonomous system or ISP. It improves IP-packet exchange and allows operators to divert and route traffic around link failures, congestion, and bottlenecks.
Multiprotocol Label Switching	MPLS. MPLS integrates Layer 2 network link information into Layer 3 within an autonomous system or ISP. It improves IP-packet exchange and allows operators to divert and route traffic around link failures, congestion, and bottlenecks.
N	
N + 1 Redundancy	The ability for service engines to use one service engine as a backup.
NAF	Network Adaptation Function. NAF. The NAF dynamically resizes network links and queue sizes, based on the ability of the underlying network to adapt after a request from the ACF.
Namespace	A namespace helps distinguish two or more values that otherwise would conflict with each other.
NAS	Network Attached Storage. A NAS device is a server dedicated to file sharing, allowing more hard disk storage space to be added to a network that already utilizes servers without shutting them down for maintenance and upgrades. A NAS device can exist anywhere in a LAN and can be made up of multiple networked NAS devices.
NAV	Network Admin view. In the BPS and BPDS graphical user interfaces to the BPM, this is the network view where you can perform administration tasks.
Network	A network is a group of two or more computer systems linked together. Local-area networks (LANs), wide-area networks (WANs), and metropolitan-area networks MANs are typical networks.
Network Adaptation Function	NAF. The NA) dynamically resizes network links and queue sizes, based on the ability of the underlying network to adapt after a request from the ACF.
Network Admin View	NAV. In the BPS and BPDS graphical user interfaces to the BPM, this is the network view where you can perform administration tasks.
Network Attached Storage	NAS. A NAS device is a server dedicated to file sharing, allowing more hard disk storage space to be added to a network that already utilizes servers without shutting them down for maintenance and upgrades. A NAS device can exist anywhere in a LAN and can be made up of multiple networked NAS devices.
Network Event	A network event is a set of install and uninstall rules, contained within a profile, that are performed in sequence.

Table A-1. Terms and Definitions.

Term	Definition
Network Manager	NM. The NM product provides a framework for controlling and querying the element configurations in the broadband network.
Network Policy	A network policy is a device rule entry. The device rule contains commands to configure a network device to apply a network policy. See also Device Rule, Policy Rule.
Network Realm	The Network Realm stores specific network adaptation information, such as the devices active on a particular Resource Controller, profiles, and handlers. The Network Realm is centrally provisioned on the Topology Database Server, and it is distributed to all Resource Controllers.
Network Session	A network session represents a single point-to-point connection in the network, for example, a VoIP call.
Network Storage Function	NSF. The Network Storage Function provides access to the Network Information Model.
NM	Network Manager. The NM product provides a framework for controlling and querying the element configurations in the broadband network.
Node	In networks, a processing location. A node can be a computer or some other device, such as a printer. Every node has a unique network address, sometimes called a Data Link Control (DLC) address or Media Access Control (MAC) address.
NSF	Network Storage Function. The NSF provides access to the Network Information Model.
O	
Object	An agent, controller, function, service, switch, or service within the Broadband Policy Manager (BPM).
Object Dependency	An exact object type, for example a Cisco 2500 router agent, that a service depends on. The service designer 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.
Object Type	In the BPDS, an object type is defined with attributes. It can own contain, and associate with other object types.
OC	Orchestration Controller. That portion of the Broadband Policy Managers (BPM) that controls processes such as username and password authentication.
Operation and Support System	OSS. OSS refers to a suite of programs that enable an enterprise to monitor, analyze, and manage a network system. The term originally referred to a management system that controlled telephone and computer networks. It now applies to the business world to mean a system that supports network operations.
Operator	A representation of actions to be undertaken on a system networked to a Broadband Policy Managers (BPM).
Orchestration Controller	OC. That portion of the Broadband Policy Managers (BPM) that controls processes such as username and password authentication.
Orchestration Network	The process for handling service calls over a network. It defines the flow of control and information between work units.

Table A-1. Terms and Definitions.

Term	Definition
OSS	Operation and Support Systems. OSS refers to a suite of programs that enable an enterprise to monitor, analyze, and manage a network system.
P	
Pad	A collection of pins on an operator. This appears as a box along the edge of an operator.
Path Computation Function	PCF. The PCF determines the path through the topology for any given end-to-end session, as requested by the ACF.
PCF	Path Computation Function. The PCF determines the path through the topology for any given end-to-end session, as requested by the ACF.
PDP	Policy Decision Point. The PDP is a component of policy-based management. When a user tries to access a file or other resource on a system using policy-based access management, the PDP decides whether or not to authorize the user based on user attributes.
PE	Policy Engine. The software that stores and manages user profile information, subscriber access records, policy rules; also known as the policy database.
PEP	Policy Enforcement Point. The PEP is the logical entity or place on a server that makes admission control and policy decisions in response to a request from a user wanting to access a resource on a computer or network server.
PHP	Hypertext Preprocessor (PHP). PHP is an open source, server-side, HTML embedded scripting language used to create dynamic Web pages.
PIF	Protocol Interface Function. A PIF service encapsulates an interface with an external device or service
PIF Agent	An Agent that acts an adaptor between the system and an external device or service.
Pin	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.
PMF	Profile Management Function. The Profile Management Function (PMF) activates and deactivates network profiles on subscriber sessions.
Point-to-Point Protocol Over ATM	PPPoA. PPPoA relies on two widely accepted standards: PPP and ATM. It is an end-to-end asymmetric digital subscriber line (ADSL) architecture.
Point-to-Point Termination Aggregation	PTA. This is a method of aggregating IP traffic by terminating PPP sessions and amassing the IP traffic into a single routing domain.
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 subscriber 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.

Table A-1. Terms and Definitions.

Term	Definition
Policy Database	The database of policy objects that services access to make policy decisions.
Policy Decision Point	PDP. The PDP is a component of policy-based management. When a user tries to access a file or other resource on a system using policy-based access management, the PDP decides whether or not to authorize the user based on user attributes.
Policy Enforcement Point	PEP. The PEP is the logical entity or place on a server that makes admission control and policy decisions in response to a request from a user wanting to access a resource on a computer or network server.
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.
Policy Repository	The Policy Repository BPM stores all persistent data associated with customers and services. It utilizes industry-standard database technology that allows any of the underlying system elements to interrogate it.
Pool	A pool represents a range of IP addresses. A BRAS handles one or more address ranges. A Resource Controller potentially handles multiple BRASs. So a typical Resource Controller can handle multiple ranges of IP addresses (multiple pools).
PPPoA	Point-to-Point Protocol Over Asynchronous Transfer Mode. PPPoA relies on two widely accepted standards: PPP and ATM. It is an end-to-end asymmetric digital subscriber line (ADSL) architecture.
Presence Director	The Presence Director is an optional, modified, Director service that handles receives session requests and distributes them to the appropriate Resource Controllers.
Profile	A profile is a procedure for changing a set of related network elements for a given purpose, for example, increasing the bandwidth associated with a network session.
Profile Management Function	PMF. The Profile Management Function (PMF) activates and deactivates network profiles on subscriber sessions.
Property	The parameter or characteristic of an agent or device.
Protocol Interface Function	PIF. A PIF service encapsulates an interface with an external device or service.
PTA	Point-to-Point Termination Aggregation. This is a method of aggregating IP traffic by terminating PPP sessions and amassing the IP traffic into a single routing domain.
Q	
QoS	Quality of Service. QoS specifies a guaranteed throughput level that allows providers to guarantee to their customers that end-to-end latency will not exceed a specified level.
Quality of Service	QoS. QoS specifies a guaranteed throughput level that allows service providers to guarantee to their customers that end-to-end latency will not exceed a specified level.

Table A-1. Terms and Definitions.

Term	Definition
R	
RACS	Resource and Admission Control Subsystem. RACS consists of the Policy Decision Function (PDF) and Access-RAC Function (A-RACF), which controls QoS within the access network.
RADIUS	Remote Authentication Dial-In User Service. RADIUS is a client/server protocol enabling remote access server communication with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database and set up a policy that can be applied at a single administered network point.
Realm	A realm represents a collection of information, stored in the database, that should be transferred, as a unit, between BPM systems. The realm defines a unit for intersystem communication and improves performance by restricting lookups and updates against smaller data sets.
Remote Authentication Dial-in User Service	RADIUS. RADIUS is a client/server protocol enabling remote access server communication with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database and set up a policy that can be applied at a single administered network point.
Remote Method Invocation	RMI. RMI is the basis of distributed object computing in the Java environment. It defines how Java components can interoperate in a Java environment.
Resource	A resource is any device or other item that can be used. Devices such as printers and disk drives are resources. Memory is also a resource. In many operating systems, a resource is specifically data or routines that are available to programs. These are also called system resources.
Resource and Admission Control Subsystem	RACS. RACS consists of the Policy Decision Function (PDF) and Access-RAC Function (A-RACF), which controls QoS within the access network.
Resource Controller	A Resource Controller is a stateful installation that tracks resource utilization for the system.
Resource Realm	A Resource Realm represents a BRAS device and its connected CPE equipment. The Resource Realm is provisioned on the Topology Database Server and distributed to the Resource Controller that coordinates activity for that BRAs. At runtime, the Resource Realm stores capacity and usage information required to perform CAC decisions.
RMI	Remote Method Invocation. RMI is the basis of distributed object computing in the Java environment. It defines how Java components can interoperate in a Java environment.
Role	A role is as a functional category for device types and device instances. For example, *bras* and *dpi* are roles.

Table A-1. Terms and Definitions.

Term	Definition
Role-based Dependency	A dependency in which a service designer indicates that multiple service elements support the same interface. The designer 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 route is a path between operators.
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 subscriber. 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	
S-VLAN	Stacked VLAN. An S-VLAN provides a two-level S-VLAN tag structure that extends the VLAN ID space to more than 16 million VLANs.
SAV	Service Admin view. In the BPS and BPDS graphical user interfaces to the BPM, this is the view where you can perform service tasks.
Schema	A set of rules and syntax for storing data.
SDV	Service Design view. In the BPS and BPDS graphical user interfaces to the BPM, this is the view where you can design services.
SE	Service Engine. SE is an unassigned and unconfigured system. It is also known as the backend.
Service	An application, created by the BPM designer, 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) and can comprise one or more flows.
Service Admin View	SAV. In the BPS and BPDS graphical user interfaces to the BPM, this is the view where you can perform service tasks.
Service Configuration	The information needed to construct a service. The service configuration specifies agent configurations for each function in the service type. The BPM designer creates the service configuration.
Service Dependency	The dependencies of a service, created by the service designer. The designer builds a service by defining data-flows that use operators from multiple objects, including agents and other services. The designer builds a service upon a concrete set of agents and services. If a service is portable across different agents and services, the designer specifies any constraints on the concrete instances and specifies the interfaces that those concrete instances must support.
Service Design View	SDV. In the BPS and BPDS graphical user interfaces to the BPM, this is the view where you can design services.
Service Engine	SE. SE is the generic term for an unassigned and unconfigured system. it is also known as the backend.
Service Interface Dependency	If a service uses a particular service interface, but does not require that a specific object provide the service interface, the service designer 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.

Table A-1. Terms and Definitions.

Term	Definition
Service Instance	The running of a service type created by the subscriber.
Service Level Agreement	SLA. An SLA is a contract between an ASP and the end user that stipulates the required level of service and its fee.
Service Palette	The agent types available to a service.
Service Profile	A collection of services and information about service execution.
Service Provider	SP. This is the provider of Internet connectivity services.
Service Type	The definition of what agent types are required for a service; the defined flow of data between functions of agent types. The service designer creates the service type.
Servlet	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.
Session Management Application	SMA. Within the Session Manager, the SMA encapsulates customer-specific business logic for managing network sessions.
Session Management Function	SMF. The SMF encapsulates customer-specific business logic applied to network sessions. Abstracted from specific protocols and devices used in the network through the DAF and PIF layers, the SMF notifies applications of session state changes.
Session Manager	SM. The SM provides a framework for tracking user sessions connecting to the network.
Session Realm	A Session Realm stores Session Manager contexts and assists in the decision-making process during network adaptation.
Session Storage Function	SSF. The SSF provides access to the Session Information Model.
SF	Statistics Function. The SF records and queries system statistics and provides a location for various components to store runtime state statistics.
Shared Secret	An authentication string that ensures security between devices. KERBEROS is an instance of a shared-secret authentication protocol.
SIF	Signaling Interface Function (SIF): The SIF sends QoS requests from an application to the Director ACF. If more than one Director exists, an external Load Balancer selects a Director. The SIF receives replies from Director ACFs and forwards them to the application.
Signaling Interface Function	SIF. The SIF sends QoS requests an application to the Director ACF. If more than one Director exists, an external Load Balancer selects a Director. The SIF receives replies from Director ACFs and forwards them to the application.
Simple Object Access Protocol	SOAP. This is a lightweight XML-based messaging protocol that encodes the information in Web service request and response messages before sending them over a network. SOAP messages are independent of any operating system or protocol and may be transported using a variety of Internet protocols, including SMTP, MIME, and HTTP.
Simple Type	In the BPDS Object manager tool, a simple type is similar to data type, except it can express with enumerations.

Table A-1. Terms and Definitions.

Term	Definition
Simple Network Management Protocol	SNMP. A protocol by which networked devices are periodically polled for information as part of a network management system.
SLA	Service Level Agreement. An SLA is a contract between an ASP and the end user that stipulates a required level of service and its fee.
SM	Session Manager. The SM provides a framework for tracking user sessions connecting to the network.
SMA	Session Management Application. Within the Session Manager, the SMA encapsulates customer-specific business logic for managing network sessions.
SMF	Session Management Function. The SMF encapsulates customer-specific business logic applied to network sessions. Abstracted from specific protocols and devices used in the network through the DAF and PIF layers, the SMF notifies applications of session state changes.
SNMP	Simple Network Management Protocol. A protocol by which networked devices are periodically polled for information as part of a network management system.
SOAP	Simple Object Access Protocol. This is a lightweight XML-based messaging protocol that encodes the information in Web service request and response messages before sending them over a network. SOAP messages are independent of any operating system or protocol and may be transported using a variety of Internet protocols, including SMTP, MIME, and HTTP.
SP	Service Provider. This is the provider of Internet connectivity services.
Specification	A type definition that includes interface definitions, configuration schemas, and binding information.
SQL	Structured Query Language. SQL is a standardized query language for requesting information from a database. SQL enables several users on a local-area network to access the same database simultaneously.
SSF	Session Storage Function. The SSF provides access to the Session Information Model.
Stacked VLAN	S-VLAN. An S-VLAN provides a two-level S-VLAN tag structure that extends the VLAN ID space to more than 16 million VLANs.
Standby BPM	In a pair of BPMs, the standby BPM constantly monitors the health of the active BPM to assess its ability to process requests. If the active BPM is not viable, the standby BPM becomes the active.
Statistics Function	SF. The SF records and queries system statistics and provides a location for various components to store runtime state statistics.
Status	A status is a condition used in conjunction with network sessions.
Structured Query Language	SQL. SQL is a standardized query language for requesting information from a database. SQL enables several users on a local-area network to access the same database simultaneously.
Subscriber	A customer of a service provider. The service provider delivers a variety of online services, including e-mail, stock quotes, news, and online forums.
Subscriber Profile	A table entry containing information, such as authentication, authorization, and location on a specific subscriber.

Table A-1. Terms and Definitions.

Term	Definition
Super Operator	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.
Switch	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.
Super User	The term denotes the highest level of user privilege. It allows unlimited access to a system. Usually, super user is the highest level of privilege for applications, as opposed to operating or network systems.
T	
TAF	Topology Awareness Function. The TAF extracts and reacts to changes in the underlying network. The information can be read from provisioning files or received from the TDS.
TISPAN	Telecommunications and Internet Services and Protocol for Advanced Networking. TISPAN is the ETSI core competence center for fixed networks and for migration from switched circuit networks to packet-based networks with an architecture that can serve in both. TISPAN is responsible for all aspects of standardization for present and future converged networks.
Telecommuni-cations and Internet Services and Protocol for Advanced Networking	TISPAN. TISPAN is the ETSI core competence center for fixed networks and for migration from switched circuit networks to packet-based networks with an architecture that can serve in both. TISPAN is responsible for all aspects of standardization for present and future converged networks.
Topology Awareness Function	TAF. The TAF extracts and reacts to changes in the underlying network. The information can be read from provisioning files or received from the TDS.
Topology Database Server	In resilient pairs, Topology Database Servers maintain the global topology database for the system as a whole. The Director detects delayed response times or dropped requests and notifies the Topology Database Server. The Topology Database Server initiates Resource Controller failover when necessary.
Topology Store Function	TSF. The TSF maintains the TIM for a given BP Resource Controller system component.
Transaction Remote Procedure Call	TRPC. The TRPC protocol is the interface between Cisco BPM components.
TRPC	Transaction Remote Procedure Call.The TRPC protocol is the interface between Cisco BPM components.
TSF	Topology Store Function. The TSF maintains the TIM for a given BP Resource Controller system component.
Type	A BPM component group that has a unique specification. It may have an implementation, and it may have one or more configurations and instances.
U	
V	

Table A-1. Terms and Definitions.

Term	Definition
VC	Virtual Circuit. A connection between two devices that acts as though it's a direct connection even though it may physically be circuitous.
Virtual Circuit	VC. A VC is a connection between two devices that acts as though it's a direct connection even though it may physically be circuitous.
Virtual LAN	VLAN. A network of computers that behave as if connected to the same wire even though they can be physically located on different segments of a LAN. VLANs are configured through software rather than hardware and extremely flexible.
Virtual Path	VP. A VC is a set of links across an ATM network between two specified end points.
Virtual Private Network	VPN. A VPN is constructed using public wires to connect nodes. A number of systems exist that enable the creation of networks using the Internet as the medium for transporting data. They use security mechanisms to ensure that only authorized users can access the network and data cannot be intercepted.
VLAN	Virtual LAN. A network of computers that behave as if they are connected to the same wire even though they may be physically located on different segments of a LAN. VLANs are configured through software rather than hardware and are extremely flexible.
Voice-over-IP	VoIP. Voice delivered using the Internet Protocol.
VoIP	Voice-over-IP. Voice delivered using the Internet Protocol.
VP	Virtual Path. VP. A VP is a set of link across an ATM network between two specified end points.
VPN	Virtual Private Network. A VPN is constructed using public wires to connect nodes. A number of systems exist that enable the creation of networks using the Internet as the medium for transporting data. They use security mechanisms to ensure that only authorized users can access the network and data cannot be intercepted.
W	
WDSL	Wireless Digital Subscriber Line. WDSL is an XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information. It is extensible to allow description of endpoints and their messages regardless of what message formats or network protocols are used to communicate.
Wireless Digital Subscriber Line	WDSL. WDSL is an XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information. It is extensible to allow description of endpoints and their messages regardless of what message formats or network protocols are used to communicate.
Workspace	The BPDS area where the designer visually programs services.

Index