Oracle® Communications IP Service Activator

QoS User's Guide

Release 7.5
F59544-01
September 2022

ORACLE

Oracle Communications IP Service Activator QoS User's Guide, Release 7.5

F59544-01

Contents

Preface

Audience viii
Documentation Accessibility viii
Diversity and Inclusion viii

1 Applying a QoS or Access Control Policy

Overview 1-1
- Standard PHB and Modular QoS CLI PHB Groups 1-3

Policy Roles 1-4
- Using Roles in Policy Elements 1-5

Policy Inheritance 1-6
Before Implementing a QoS or Access Control Policy 1-9
- Set Up Basic Data 1-10
- Check Capabilities 1-10
- Set Up and Assign Policy Roles 1-10
- Assign Traffic to Appropriate Classes of Service 1-11
- Consider Where to Apply Policy Elements 1-11
- Organizing QoS Objects Into User-defined Folders 1-12
- Marking on Cisco Routers 1-12

2 Setting Up Basic Policy Data

Importing QoS-related Policy Files 2-1
- The default.policy File Summary 2-1
  - The default.dscp.policy File 2-2
- The advanced.policy File Summary 2-2
- Additional Policy Files 2-2
- Loading Policy Configuration Files 2-2

Class of Service Data 2-3
- DiffServ Codepoints 2-4
- IP Precedence 2-5
- MPLS Experimental Bits 2-5

MPLS Topmost Experimental Bits 2-5
Frame Relay Discard Eligible Bit 2-6
ATM Cell Loss Priority Bit 2-6
Discard-class 2-6
Trust Type 2-6
The advanced.policy File Details 2-6
Creating a New Packet Marking 2-8
Flexible IP Precedence and DSCP Support 2-9
Defining Packet Markings in Cisco IOS Cartridge Configuration Options 2-9
Classes of Service 2-10
Policy Components 2-12
Setting Up Traffic Types 2-12
Setting Up a Compound Traffic Type 2-15
Setting Up a Traffic Type Group 2-16
Setting Up a Classification 2-16
Using Classifications with Policy Rules 2-17
Using Classifications with MQC PHB Groups 2-17
Aggregation 2-20
Strict Aggregation 2-23
Setting Up a Date and Time Template 2-24
Setting Up IP Protocols 2-24
Setting Up Accounts 2-25

3 Defining QoS and Access Control

Introduction 3-1
Using Roles in Rules 3-2
Rule Support on an Interface 3-4
Using Roles in Rules 3-5
Classification Rules 3-5
Setting Up a Classification Rule 3-7
Policing Rules 3-8
Access Rules 3-10
Copying Classification, Policing and Access Rules 3-11
Using the Deny Classification in Cisco ACLs 3-12
User Interface 3-12
Updating Multiple Rules 3-13
Copying Rules 3-14
Implementing Rules 3-15
Checking Implemented Rules 3-15
Viewing Implemented Rules 3-15

Viewing System Statistics and Statistic Summary Information 3-15
Managing Rules 3-16
Changing the Sequence Order of Rules 3-16
How Rule Conflicts are Avoided 3-16
Disabling Rules 3-17

4 Defining Standard Per Hop Behavior Groups

Introduction 4-1
Supported Traffic Shaping/Queuing Mechanisms 4-1
Class of Service Mechanisms 4-2
VC Traffic Shaping Mechanisms 4-2
Vendor Support 4-2
Class of Service Mechanism Combinations 4-3
Before Setting Up a Standard PHB Group 4-4
Selecting the Queuing or Traffic Shaping Mechanisms 4-4
Deciding Where to Apply the Standard PHB Groups 4-4
Using Roles in PHB Groups 4-5
Importing Policy Files 4-5
Setting Up a Standard PHB Group 4-5
Setup and Application of PHB and MQC PHB Groups as Separate Operations 4-5
Setup and Application of PHB and MQC PHB Groups as a Combined Single Operation 4-6
Setting Up a Standard PHB Group 4-6
Setting up Weighted Round Robin 4-7
Setting up Priority Queuing 4-7
Setting Up Rate Limiting 4-8
Setting Up Weighted Random Early Detection 4-8
Setting Up Weighted Fair Queuing 4-9
Setting Up ATM Traffic Shaping 4-11
Setting Up Frame Relay Traffic Shaping 4-11
Distributed Traffic Shaping 4-12

5 Extending IP Service Activator with Configuration Policies

About Configuration Policies 5-1
Obtaining and Creating Configuration Policies 5-1
Getting More Information About Configuration Policies 5-2
Configuration Policy Groupings 5-2
Viewing and Customizing the Organization of Configuration Policies 5-2
Applying Configuration Policies 5-4
Disabling Applied Configuration Policies 5-4

Applying Configuration Policies at the Device Level 5-4
General Device-Level Configuration Policies 5-5
User Authentication Configuration Policy 5-5
User Data Configuration Policy 5-6
Using Collection-Based Configuration Policies 5-6
QoS and Attachment Configuration Policies 5-7
Vendor Cartridge Support for Various QoS Configuration Policies 5-7
Overview of Attachment QoS Policies 5-7
Overview of Vendor-Specific QoS Policies 5-8
QoS Configuration Policies 5-8
Installation of QoS and Attachment Configuration Policies 5-8
Role-based Inheritance 5-8
Attachment QoS Configuration Policies 5-8
qosCosAttachment 5-9
Vendor-Specific QoS Configuration Policies 5-9
Cisco QoS Configuration Policies 5-9
CatOSPolicingRule 5-9

6 Implementing and Managing Per Hop Behavior Groups

Implementing a PHB Group 6-1
Associating a PHB Group with a Policy Target 6-1
Committing the Transaction 6-1
Checking Implemented PHB Groups 6-2
Abstract and Concrete PHB Groups 6-2
PHB Group Status 6-2
Viewing Implemented PHB Groups 6-3
Information Displayed About PHB Groups 6-3
Changing the Evaluation Order of PHB Groups 6-4

7 Defining MQC PHB Groups

Introduction 7-1
Supported Traffic Management Mechanisms 7-2
Before Setting Up an MQC PHB Group 7-3
Deciding Which QoS Actions to Select 7-3
Defining Classes of Service 7-3
Check Capabilities 7-3
Deciding Where to Apply MQC PHB Groups 7-3
Using Roles in MQC PHB Groups 7-4
Setting Up an MQC PHB Group 7-4

Specifying Evaluation Order 7-6
Setting Up Low Latency Queuing 7-7
Multi-Level Priority Queuing 7-7
Setting Up Class-Based Weighted Fair Queuing 7-9
Setting Up Class-Based Policing 7-9
Setting Up a Policing Action 7-12
Applying a Policing Action 7-13
Setting Up Class-Based Shaping 7-14
Setting Up Class-Based Marking 7-16
Setting Up Congestion Avoidance 7-16
Nesting MQC PHB Groups 7-17
RTP Header Compression 7-19

8 Example Policy Setups

Using Roles to Apply Policy 8-1
Requirements 8-1
Solution 8-2
Applying Policy to a VC Endpoint 8-4
Using Classifications in Rules 8-6

Preface

This guide explains how to configure quality of service (QoS) and access control policies with Oracle Communications IP Service Activator.

Audience

This guide is intended for network configuration engineers.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

1

Applying a QoS or Access Control Policy

This chapter introduces the Oracle Communications IP Service Activator elements that can be used to define a QoS or security policy and highlights some of the issues you need to consider. This chapter:

- Outlines IP Service Activator's rules, Per Hop Behavior (PHB) groups and driver scripts.
- Describes the policy roles that enable you to group sets of devices and interfaces and so apply policy on a group by group basis.
- Explains how to use policy roles in the policy elements you define.
- Describes IP Service Activator's policy inheritance model.
- Outlines the tasks involved in setting up a QoS or access control policy.
- Highlights some of the points you need to consider when setting up a QoS or security policy.
- Explains how to implement the QoS or access control policy and describes what happens when policy is propagated to the network.
- Describes IP Service Activator's concept of abstract and concrete policy elements and explains how they appear in the user interface.

Overview

IP Service Activator provides the following basic building blocks for creating a QoS or access control policy:

- Policy rules: There are the following rule types, each with a distinct function:
  - Classification rules enable you to mark traffic and optionally manage bandwidth.
  - Policing rules police the bandwidth used by a particular traffic type and, optionally, re-mark traffic.
  - Access rules implement security by permitting or denying traffic.
- PHB groups allow QoS mechanisms to be applied to interfaces. There are the following types of PHB groups:
  - Standard PHB groups: Allow you to implement QoS mechanisms.
  - MQC PHB groups: Allow you to implement Modular QoS CLI mechanisms developed by Cisco to simplify the configuration of QoS on all device types.
- Configuration policies: Flexible way of expressing configuration models and extending IP Service Activator functionality within a policy framework.

These basic building blocks are collectively referred to as policy elements.

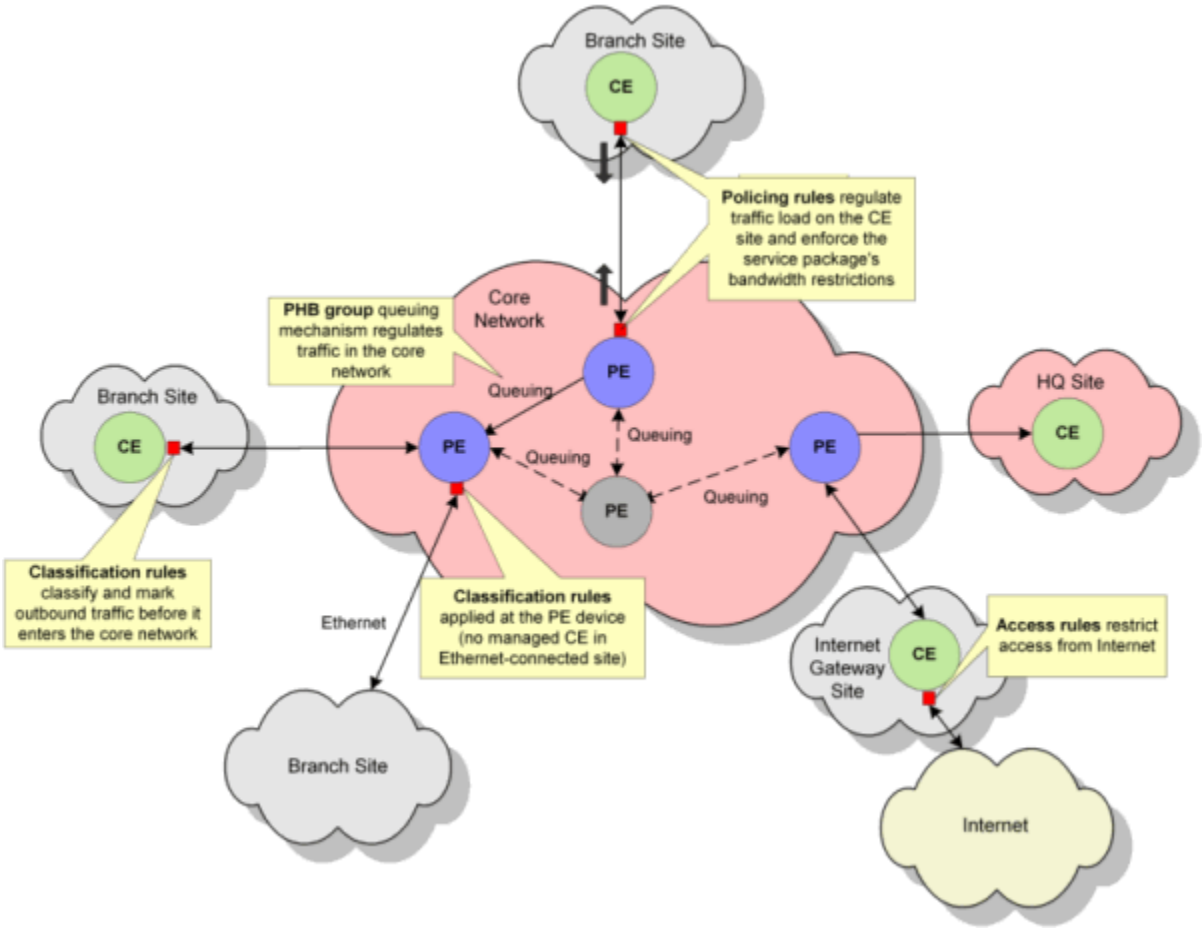
Figure 1-1 illustrates how and where you might apply rules and standard PHB groups.

IP Service Activator provides an easily maintainable method for applying policy through a policy inheritance model and the concept of roles. The inheritance model enables policy defined at a high level, such as the domain or network, to be inherited to lower level objects,

such as devices and interfaces. Roles enable you to group devices and interfaces by, for example, customer and service package, and create policy targeted at that group. Policy can be directed towards specific groups of devices and interfaces.

Rules, PHB groups, and configuration policies can be applied to any policy target – that is, a customer, VPN or site, or a network component such as a device or interface. The configuration associated with a policy element is inherited through the inheritance model and applied at the relevant devices, interfaces, sub-interfaces or VC endpoints.

Figure 1-1 Rules and Standard PHB Application



> **Note:**
>
> You can apply rules, configuration policies, and PHB groups to domains.

To support the definition of rules, a range of rule components can be defined and used within any number of policy rules. A number of these components can be created by loading a set of example policy files.

See "Setting Up Basic Policy Data " for more information about rule components. See "Importing Policy Files" for information about loading example policy files into IP Service Activator.

Standard PHB and Modular QoS CLI PHB Groups

Standard PHB groups provide a method for implementing a QoS policy mechanism for traffic queuing and/or shaping on the interfaces of specific device types. The QoS mechanism that you select is applied to all of the classes of service associated with the standard PHB group. You can apply other QoS policies to the same interfaces using policing and classification rules. The Class of Service (CoS) that is associated with a PHB group is defined by packet marking. See "Defining Standard Per Hop Behavior Groups " for more information about standard PHB groups.Modular QoS CLI (MQC) PHB groups use Cisco's simplified configuration of policy mechanisms and actions for traffic queuing, shaping, policing, congestion avoidance and re-marking on the interfaces of Cisco routers and switches. MQC PHB groups differ from standard PHB groups in a number of ways:

- They provide a wider range of QoS mechanisms than standard PHB groups – for example, they can be used to police and classify traffic as well as applying a queuing mechanism.
- Several different QoS mechanisms may be specified for each of the classes of service associated with an MQC PHB group.
- The traffic class that an MQC PHB group applies to is defined by a classification or classification group, unlike standard PHB groups that apply to traffic characterized by a packet marking.

> **Note:**
>
> You can associate a CoS defined by a classification or classification group and/or a packet marking with an MQC PHB group but packet markings are ignored. If you wish to define a traffic class that is characterized by a packet marking, you must create a packet marking traffic type and associate it with a classification.

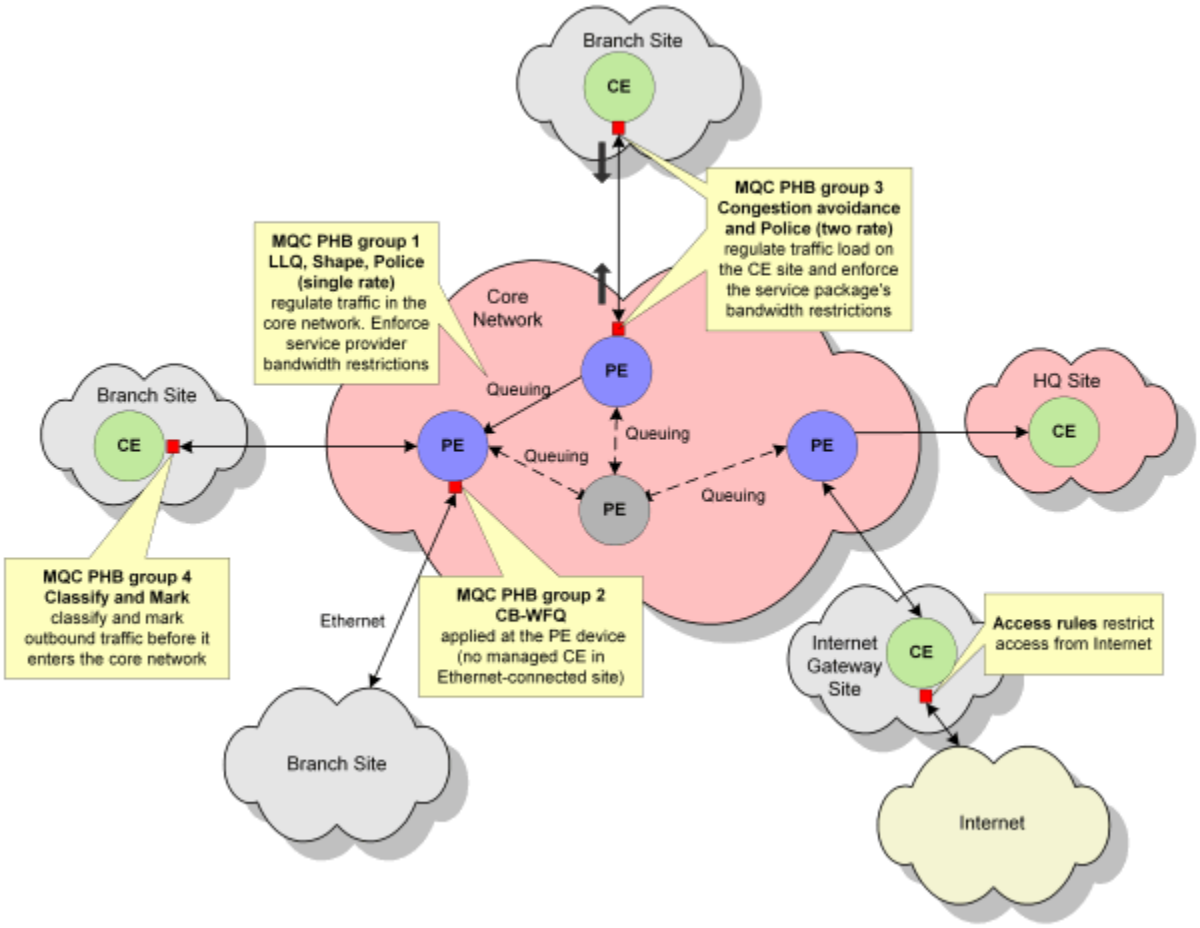
- MQC PHB groups can be nested, enabling you to re-use an MQC PHB group that defines QoS actions for one or more classes of service in multiple 'parent' MQC PHB groups.

> **Note:**
>
> In many instances, policy rules and MQC PHB groups can be configured on the same interface. Note, however, that if a classification rule is configured on an interface using policy maps, you cannot configure an MQC PHB group on the same interface. For information about which mechanisms and options are used to configure classification rules, see the applicable cartridge guide.

See "Defining MQC PHB Groups " for more information about MQC PHB groups.

Figure 1-2 illustrates how and where you might apply MQC PHB groups.

Figure 1-2 MQC PHB Group Application



Policy Roles

Some policies apply throughout the network while other policies apply only at certain points. Roles enable you to group a set of policy targets – such as a set of devices or interfaces – and apply one or more policies and PHB groups to the policy target group. Roles can be assigned to network components at the device level and below and associated with policy elements. By applying roles to selected policy targets, rules and PHB groups, you define the policy that will be applied at specific points in the network.

IP Service Activator supports two types of roles:

- System-defined roles: A set of system-defined roles automatically provided to classify devices and interfaces according to their function in a VPN.
- User-defined roles: Roles created by users to support their own policy setup.

You can use system-defined and user-defined roles in combination. For policy targets and policy elements, you can assign one system-defined role and/or any number of user-defined roles. For policy elements, you can assign one system-defined role and zero or one user-defined roles.

The number and type of roles you choose to create will depend on the network to be managed and the number of variables you need to control. As an example, you might

create roles for each service package, customer and bandwidth connection that feature in the network.

For more information on defining roles and assigning them to policy targets, see *IP Service Activator User's Guide*.

Using Roles in Policy Elements

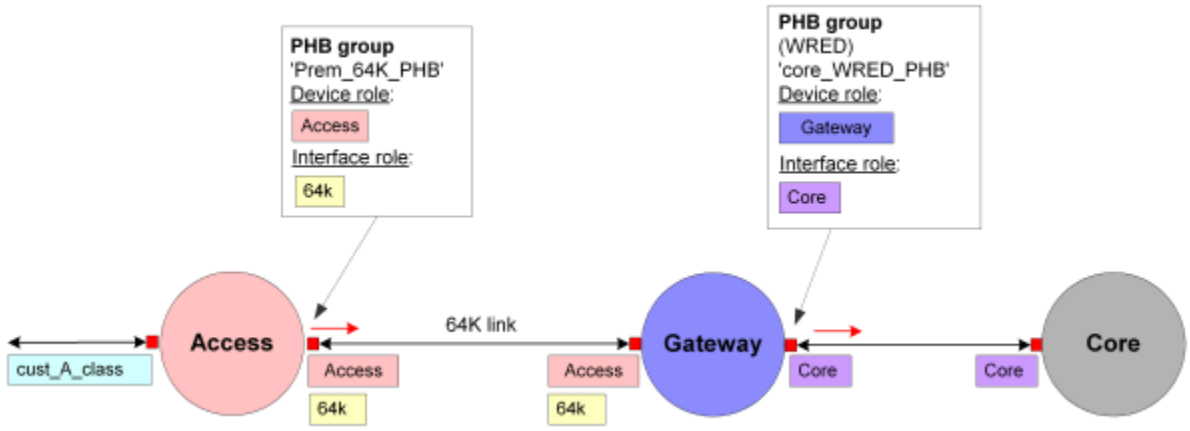
In order for a policy element to be applied to a policy target, it must have both a device and an interface role associated with it. This role combination specifies where the policy element will be applied. For example, by associating the Gateway device role and Access interface role with a PHB group, configuration is applied only at Access interfaces on Gateway devices.

> **Note:**
>
> When you create a policy element there are no policy roles associated with it by default. You must associate both a device and an interface role for the policy element's configuration to be applied at the appropriate points in the network. If either the device or interface role are not specified, no configuration is applied.

There are also device configuration policies that use only a device role; there is no interface role defined for device configuration policies.

Figure 1-3 illustrates the use of roles in PHB groups. Roles are used within two PHB groups – **Prem_64K_PHB** and **core_WRED_PHB** – to target policy at interfaces that are tagged with matching roles.

Figure 1-3 Using Roles in PHB Groups



For both device and interface roles, you can associate one system-defined role and zero or more user-defined roles with a policy element. If a policy element has only one device and/or interface role associated with it, its policy is applied to policy targets whose assigned roles include that role – that is, the policy target may have additional roles assigned to it. For example, if a policy element has the following roles associated with it:

- Device role: Access
- Interface role: 64K

Configuration will be applied to interfaces tagged with roles named Core and 64K as well as those tagged with the 64K role only, provided the parent device's assigned roles include Access.

Where two or more device or interface roles are specified, the policy element is only applied to policy targets tagged with all of the specified roles. For example, if a policy element definition specifies the following:

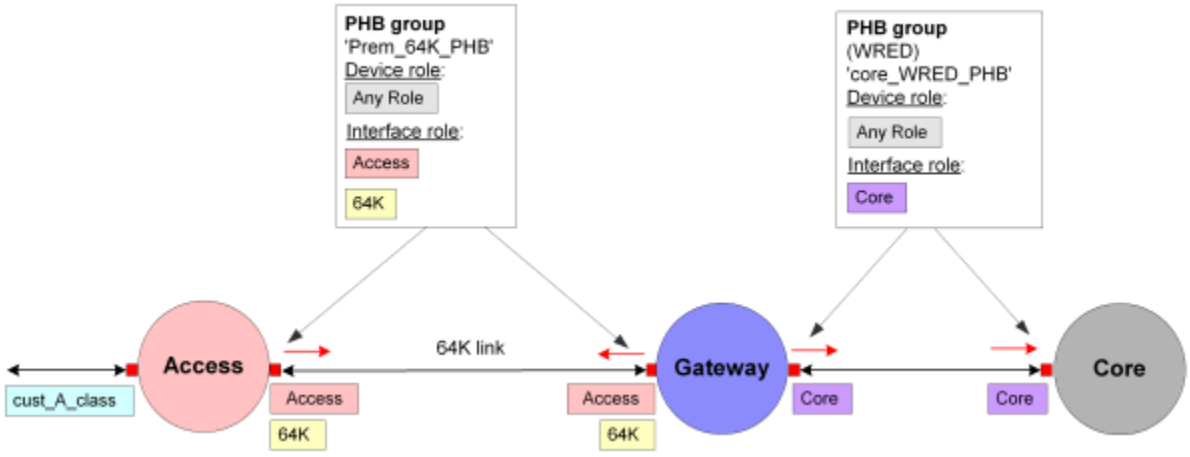
- Device roles: Access
- Interface roles: Access, 64K

Configuration will be applied only to interfaces tagged with the Access and 64K roles whose parent devices are tagged with the Access role. Configuration is not applied if the interface is tagged with only one of the specified roles.

> **Note:**
>
> The system-defined role **Any Role** can be specified within a policy element definition as the device and/or interface role. This role acts as a wildcard, effectively instructing IP Service Activator to ignore the device and/or interface role. However the device or interface must have at least one role in order for **Any Role** to match it.

In Figure 1-4, **Any Role** is specified as the device role. IP Service Activator therefore disregards the device role (as long as the device has a role) and applies the policy element wherever the interface roles match those in the policy element definition.

Figure 1-4 Any Role Example



Policy Inheritance

IP Service Activator supports a policy inheritance model – QoS or access control policy applied to a policy target is automatically inherited by lower-level objects. For

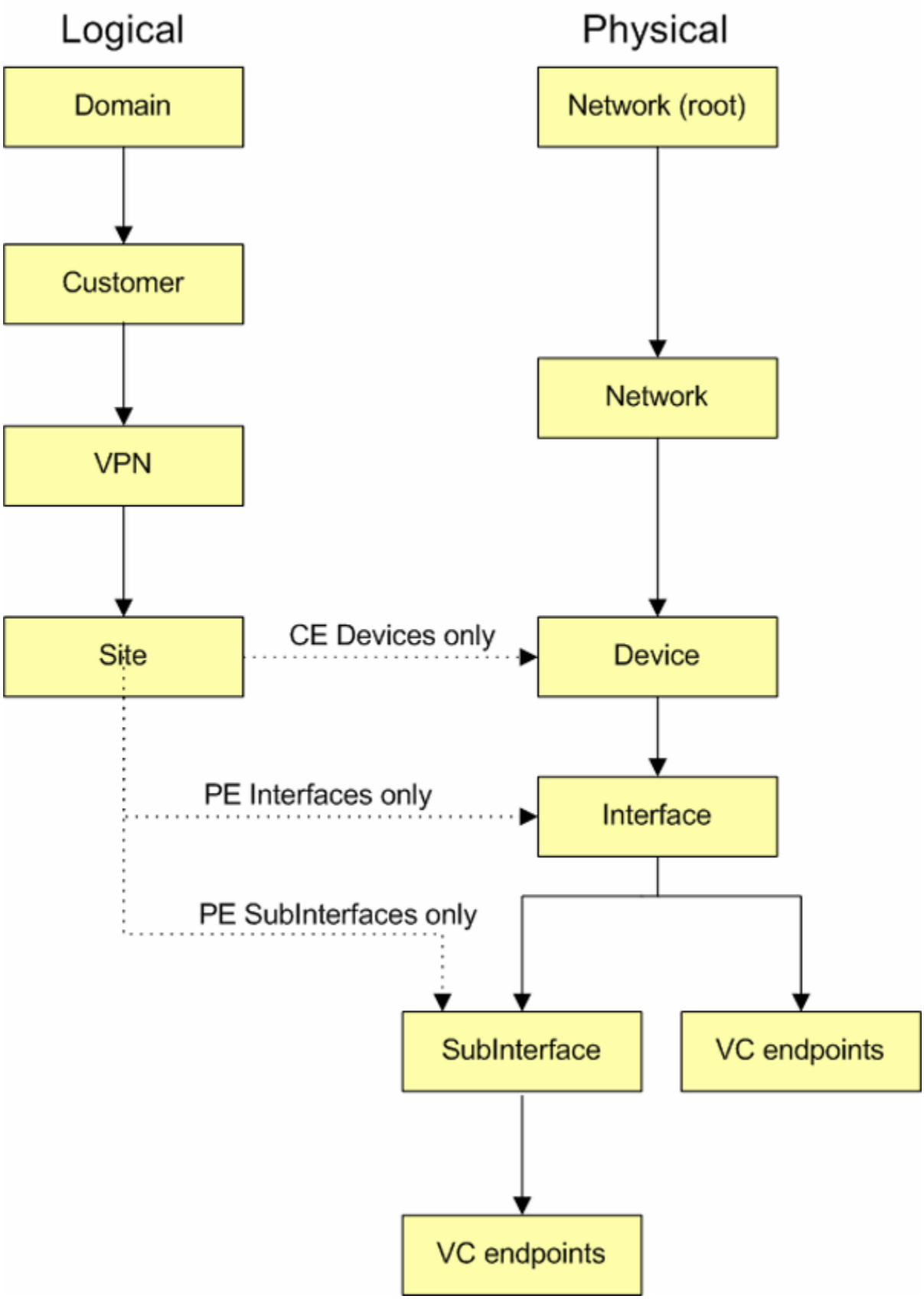
example, a rule that is applied to the network is inherited by the devices that make up that network. Note that devices and interfaces must be tagged with the appropriate role(s) for policy to be inherited.

There are the following branches in the inheritance model:

- Logical: Includes domains, customers and VPNs.
- Physical: Tncludes networks, devices and interfaces.

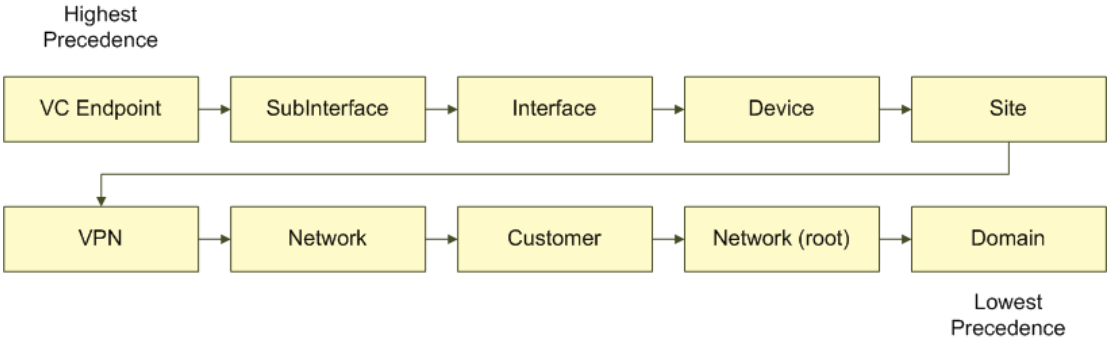
The branches converge at device level. Figure 1-5 shows an example of inheritance.

Figure 1-5 Inheritance



Where policy is defined at a low-level object (high precedence), and would conflict with an inherited policy (low precedence), the locally-defined policy takes precedence over the inherited policy. See Figure 1-6 for the full list of objects in order of policy precedence from high to low.

Figure 1-6 Policy Precedence, High to Low



In the case of rules, locally-defined rules are evaluated before inherited rules. For PHB groups, only one PHB group can be applied to an interface. However, it is possible for a concrete standard PHB group configured with either Frame Relay traffic shaping or ATM traffic shaping to be installed on the same interface as a concrete MQC PHB group that is configured with other QoS mechanisms.

A locally-defined PHB group overrides a PHB group applied at a higher level. This means you can define broad high-level policies and refine or supplement those policies at lower points in the hierarchy.

> **Note:**
>
> Policy applied to a customer is inherited to a site, unless the site is a member of a VPN to which a policy element of the same type has been applied. In this case, the policy applied to the VPN overrides that applied to the customer. This is valid only for policies applied through MQC PHBs or Standard PHBs.

When you view the policy that applies to a policy target, IP Service Activator indicates whether it has been inherited from above or defined at the policy target. See "Checking Implemented Rules" and "Checking Implemented PHB Groups" for more information.

Before Implementing a QoS or Access Control Policy

A detailed analysis of the network to be managed and the requirements to be met are essential pre-requisites for implementing a QoS or access control policy.

This section outlines the tasks you need to perform and highlights the points you need to consider when setting up a QoS or access control policy. It assumes that a detailed analysis phase has been performed.

Set Up Basic Data

You need to make sure that you have set up all necessary CoS and rule component data before creating policy rules and PHB groups:

- Set up classes of service to associate with PHB groups.

  A CoS may be defined by a packet marking and/or a classification or classification group.
- Set up packet markings (for example, DiffServ codepoints, IP Precedence, MPLS experimental bits and MPLS Topmost experimental bits, Frame Relay DE bit, ATM CLP bit, Discard-class, Trust Types, COS, COS Inner, QoS Group).
- Set up traffic types that identify the categories of traffic that you want to manage.
- Set up classifications and classification groups that classify existing traffic types by source and/or destination if required.

  Classifications and classification groups can be associated with policy rules and with the classes of service that you associate with MQC PHB groups.
- Set up account groups that identify the source and destination points of the traffic to be managed. This is optional, as you can also identify source and destination points by IP address within a classification.
- Set up date and time templates, if relevant.

See "Setting Up Basic Policy Data " for more information.

Check Capabilities

Before setting up policy rules and PHB groups, you need to know the capabilities of the interfaces to which you intend to apply policy. Check the Capabilities property page on the properties dialog box of relevant interfaces if necessary. See *IP Service Activator User's Guide* for information about retrieving capabilities.

Set Up and Assign Policy Roles

Policy roles can be associated with network components and with rules, PHB groups, and configuration policies. By applying a role to a policy target you effectively specify which policy will be applied at that point. Before setting up rules and PHB groups, you should decide whether to use system and/or user-defined roles and decide which roles to apply to each policy target.

> **Note:**
>
> You must assign a role manually for each device. Do not use role assignment rules. For more information, see *IP Service Activator User's Guide*.

Assign Traffic to Appropriate Classes of Service

A CoS defines a class of traffic based on packet characteristics allowing traffic on the network to be identified. A CoS can be defined by one or more packet markings (coarse-grained) or by additional parameters such as source and/or destination IP address and traffic type (fine-grained). These additional parameters are defined by a classification or classification group.

> **Note:**
>
> Fine-grained and coarse-grained refer to component granularity. Smaller tasks requiring low latency (such as accessing specific client data) call for the use of fine-grained components in an application. Fine-grained components are used where smaller data packets are sent in short durations of time. Coarse-grained components have a wider reference and can be re-used in multiple contexts. Coarse-grained components are used where larger data packets are sent in longer time intervals.

A PHB group applies QoS mechanisms to classes of service that are associated with the PHB group. Therefore, before creating PHB groups you need to create suitable classes of service. Note the following:

- A standard PHB group applies to a CoS characterized by a packet marking
- An MQC PHB group applies to a CoS defined by a classification or classification group

If you associate a CoS that is associated with both a packet marking and a classification or classification group with a standard or MQC PHB group, each PHB group type ignores any irrelevant part of a CoS definition. For more information, see "Classes of Service".

Policy rules operate on traffic types, classifications or classification groups. If required, a policy rule can be associated with a class of service (CoS) by creating a policy rule that specifies either the same packet marking associated with the CoS or a classification or classification group that specifies a traffic type that has the same packet marking associated with the CoS. A CoS can have several packet markings and PHBs associated with it.

See "Setting Up Traffic Types" and "Setting Up a Classification" for more information.

Consider Where to Apply Policy Elements

Policy rules, PHB groups, and configuration policies can be created at various levels in IP Service Activator and are automatically inherited so that they are applied to interfaces tagged with the appropriate role. For example, a rule created at the domain level applies throughout the domain (if the rule's matching criteria are met), while one created at the device level applies to that device's interfaces only (again, if the rule's matching criteria are met).

> **Note:**
>
> There are also device configuration policies that use only a device role; there is no interface role defined for device configuration policies.

Organizing QoS Objects Into User-defined Folders

A number of QoS objects can be organized in the IP Service Activator GUI into folders and sub-folders:

- PHBs and MQC PHBs
- Classifications and classification groups
- CoS
- Roles

For example, PHBs and MQC PHBs are located under the **PHB Groups** folder in the **Policy** tab. To create a folder, right-click on the appropriate parent object under the **PHB Groups** folder, or the **PHB Groups** folder itself, and select **Add Folder** from the pop-up menu. To add a PHB or MQC PHB to an interface, simply drag and drop it.

User-defined folders for the other QoS objects are similarly created under their top-level system-defined folder in the **Policy** tab.

User-defined folders can contain sub-folders. Drag and drop operations can be used to move folders, or their contents. You can also define folder permissions to restrict access to a subset of users for these folders.

For more information on managing user-defined folders, refer to *IP Service Activator User's Guide*.

Marking on Cisco Routers

When using an MQC PHB group or a classification and/or a policing rule to implement a QoS policy on Cisco routers, you need to consider which marking mechanism to use.

The Cisco cartridge can mark packets in several different ways. Marking is applied either using Cisco route maps or by means of class maps and policy maps (Class-Based Marking) on devices that support MQC or Network–Based Application Recognition (NBAR). The ability to mark on an inbound or outbound interface depends on the Cisco device type. You should therefore check device capabilities before formulating policy rules. For information on checking device capabilities, see *IP Service Activator User's Guide*.

Alternatively, the cartridge can be configured to mark using the Committed Access Rate (CAR) mechanism, on either the inbound or the outbound interfaces. At present, CAR is implemented by means of a command-line parameter.

For detailed information, see *IP Service Activator Cisco IOS Cartridge Guide*.

2
Setting Up Basic Policy Data

This chapter describes the basic data you need to define before setting up a QoS or security policy for Oracle Communications IP Service Activator. This includes the following:

- Importing policy files: A brief description of how to load optional files that provide values for standard IP Precedence codepoints and MPLS experimental bits, and sample policy rules, role assignment rules, and Per Hop Behavior (PHB) groups. See "Extending IP Service Activator with Configuration Policies " for detailed information on configuration policies.
- Class of service (CoS) data: Needed if you are setting up a QoS policy.
- Rule components: IP protocols, traffic types, classifications, and date and time templates, used when setting up rules and classes of service.
- Accounts (optional): Used to identify the users of services.

Importing QoS-related Policy Files

Configuration policies are loaded through the same mechanism as other policy files. To use configuration policies, they must be pre-loaded. For details, see *IP Service Activator System Administrator's Guide*.

Various policy files are available to load pre-configured QoS definitions. The **default.policy** and **advanced.policy** files provide standard values for IP Precedence codepoints and MPLS experimental bits.

For details on the objects created by a policy file, see the file itself. The **default.policy** file is located at:

ServiceActivatorHome\Oracle Communications\Service Activator\SamplePolicy

The default.policy File Summary

The **default.policy** file creates some basic policy data, including basic Gold, Silver and Bronze classes of service and their associated codepoints and traffic types. If you do not load this default data, you will have to create all the basic component data yourself. Do not import this policy file into a domain into which an older **default.policy** file or **default.dscp.policy** file has been imported.

This file should be loaded first, before other policy files.

The **default.policy** file defines the Gold, Silver, and Bronze classes of service, shown in Table 2-1.

Table 2-1 The Default.Policy File Classes of Service

CoS	Packet Marking	Codepoint Value
Gold	IP Precedence 5	40

Table 2-1 (Cont.) The Default.Policy File Classes of Service

CoS	Packet Marking	Codepoint Value
Silver	IP Precedence 3	24
Bronze	IP Precedence 0	0

The default.dscp.policy File

The **default.dscp.policy** file creates DSCP values when loaded. This file is a variant of the **default.policy** file and is compatible with IP Service Activator releases prior to 5.1.3. Packet marking policies use DSCP values, instead of IP Precedence values. Do not import this policy file into a domain into which the new **default.policy** file has already been imported.

The advanced.policy File Summary

The **advanced.policy** file creates additional packet markings and classes of service, as well as classifications, classification groups and traffic types when loaded. This data is useful if your routers support the full range of DiffServ codepoints, IP Precedence value and/or MPLS experimental bits. Load the **default.policy** file before loading this file.

See "The advanced.policy File Details" for a list of standard DiffServ codepoints.

Additional Policy Files

You can load the following files that provide sample policy rules, role assignment rules, and PHB groups. You can use these as a basis for creating your own rules and PHB groups:

- **Rule_and_PHB.policy** file: Creates some example policy rules, PHB groups and role assignment rules. Load the **default.policy** and **advanced.policy** files before loading this file.
- **Role_Assignment_Rules.policy** file: Defines a set of role assignment rules that allocate system-defined roles to devices and interfaces.

Additional policy files include:

- **SharedPolicyData.policy** file: Loaded automatically at system startup. It defines a set of commonly-used IP protocols which are available in any domain you create. You only need to load this file if the IP protocols are deleted or edited incorrectly.

Loading Policy Configuration Files

To load a policy configuration file:

1. On the **Domain** dialog box, select the **Setup** tab.
2. Click **Browse** to view the available configuration files in the **SamplePolicy** folder.
3. Select the file to load and click **Open**. A brief explanation of the file appears in the **File Information** panel.

4. Click **Load** to load the selected file and create the data. Note that these files must be loaded in the following order:
   a. **default.policy**
   b. **advanced.policy**
   c. **Rule_and_PHB.policy**

> **Note:**
>
> Do not load **Rule_and_PHB.policy** if you have already created standard PHB groups.

You must specify the device and interface roles to which these example standard PHB groups apply before using them. See "Using Roles in Policy Elements" for information on using roles in policy elements.

Class of Service Data

Classes of service define classes of traffic based on packet characteristics allowing traffic on the network to be identified. Specific QoS mechanisms, such as a guaranteed bandwidth or a particular queuing priority, can be applied to specific classes of traffic.

Traffic is allocated to a CoS according to how the CoS is defined. A CoS can be defined by various methods including packet marking, source/destination IP/MAC address, account or traffic type. Subsequent routers can apply differentiated QoS based on the class of service for traffic on a per-packet basis. For more information about Differentiated Service, see *IP Service Activator Concepts*.

The CoS data used by IP Service Activator is fundamental to establishing a policy-based QoS system. It consists of the following:

- Packet Markings: Define the bit settings which identify the traffic class to which IP or MPLS packets belong. You can use Packet Markings to determine which class a packet belongs to, or to change its class by re-marking it.

  The types of packet marking available are:

  – DiffServ codepoints: IP DiffServ codepoint bits in the DiffServ field of the IP packet header. Up to 64 DiffServ codepoints can be set up, each one corresponding to a different setting in the header of an IP packet
  – IP Precedence: IP Precedence bits in the IP Precedence field of the IP packet header. Up to eight IP Precedence values (0-7) can be defined, each one corresponding with a different setting in the header of an IP packet
  – MPLS experimental bits: CoS/experimental bits section of the MPLS header. Up to eight MPLS experimental bit values can be defined, each one corresponding to a CoS experimental bit value in the MPLS label
  – MPLS Topmost experimental bits: CoS/experimental bits section of the topmost MPLS header. Up to eight MPLS topmost experimental bit values can be defined, each one corresponding to a CoS experimental bit value in the topmost MPLS label
  – Frame Relay Discard Eligible (DE) bit: DE bit of the address field of the Frame Relay frame header. 0 or 1 in the Address field of the Frame Relay frame header

  - ATM Cell Loss Priority (CLP) bit: CLP bit in the ATM cell header. 0 or 1 in the ATM cell header
  - Discard-class: Defines an integer between 0 to 7, each one corresponding to a different setting indicating the type of traffic to be dropped when there is a congestion in the network.
  - Trust Type: specifies which CoS type is to be trusted. The options are: trust-cos, trust-ipprec, trust-dscp.
  - COS: Defines an integer between 0 to 7, used to set Layer 2 CoS for an outgoing packet.
  - COS Inner: Defines an integer between 0 to 7, used to mark inner CoS field in a bridged frame.
  - QoS Group: Defines an integer between 0 to 1023, each one corresponding to a system class. This marking is local to one device because it is not a field of the IP packet header.

> **Note:**
>
> Packet markings that specify settings for the Frame Relay Discard Eligible bit and/or ATM Cell Loss Priority bit can only be used by classes of service associated with PHB groups.

- Classes of Service: Define classification categories for identifying traffic on the network. Classes of service can be defined by packet marking (coarse grained), or by more detailed classifications such as source and/or destination IP address and traffic type (fine grained).

You can load the following policy configuration files which provide standard IP DiffServ codepoint values for IP Precedence codepoints and values for MPLS experimental bits:

- The **default.policy** file: described in "The default.policy File Summary"
- The **advanced.policy** file: described in "The advanced.policy File Summary"

The packet markings defined by these files are described in the following sections.

You can make changes to the packet markings created by these files:

- You can rename existing codepoints, though we recommend that you do not change standard names.
- You can create new codepoints, though you should ensure that they can be recognized by devices.

DiffServ Codepoints

Each DiffServ codepoint corresponds to a setting in the IP Precedence/DiffServ codepoint section of the header of an IPv4 or IPv6 packet. The DiffServ standard defines a 6-bit field, allowing up to 64 codepoints. As a result, up to 64 classes of service may be defined.

Packets can be re-marked at any point in the network using classification rules or using MQC PHB groups. See "Classification Rules" for information about defining

classification rules. See "Defining MQC PHB Groups " for more information about defining MQC PHB groups.

> **Note:**
>
> Before setting up a QoS policy, you need to know which codepoints are supported on the devices in your network – for example, whether they can recognize and mark with the full range of DiffServ codepoints or just the IP Precedence bits. To check the codepoints supported on a particular interface, see the appropriate Capabilities property page. For more information on viewing an interface's capabilities see *IP Service Activator User's Guide*.

The codepoints that are defined in IP Service Activator are listed in the **Packet Markings** folder on the **Policy** tab. IP Service Activator includes a set of policy configuration files that you can load into IP Service Activator to set up basic standard codepoints; see "Importing QoS-related Policy Files" for more information. You can also define codepoints in the user interface.

IP Precedence

Each IP Precedence value corresponds to a setting in the IP Precedence section of the header of an IPv4 or IPv6 packet. There are eight classes of services in IP Precedence. The classification range is 0-7 where 0 (zero) is the lowest and 7 is the highest priority.

MPLS Experimental Bits

For MPLS traffic, a label is attached to each IP packet at the ingress router to the Label Switched Path (LSP). This label is used by routers when forwarding packets along the path, and the IP packet header is not examined at any point along the LSP. The three IP Precedence bits are copied from the IP header into the three bits within the MPLS label known as the MPLS experimental bits or CoS experimental bits.

The application that generates the IPv4 or IPv6 packet controls the original IP Precedence value. However, some devices are able to reset this value, which can be useful if a precedence is set for a packet at the edge of the network and a service provider wants to override this value while the packet transits the core.

IP Service Activator is able to set the MPLS experimental bits where this is supported by devices.

Packets can be remarked at any point in the network using classification rules or MQC PHB groups. See "Classification Rules" for information on defining classification rules. See "Defining MQC PHB Groups " for more information on defining MQC PHB groups.

MPLS Topmost Experimental Bits

These are the same bits as the MPLS experimental bits, but set only on the topmost MPLS label on a packet. MPLS labels are added to IP packets on entry to an MPLS network. Typically, the three IP Precedence bits are copied from the IP header into these bits. Some devices are able to reset this value, which can enable the service provider to override a packet's precedence while it transits the core. Some devices also support setting and evaluating the MPLS experimental bits only on the Topmost MPLS label.

Packets can be remarked at any point in the network using classification rules or MQC PHB groups. The MPLS Topmost packet marking is used to mark the MPLS Experimental bits in only the topmost MPLS label of a packet. This Packet Marking is applicable only in MQC PHBs and only to perform policing and marking actions. Other actions will trigger the device to return errors which are then displayed in the **Faults** pane.

See "Classification Rules" for information about defining classification rules. See "Defining MQC PHB Groups " for more information about defining MQC PHB groups.

Frame Relay Discard Eligible Bit

The Frame Relay DE bit is part of the Frame address field in the Frame Relay frame header. This bit is normally set to indicate that the frame has a lower importance than other frames. When congestion occurs, frames with the DE bit set will be dropped before frames whose DE bits are not set.

ATM Cell Loss Priority Bit

The ATM CLP bit is part of the ATM Cell header. This bit is normally set to indicate that the cell has a lower importance than other cells. When congestion occurs, cells with the CLP bit set will be dropped before frames whose CLP bits are not set.

Discard-class

You can use this command to specify the type of traffic that will be dropped when there is congestion.

Trust Type

This configures the trust state, which selects the value that QoS uses as the source of the internal DSCP value. For example, if Trust type is set to trust-ipprec, the ToS bits in the incoming packets contain an IP precedence value and derives the internal DSCP value from the IP precedence bits.

The advanced.policy File Details

The advanced.policy file defines the IETF standard DiffServ Class Selector, Best Effort, Assured Forwarding and Expedited Forwarding codepoints. If you want to use the codepoints defined in this file, you need to load it into IP Service Activator. See "Importing QoS-related Policy Files" for more information.

The **advanced.policy** codepoints are defined in Table 2-2.

Table 2-2 Advanced.Policy Codepoints

Codepoint Name	DiffServ Codepoint
BE	0
CS0	0
CS1	8
CS2	16

Table 2-2 (Cont.) Advanced.Policy Codepoints

Codepoint Name	DiffServ Codepoint
CS3	24
CS4	32
CS5	40
CS6	48
CS7	56
AF11	10
AF12	12
AF13	14
AF21	18
AF22	20
AF23	22
AF31	26
AF32	28
AF33	30
AF41	34
AF42	36
AF43	38
EF	46

The COS values defined by the **advanced.policy** file are shown in Table 2-3.

Table 2-3 Advanced.Policy COS Values

Name	COS Value
COS 0	0
COS 1	1
COS 2	2
COS 3	3
COS 4	4
COS 5	5
COS 6	6
COS 7	7

The COS Inner values defined by the **advanced.policy** file are shown in Table 2-4.

Table 2-4 Advanced.Policy COS Inner Values

Name	COS Inner Value
COS Inner 0	0

Table 2-4 (Cont.) Advanced.Policy COS Inner Values

Name	COS Inner Value
COS Inner 1	1
COS Inner 2	2
COS Inner 3	3
COS Inner 4	4
COS Inner 5	5
COS Inner 6	6
COS Inner 7	7

The MPLS experimental bits defined by the **advanced.policy** file are shown in Table 2-5.

Table 2-5 Advanced.Policy MPLS Experimental Bit Values

Name	MPLS Experimental Bit Value
MPLS Exp 0	0
MPLS Exp 1	1
MPLS Exp 2	2
MPLS Exp 3	3
MPLS Exp 4	4
MPLS Exp 5	5
MPLS Exp 6	6
MPLS Exp 7	7

For details about the objects that are created by a policy file, see the file itself. The **advanced.policy** file is located in the **Sample Policy** folder in your IP Service Activator installation, found in:

ServiceActivatorHome\Oracle Communications\Service Activator\SamplePolicy

Creating a New Packet Marking

You create packet markings on the **Policy** tab.

To create a new packet marking:

1. On the **Policy** tab, select the **Packet Markings** folder.
2. Select **Add Packet Marking** from the pop-up menu.

   The **Packet Marking** dialog box opens.
3. Enter the following details:
   - **Name**: an identifying name for the marking object
   - **Marking**: do one of the following:

- Select **DiffServ Codepoint** and define the appropriate codepoint value in the range 0-63.
- Select **IP Precedence** and define the appropriate value in the range 0-7.
- Select **MPLS - Experimental** and define the appropriate bit value in the range 0-7.
- Select **MPLS - Topmost** and define the appropriate bit value in the range 0-7.
- Select **Frame Relay Discard Eligible** and specify either **Enabled** or **Disabled**.
- Select **ATM Cell Loss Priority** and specify either **Enabled** or **Disabled**.
- Select **Discard class** and define the appropriate value in the range 0-7.
- Select **Trust Types** and choose a value from the options **trust-cos**, **trust-ipprec**, and **trust-dscp**.
- Select **COS** and select a value in the range of 0-7.
- Select **COS Inner** and select a value in the range of 0-7.
- Select **QoS Group** and select a value in the range of 0-1023.

4. Click **OK** to close the dialog box.

> **Note:**
>
> If you have loaded the **default.policy** file and/or **advanced.policy** file, packet markings for some DiffServ codepoints and MPLS experimental bit values will already exist.

Flexible IP Precedence and DSCP Support

DSCP and IP Precedence packet marking are equally supported within the object model. This allows configuration for IP Precedence and DSCP to co-exist on a single device.

Defining Packet Markings in Cisco IOS Cartridge Configuration Options

The following options can be configured before and after deployment to define which packet marking type is used for the particular command:

- cartridge.cisco.qos.policymap.setTosType
- cartridge.cisco.qos.policymap.wredType
- cartridge.cisco.qos.phbwfq.dropStrategy.wredType
- cartridge.cisco.qos.interface.wredType
- cartridge.cisco.qos.car.setTosType
- cartridge.cisco.qos.acl.numbered.tosType
- cartridge.cisco.qos.acl.named.tosType
- cartridge.cisco.qos.policymap.police.tosType
- cartridge.cisco.qos.classmap.tosType

See *IP Service Activator Cisco IOS Cartridge Guide* for more information on the possible values that can be set to determine the packet marking type.

Classes of Service

A CoS is a logical grouping of traffic based on marking and classification rules for the purpose of providing differentiated QoS.

There are two policy configuration files you can load that pre-define classes of service:

- The **default.policy** file, see "The default.policy File Summary"
- The **advanced.policy** file, see "The advanced.policy File Summary"

See "Importing QoS-related Policy Files" for information about loading policy configuration files.

You associate classes of service with standard PHB groups and MQC PHB groups:

- When associated with a standard PHB group, a CoS specifies the queuing mechanism, rate-limiting, and traffic shaping (ATM and FR) to be applied to a traffic class.
- When associated with an MQC PHB group, a CoS allows a complete QoS policy to be applied to a traffic class including mechanisms for queuing, shaping, policing and re-marking.

A PHB group may have one or more classes of service associated with it. You can apply PHB groups to the network or specific devices and in this way specify how traffic in each CoS is treated.

A CoS can be defined in terms of the following:

- One or more packet markings (coarse-grained)
- A classification or classification group – classifications may be defined, for example, by source and/or destination IP address or account and traffic type (fine-grained)

> **Note:**
>
> A standard PHB group applies to a CoS characterized by a packet marking, while an MQC PHB group applies to a CoS defined by a classification or classification group. Each PHB group type ignores any **irrelevant** part of a CoS definition.

Although it is possible to associate several markings with a CoS, they are normally matched on a one-to-one basis.

The classes of service that are defined in IP Service Activator are listed in the **Policy** tab's **Classes of Service** folder. IP Service Activator is shipped with a set of policy configuration files that you can load to set up basic standard classes. You can also define new classes of service in the user interface.

In addition, a Default Class of Service is created automatically. A default CoS refers to the CoS used when no other user-defined CoS is selected for a MQC, MQC PHB or policing rule. You can use the Default Class of Service when setting up PHB groups to

define a default behavior for unmarked traffic. However, the default CoS can't be linked to either a codepoint or a classification object. The default behavior of this CoS is vendor specific.

You can edit the classes of service created by the configuration files if you wish. For example, you can:

- Rename existing classes of service to something appropriate to your organization
- Delete classes of service that you do not intend to use

  You cannot delete the Default Class of Service, and you cannot delete a CoS that is used by a PHB group.
- Create a new CoS

To create a new class of service:

1. On the **Policy** tab, select the **Classes of Service** folder.
2. Select **Add Class of Service** from the pop-up menu.

   The **Class of Service** dialog box opens.
3. Specify an identifying name and a configured name for the CoS and click **OK**.

To associate a specific packet marking with a CoS:

1. Organize the display so that the relevant packet marking and CoS are both visible.

   Packet markings and classes of service are listed on the **Policy** tab.
2. Drag the marking object on to the CoS.

   IP Service Activator lists the associated packet marking on the CoS's **Packet Marking** property page.

or:

1. On the **Policy** tab, select the relevant CoS and select **Properties** from the pop-up menu.

   The CoS dialog box opens.
2. Select the **Packet Marking** property page and select the check box associated with the relevant packet marking.

   You can select a number of packet markings to associate with a CoS.

To associate a classification or classification group with a CoS:

1. Organize the display so that the relevant classification or classification group and CoS are both visible.

   Classifications and classes of service are listed on the **Policy** tab.
2. Drag the classification or classification group object on to the CoS.

   IP Service Activator displays the associated classification or classification group on the CoS's **Classification** property page.

or:

1. On the **Policy** tab, select the relevant CoS and select **Properties** from the pop-up menu.

   The CoS dialog box opens.
2. Select the **Classification** property page, select a classification or classification group and click **Apply**.

You can only associate a single classification or classification group with a CoS.

> **Note:**
>
> A fine-grained CoS can only be associated with MQC PHB groups.

To view a CoS's packet markings and classifications or classification groups:

1. On the Policy tab, double-click on the **Classes of Service** folder.

   IP Service Activator lists details of the packet markings and classifications or classification groups associated with each CoS in the details pane.

Policy Components

Policy components are the standard definitions and templates that can be used when setting up policy rules and MQC PHB groups. These include:

- Traffic types: Define the network traffic that can be affected by rules and MQC PHB groups. If you have loaded the default configuration files, a number of traffic types are already included in IP Service Activator, defining traffic according to port number and CoS (Gold, Silver and Bronze). If you wish, you can define further traffic types that identify specific network traffic that you want to manage.
- Classifications and classification groups: Define network traffic by source and/or destination IP address or account and traffic type. If you have loaded the default configuration files, a number of classification groups are already included in IP Service Activator, defining traffic according to traffic type and source and destination IP address. If you wish, you can define further classifications and classification groups. Classifications and classification groups can be used with policy rules and with the classes of service associated with MQC PHB groups.
- Date and time templates: Specify the time periods during which rules are active, if they are only to apply at certain times. The use of date and time templates is optional. It is also possible to specify the effective dates and times manually when you set up the policy rule.
- IP protocols: Define the transport protocols that can be used when defining a traffic type by port and IP protocol.

Setting Up Traffic Types

You need to set up traffic types to identify the different categories of network traffic to which you want to apply a specific QoS or security policy using policy rules or MQC PHB groups.

You can set up traffic types based on a number of different methods of classifying traffic:

- Port Traffic Type – Source or destination port number and/or IP protocol. This is the most common way of classifying traffic because it is supported on all devices.
- Packet Marking – DiffServ codepoint, IP Precedence, MPLS experimental bits, Frame Relay DE bit, ATM CLP bit, Discard-class, COS, COS Inner, or QoS Group.

Traffic types that use packet markings specifying settings for the Frame Relay Discard Eligible bit and/or ATM Cell Loss Priority bit can only be used by classifications associated with classes of service associated with PHB groups.

- Domain Name – DNS domain name
- Application – Name of application protocol within the application, for example http
- Sub-application – Name of sub-application, for example H.323 video
- URL – One URL or multiple URLs can be matched with the use of a wildcard (*)

  For example, URL `http://www.website.com/dir` only matches files in the directory dir on `www.website.com`, whereas `http://www.website.com/*` would match all URLs under that website.
- MIME – The MIME type returned by HTTP and, if supported, the minimum and maximum packet length
- Input-Interface - Name of interface
- VLAN - VLAN identification number or ranges of identification numbers between 1 and 4095

The actual support for particular traffic classification methods is interface-specific. You should always check the capabilities of an interface before employing a traffic classification.

To view the classification capabilities of a specific interface, display its property pages. The **Capabilities** property page lists the device capabilities: select **Classify** under **Access**, **Classification** or **Policing** for details of the traffic types supported. For more information on viewing interface capabilities, see *IP Service Activator User's Guide*.

A number of default traffic types are set up when you load the **default.policy** configuration file. You can view these traffic types in the **Policy** tab's **Traffic Types** folder. This folder contains two subfolders:

- The **Standard Traffic Types** folder includes traffic types that allow you to identify traffic by standard DiffServ codepoints – IP precedence values 0, 3 and 5 corresponding to the Bronze, Silver and Gold classes of service.
- The **Standard Port Numbers** folder includes a number of traffic types identifying the most common TCP and UDP port numbers.

The default class of service (if selected) will match any type of traffic that is not already matched within the current context. This enables you to apply rules to all traffic that is not defined by another group.

Additional traffic types may be created by loading the **advanced.policy** configuration file. These traffic types are held in subfolders in the **Policy** tab's **Traffic Types** folder:

- The **DSCP Values** folder includes traffic types that allow you to identify traffic by DiffServ codepoint values
- The **IP Precedence** folder includes traffic types that allow you to identify traffic by **IP Precedence** values
- The **IP Protocols** folder includes traffic types that allow you to identify traffic by IP protocol
- The **MPLS EXP Values** folder includes traffic types that allow you to identify traffic by MPLS experimental bit value

You can edit the available traffic types in the following ways:

- Set up additional traffic types to identify specific network traffic.
- Set up a compound traffic type when you need to identify traffic which combines two or more traffic types, for example, packets that are both from a particular port (defined by a port traffic type) and a specific URL (defined by URL traffic type).

You can also set up a traffic type group when you want to organize traffic types into a logical or hierarchical structure.

To set up a port-based traffic type:

1. On the **Policy** tab, select the **Traffic Types** folder.

   Alternatively, to add a traffic type to an existing group, expand the **Traffic Types** folder and select the appropriate folder.
2. Select **Add Port Traffic** from the pop-up menu. The Port Traffic dialog box is displayed.
3. On the Traffic Type property page, specify the **Name** and **Remarks**.
4. On the Port Traffic property page, specify source and destination ports.

   To specify a source port, select the Enable check box in the Source pane.

   To specify a single source port, select the Single button, and then enter the number of the source port.

   To specify a range of source ports, select the Range button and enter the start and end of the range of port numbers.
5. On the Protocol Options property page, specify the TCP flags and select an ICMP option from **Messages** menu.
6. Click **OK** to close the dialog box.

For complete dialog box and property page descriptions, see IP Service Activator online Help.

To set up other traffic types:

1. On the **Policy** tab, select the **Traffic Types** folder.

   Alternatively, to add a traffic type to an existing group, expand the **Traffic Types** folder and select the appropriate folder.
2. Select the appropriate **Add... Traffic** command from the pop-up menu. Choices include:
   - Add Port Traffic
   - Add Packet Marking Traffic
   - Add Domain Name Traffic
   - Add Application Traffic
   - Add Sub-application Traffic
   - Add MIME Traffic
   - Add URL Traffic
   - Add VLAN Traffic
   - Add Input-Interface
   - Add Traffic Group

- Add Compound Traffic

For example, select **Add Packet Marking Traffic** to set up a new packet marking-based traffic type.

3. On the Traffic Type property page for the traffic type dialog box which displays, specify **Name** and **Remarks**.
4. Select the *TrafficType* Traffic property page to define further details for the traffic type. The information required depends on the traffic type being defined, as shown in Table 2-6.

> **Note:**
>
> For complete dialog box and property page descriptions, see IP Service Activator online Help.

Table 2-6 Defining Traffic Types

To Define...	Do this...
A packet marking-based traffic type	On the Packet Marking Traffic property page of the Packet Marking Traffic dialog box select the check box of a packet marking type you require and specify a value.
A domain name-based traffic type	On the Domain Name Traffic property page of the Domain Name Traffic dialog box, in the **Domain Name** field, specify the DNS domain name.
An application-based traffic type	On the Application Traffic property page of the Application Traffic dialog box, in the **Name** field, specify the application protocol name, such as realaudio for the Real Audio Streaming Protocol.
A sub-application-based traffic type	On the Sub-application Traffic property page of the Sub-application Traffic dialog box, in the **Name** field, specify the sub-application protocol name.
A URL-based traffic type	On the URL Traffic property page of the URL Traffic dialog box, in the **URL** field, enter a text string to represent a URL.
A MIME-based traffic type	On the MIME Traffic property page of the MIME Traffic dialog box, in the **MIME type** field, enter the MIME type, such as audio.
An Input-Interface traffic type	On the Input-Interface Traffic property page of the Input Interface Traffic dialog box, in the **Interface Name** field, enter the interface name.
A VLAN traffic type	On the VLAN Traffic property page of the VLAN Traffic dialog box, enter a VLAN identification number in the **VLAN Range start and end** fields. If the VLAN end range field is empty, a single VLAN is assumed.

5. Click **OK** to close the dialog box.

Setting Up a Compound Traffic Type

You can set up a compound traffic type when you need to identify traffic that combines two or more traffic types, for example, packets that are both from a particular port (defined by a port traffic type) and a specific URL (defined by a URL traffic type).

To set up a compound traffic type, create the traffic type and then define the types to be included.

To set up a compound traffic type:

1. On the **Policy** tab, select the **Traffic Types** folder.
2. Right-click and select **Add Compound Traffic** from the pop-up menu.
3. On the Traffic Type property page of the Compound Traffic Type dialog box, specify **Name** and **Remarks**.

To define the traffic types included in the compound traffic type, either:

1. Create members of the group directly, by right-clicking the compound traffic type and choosing the appropriate **Add** command from the pop-up menu.

or:

1. If the traffic type already exists, include it in the compound traffic type by dragging and dropping.

For complete dialog box and property page descriptions, see IP Service Activator online Help.

Setting Up a Traffic Type Group

Set up a traffic type group if you want to organize traffic types into a logical or hierarchical structure.

Traffic type groups are for administrative purposes only. You cannot apply policy to them.

To set up a traffic type group:

1. On the **Policy** tab, select the **Traffic Types** folder.

   Alternatively, to add a traffic type group to an existing group, expand the **Traffic Types** folder and right-click the appropriate folder.
2. Select **Add Traffic Group** from the pop-up menu.
3. On the Traffic Type property page, enter details including **Name** and **Remarks**.
4. Click **OK** to close the dialog box.

To define the members of the group, either:

1. Create members of the group directly, by right-clicking the group and selecting the appropriate **Add** command from the pop-up menu.

or:

1. If the traffic type already exists, include it in the group by dragging and dropping.

For complete dialog box and property page descriptions, see IP Service Activator online Help.

Setting Up a Classification

A classification is a method of categorizing traffic according to its source and/or destination and traffic type. This means, for example, that all traffic from New York can be assigned the same classification or subdivided by traffic type.

Classifications can also be collected into classification groups to create more complex criteria for classifying traffic. Classification groups enable you to group a number of traffic classifications – such as a set of routing protocols or application traffic – and apply the same class of service to them.

Classifications and classification groups can be:

- Linked to a policy rule

  The classification/classification group defines which traffic is acted on by the rule. Alternatively, you can create a one-off classification within the rule definition.

- Linked to a CoS

  A CoS that is linked to a classification/classification group can be associated with an MQC PHB group. The classification/classification group defines to which traffic the MQC PHB group's policy mechanisms apply.

It is possible to create a set of classifications and classification groups by loading the **advanced.policy** file. The file creates the following classification groups, held in the **Classifications** folder on the **Policy** tab:

- The DSCP Values classification group holds a set of classifications based on DiffServ codepoint packet marking traffic types
- The IP Precedence classification group holds a set of classifications based on IP Precedence packet marking traffic types
- The MPLS EXP Values classification group holds a set of classifications based on MPLS experimental bit packet marking traffic types

See "Importing QoS-related Policy Files" for information about loading policy configuration files into IP Service Activator.

Using Classifications with Policy Rules

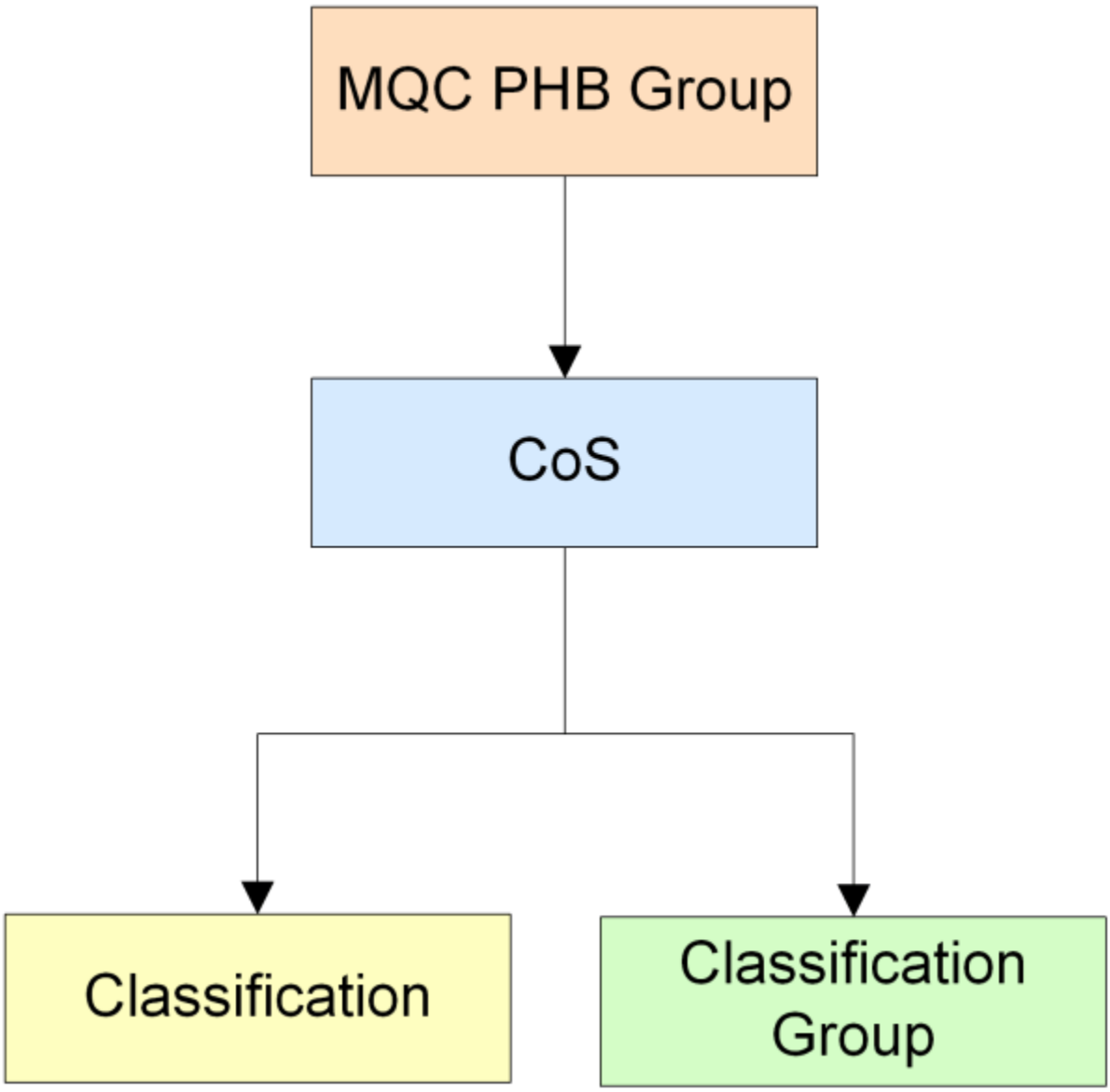
When deciding which classifications to create, we suggest you evaluate which source and destination and traffic type combinations need to have the same policy applied to them. Create a classification for each combination and, if necessary, group those classifications. You can then associate the group with the relevant rules.

See "Defining QoS and Access Control " for information about associating a classification with a rule. See "Using Classifications in Rules" for an example use of classifications and classification groups.

Using Classifications with MQC PHB Groups

A classification/classification group may be linked to a CoS which, in turn, may be linked to an MQC PHB group. The treatment to be applied to traffic that belongs to the CoS is defined by the MQC PHB group. See Figure 2-1 for more details.

Figure 2-1 MQC Classifications



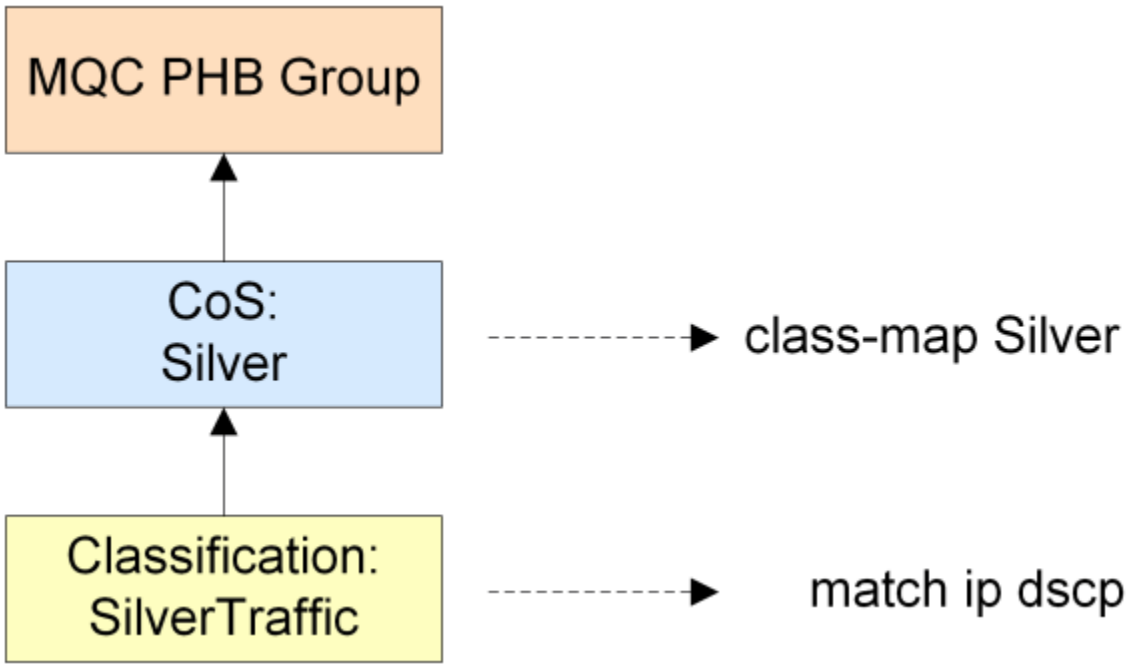
In order to explain the options IP Service Activator offers for classifications/ classification groups, it is necessary to see the configuration that is installed on the device. This includes at least one class map, generated for the CoS.

A class map defines a traffic class. There are three main elements in a traffic class:

- A name – taken from the CoS
- One or more match statements, generated for the classification or classification group linked to the CoS; a match statement specifies a criterion for classifying packets.
- An instruction on how to evaluate the match statements – match any or match all of the match statements (described in "Match Any or Match All").

For example, where a classification based on a packet marking traffic type is associated with a CoS, a class map is configured containing a single match statement for that packet marking. See Figure 2-2.

Figure 2-2 Class Map Example



Only one classification or classification group may be associated with a CoS.

Match Any or Match All

The class map generated for a CoS may contain a number of match statements.

If a CoS is linked to a classification group, you can specify how packets are evaluated against the match criteria – whether packets must **match all** of the match statements or **match any**.

A classification provides the lowest level of classification and the match criteria for a classification is therefore always **match all**. You cannot change this setting.

Named or Numbered Access Control Lists

Classifications based on source/destination IP address or port, and protocol result in one or more Access Control Lists (ACLs) being configured on the device. These ACLs are referenced by a match statement in the class map.

By default, IP Service Activator generates ACL identifiers automatically. However, you can override this and specify a name or number for an ACL.

By using aggregation – described in "Aggregation" – you can also control the number of ACLs that are configured.

To generate both named and numbered ACLs in the same structure:

1. Create a classification group.

2. Within that parent group, create one named classification group and one numbered classification group.
3. Create the required classifications for each individual group.

Nested Class Maps

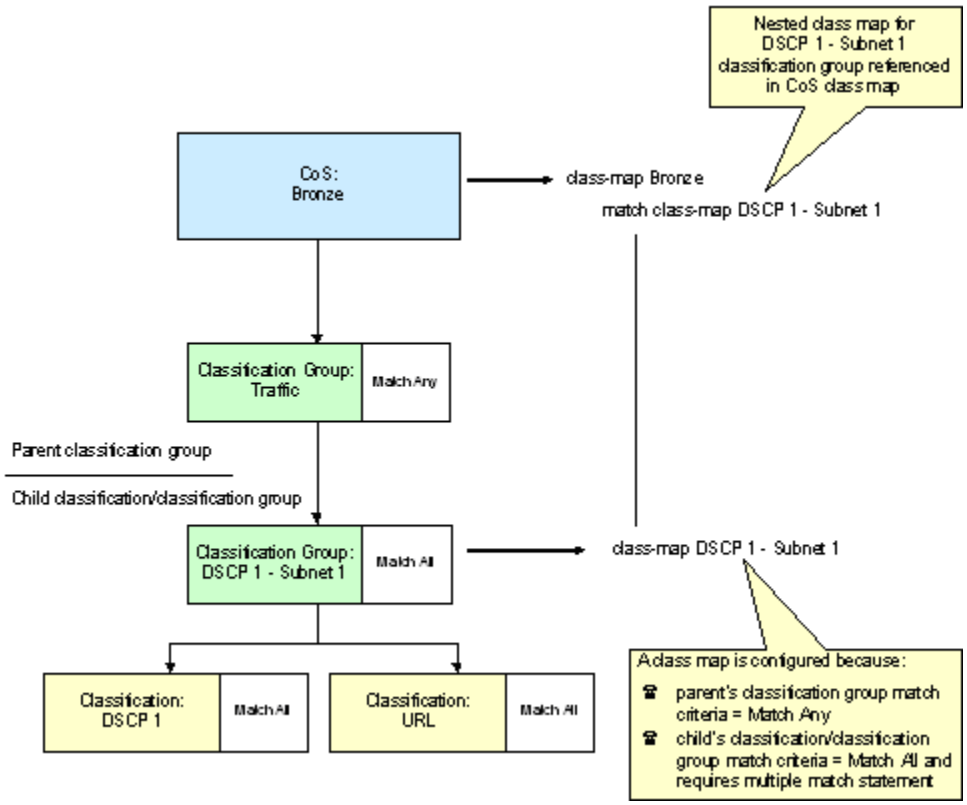
IP Service Activator always configures a class map for the CoS. A **nested** class map may also be configured for a classification/classification group if both of the following apply:

- The parent classification group's match criteria is **match any**.
- The child classification/classification group match criteria is **match all** and the classification/classification group can only be expressed with multiple match statements.

  The number of match statements generated depends on whether match statements for the classification or group may be aggregated with other match statements at the same level. See "Aggregation" for more information.

A class map generated for a classification/classification group is nested by a reference in a match statement in the CoS's class map. This is illustrated in Figure 2-3.

Figure 2-3 Nested Class Map



Aggregation

IP Service Activator supports aggregation of commands into class maps, access groups, and ACLs. In aggregation, internal rules determine how commands are

merged and promoted when the configuration statements are pushed to the device. You can specify whether match statements of the same type are aggregated into a single match statement within the parent class map.

A classification/classification group linked to a CoS may result in a number of match statements of the same type. For example, a classification group that groups classifications based on the packet marking traffic type (DiffServ codepoint).

IP Service Activator uses the following rules when applying aggregation:

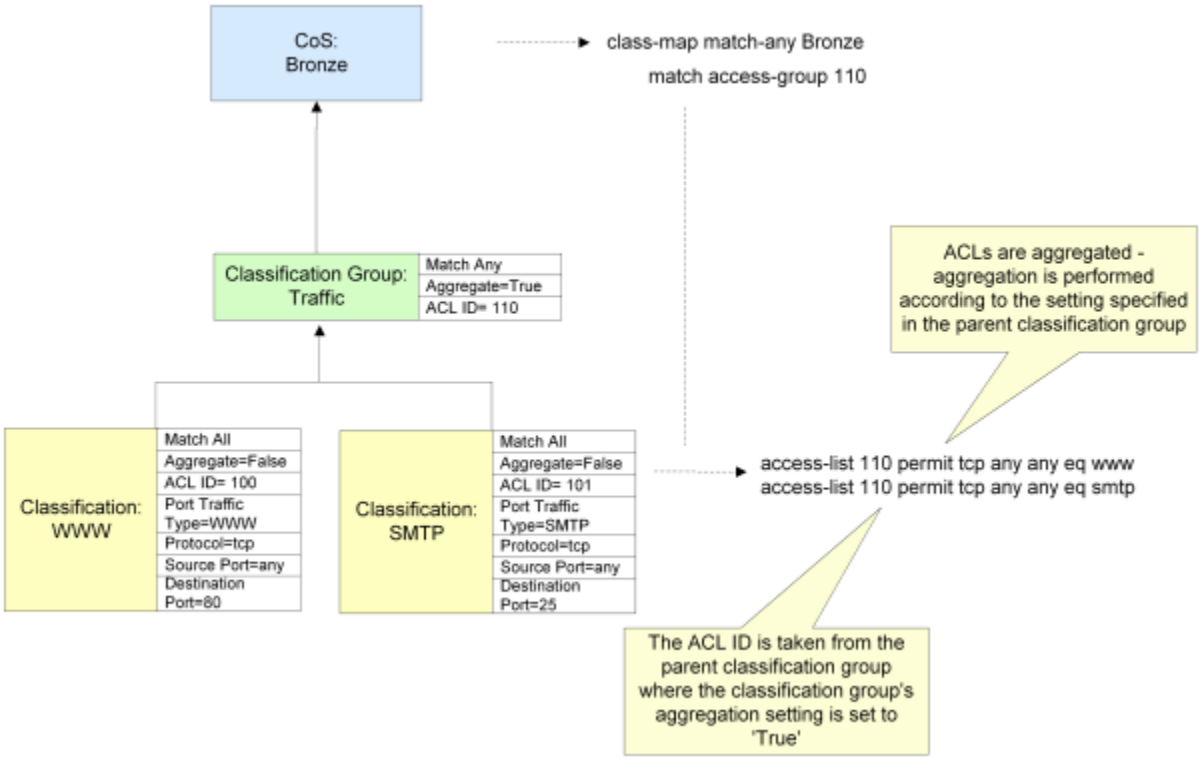
- If a classification/classification group is a child of a classification group, the aggregation setting of the parent classification group determines whether aggregation is applied to the match statements generated for the child.
- If a child classification/classification group requires an ACL and its match statements are set to aggregate by a parent classification group, the ACL identifier is taken from the parent classification group.
- A classification group set to **match any** may aggregate the match statements generated for a child classification group if:
  - The nested classification group is also set to **match any**.

  or:

  - The child classification group is set to **match all** but the classification can be expressed with a single match statement and any associated ACL has a single entry.
- A classification group set to **match all** cannot aggregate the match statements generated for a child classification/classification group.

Figure 2-4 illustrates some of these rules.

Figure 2-4 Aggregation



In this example, the aggregation setting for the parent classification group **Traffic** is set to True. Where match statements of the same type are generated for its child classifications, they are aggregated into a single match statement. Note that the aggregation setting of the parent classification group overrides those of the child classifications.

Both child classifications result in ACLs as they are based on destination port. However, because they are to be aggregated into a single match statement, only one ACL is generated incorporating the filtering criteria for both classifications. Where an ACL is created for a classification that is aggregated at the parent classification group, the ACL identifier is taken from the parent classification group.

Note that aggregation also indirectly controls:

- The number of ACLs created for relevant classifications

  For instance, by changing the aggregation setting to False for the **Traffic** classification group in the above example, two ACL lists will be generated – one for the **WWW** classification and one for the **SMTP** classification
- Whether nested class maps are generated

  If a classification group is a child of another classification group but its match statements are aggregated into a single match statement, no class map needs to be generated for the nested classification group

For complete dialog box and property page descriptions, see IP Service Activator online Help.

To set up a classification:

1. On the **Policy** tab, select the **Classifications** folder.

   Alternatively, to add a classification to an existing group, click on the classification group.
2. Right-click and select **Add Classification** from the pop-up menu.

   The Classification dialog box opens.
3. On the Details property page, specify **Name** and **Remarks**.

   Select Address type (IPv4, IPv6, MAC) from the drop down list.

   Select the Classification Match type (Include or Exclude).

   Select the Classification Option (Log, Fragments).
4. On the IP Source/Destination property page specify the source and destination values to be included in the classification.
5. On the MAC Source/Destination property page specify the source and destination values to be included in the classification.
6. On the Traffic Type property page, select the traffic type to be classified.
7. If the classification will be used with an MQC PHB group, select the MQC property page and set the value of the **Aggregate match statements** check box. Specify a choice for the **Acl Id**. Choose from **Auto Generate**, **Numbered**, or **Named**. If you choose **Numbered** or **Named**, provide the number or name to use.
8. Click **OK** to close the dialog box.

To set up a classification group:

1. On the **Policy** tab, right-click the **Classifications** folder.

2. Select **Add Classification Group** from the menu.

   The Classification Group dialog box appears.

3. On the Details property page, specify **Name** and **Remarks**.
4. If the classification group will be used with an MQC PHB group, select the MQC property page and specify some or all of **Match Any**, **Match All**, **Aggregate match statements**, **Auto Generate**, **Numbered**, and **Name**.
5. Click **OK**.
6. Add classifications to the group by doing one of the following:
   - Dragging and dropping existing classifications on to the group
   - Creating new classifications within the group by right-clicking and selecting **Add Classification** from the group's pop-up menu

> **Note:**
>
> A classification group cannot be associated with more than eight DiffServ codepoint values, defined in classifications linked to the classification group. If a classification group based on more than eight codepoints is required, subclassification groups must be created and linked to a parent classification group.

Strict Aggregation

Strict aggregation takes place through classification groups and classifications to generate a hierarchy of class maps and access groups on the device, each containing one or more individual entries. Strict aggregation helps you elaborate complex hierarchies of objects and define process flows. Different actions are applied to different traffic flows. The classification hierarchies are composed of classifications and classification groups.

Strict aggregation makes provisioning predictable and simpler. When you select **Enable strict classification aggregation**, the resulting changes to the aggregated configuration statements are more predictable. This means that you can do away with one layer of class map in the hierarchy.

Promotion

Promotion is a way to control entries generated under their current level as in their parent classification group. The entry is later translated to a class map or to an access group, if the entries are promoted at the higher level. Promotion is controlled by selecting or deselecting the **Aggregate match statements** on the MQC property page of Classification and Classification Group objects in IP Service Activator.

For a classification, selecting **Aggregate match statements** generates a class-map entry when applicable. Deselecting **Aggregate match statements** generates an ACL entry when applicable.

Merging

Merging involves grouping more than one entry into a single entity, for example, grouping multiple “match ip dscp" statements into one “match ip dscp" list. Merging is always applied on adjacent classification entries when applicable. Merging will occur when **Match Any** is

selected for a Classification group. It cannot occur when **Match All** is selected. Merging happens to entries when the command type is the same, and with adjacent entries only.

To enable strict classification aggregation:

1. On the network map or from the **Topology** tab for the specific domain, right-click a device and select **Properties**.

   The Device dialog box appears.
2. Click on the Management property page.
3. In the QoS section, select the **Enable strict classification aggregation** check box.
4. Click **OK**.
5. Commit the transaction.

   The strict classification aggregation feature for the selected device is enabled.

Setting Up a Date and Time Template

A date and time template consists of a defined time period, which can apply on specified days between any two dates. For example, you could set up a template that applies from 9:00 a.m. to 5:00 p.m. every Monday to Friday or one that applies between 3:00 p.m. and 5:30 p.m. on Tuesdays only. You can associate date and time templates with policy rules to specify that the rules are only active during certain periods.

For complete dialog box and property page descriptions, see IP Service Activator online Help.

To set up a date and time template:

1. On the **Policy** tab, select the **Date and Time Templates** folder.
2. Right-click and select **Add Date** and **Time Template** from the pop-up menu.

   The Date and Time Template dialog box opens.
3. Enter details for **Name**, **Active date range**, **Active part of day,** and **Active days**.
4. Click **OK** or **Apply**.

The defined time periods will repeat throughout the defined period of validity. For a template indicating a one-off time period, (such as 9:00 a.m. until 12:30 p.m. on 12th August) set the First and Last days to be the same. Times must be specified to the nearest five-minute boundary.

Dates and times are held in Coordinated Universal Time (UTC) throughout IP Service Activator. However, they are displayed in the local time for the workstation, adjusted for daylight savings where relevant. Remember that you may need to adjust times if rules are to apply to different time zones.

Setting Up IP Protocols

IP protocols are used when defining traffic types by port and IP protocol. A number of commonly-used IP protocols are included in IP Service Activator on installation.

You should not need to change these protocol definitions, but you can view them and, if necessary, set up additional protocols for classifying network traffic.

If the standard IP protocols are deleted by accident, you can restore them by reloading the **SharedPolicyData.policy** file. For complete dialog box and property page descriptions, see IP Service Activator online Help.

To view an IP protocol:

1. On the **Policy** tab, expand the **IP Protocols** folder.

   IP Service Activator lists the defined IP protocols.

2. To view a protocol's details, double-click the relevant protocol or right-click the protocol and select **Properties** from the pop-up menu.

   The IP Protocol dialog box opens.

To add an IP protocol:

1. On the **Policy** tab, right-click the **IP Protocols** folder and select **Add IP Protocol** from the pop-up menu.
2. Specify details including **Protocol name** and **Protocol number**.
3. Click **OK**.

Setting Up Accounts

Accounts can be used to define the users of QoS and security services and act as the source and destination points for rules.

You can define the source and destination points between which a rule applies within the rule itself, or using classifications. For information on defining classification rules see "Classification Rules", for defining access rules see "Access Rules", and for policing rules see "Policing Rules". See "Setting Up a Classification" for information on defining classifications.

An account is always identified by an IP address, but may represent an individual user, a specific host computer or a subnet. You can also set up account groups that include a number of accounts of any type. You can use these groups to apply policy to several accounts simultaneously or use them for organizational purposes only. You can also create default account groups based on the sites you have created.

For complete dialog box and property page descriptions, see IP Service Activator online Help.

Set up a user account when you need to manage network traffic to or from a specific person. To set up an account for an individual user:

1. On the **Accounts** tab, select the **Accounts** folder.

   Alternatively, to add a user to an existing account group, expand the **Accounts** folder and select the appropriate account group. See "Setting Up Accounts" for information on creating account groups.

2. Right-click and select **Add User Account** from the pop-up menu.

   The User Account dialog box opens.

3. On the User Account property page, enter details including **First Name**, **Last Name**, **User Id**, **Contact**, and **Location**.

4. On the IP Address property page, enter a value for **IP Address** - the IP address of the user's workstation.

> **Note:**
>
> The user is identified by the workstation IP address. You can enter additional information if you wish, but it is not used by IP Service Activator.

5. Click **OK** to close the dialog box.

You can set up a host account when you need to manage network traffic to or from a specific host computer. To set up an account for a host computer:

1. On the **Accounts** tab, select the **Accounts** folder.

   Alternatively, to add a host to an existing account group, expand the **Accounts** folder and select the appropriate account group. See "Setting Up Accounts" for information on creating account groups.

2. Right-click and select **Add Host Account** from the pop-up menu.
3. On the Details property page, enter details including **Name** and **Remarks**.
4. On the Host Account property page, enter the **IP address** - the IP address of the workstation. Alternatively, you can enter the DNS name and click the **DNS lookup** button to look up the IP address.
5. Click **OK** to close the dialog box.

Set up a subnet account when you need to manage network traffic to or from an entire subnet. To set up an account for a subnet:

1. On the **Accounts** tab, select the **Accounts** folder.

   Alternatively, to add a subnet account to an existing account group, expand the **Accounts** folder and select the appropriate account group. See "Setting Up Accounts" for information on creating account groups.

2. Right-click and select **Add Subnet Account** from the pop-up menu.
3. On the Details property page, enter details including **Name** and **Remarks**.
4. On the Subnet Account property page, enter details including **Subnet Address** and **Subnet Mask**.
5. Click **OK** to close the dialog box.

Set up an account group when you have a requirement to apply policy to a number of different individuals, host computers or subnets. You can also use account groups to create a hierarchical structure for organizational purposes or to represent the structure of a company.

Setting up an account group involves creating a named group and then defining its members. To set up an account group:

1. On the **Accounts** tab, select the **Accounts** folder.

   Alternatively, to add a group as a subset of an existing account group, expand the Accounts folder and select the appropriate account group.

2. Right-click and select **Add Group Account** from the pop-up menu.

3. On the Details property page, enter details including **Name** and **Remarks**.
4. Click **OK**.
5. To define the members of the group, either:
   - Create members of the group directly, by right-clicking the group and selecting **Add User Account**, **Add Host Account,** or **Add Subnet Account** from the pop-up menu.

   or:

   - If an account already exists, you can include it in the group by dragging and dropping.

You can automatically set up default account information for the sites you have created. Suitable account group, subnet accounts and host accounts will be created, which you can edit if required.

Note that you must have already set up all relevant sites and assigned the appropriate interfaces/devices to them. An account is created for a site if the site meets the following conditions:

- The site contains a device with the Access role assigned to it, or no role assigned
- The device has interfaces or sub-interfaces that have the role Local or Disabled assigned to them and they are not shut down
- The interfaces have subnets connected to them

To define account groups automatically for defined sites:

1. From the **Tools** menu, select **Create Site Accounts**.

IP Service Activator examines all sites that are set up. For any access router associated with a site account, it examines the segments and hosts and attempts to create a set of meaningful accounts:

- For each site, an account group is created. The group is given the same name as the site.
- For each segment that has host systems defined, an account group is created. The group is given the name Segment IP address hosts. Within this group, a host account is created for each host system on the segment. The name of the host is used as the name of the account.
- For a segment that does not have host systems defined, a subnet account is created. The IP address of the segment is used as the name of the account.

The new sites are listed on the **Accounts** tab beneath the **Accounts** folder.

3
Defining QoS and Access Control

This chapter describes the rule types that feature in Oracle Communications IP Service Activator. The chapter:

- Provides an overview of each rule type and its function.
- Describes where rules can be applied.
- Gives detailed information for creating classification, policing and access rules.
- Describes how to implement rules.
- Explains how to check the status of implemented rules.
- Describes how to manage and disable rules.

Introduction

Rules are one of the building blocks you use to create a QoS or security policy. You can use rules to:

- Mark traffic and optionally manage bandwidth – classification rules
- Police the bandwidth used by a particular traffic type or classification and specify the treatment for traffic that conforms to or exceeds the bandwidth requirements – policing rules
- Implement security by permitting or denying network traffic – access rules

You can apply rules to any policy target – that is, any network component, a customer, site or VPN – and you can apply any type of rule at any point in the network. For example, you can apply a classification rule to a device at the network edge or in the core. However, some general guidelines for deployment are:

- Use classification rules at the outbound interface of devices at the network edge – that is, CE (access) devices.
- Use policing rules at the outbound interface of devices at the network edge or inbound interfaces at the core edge – that is, CE (access) or PE (gateway) devices. Policing at CE devices is preferable as it reduces traffic at the earliest possible point. However, if the CE device is not managed by the service provider, this may not be possible.
- Use access rules at the network edge – that is, CE (access) devices. Access rules can also be used within the core network to protect specific servers.

> **Note:**
>
> The ability to install a rule is dependent on an interface's capabilities. For example, an access rule can only be installed on an interface whose capabilities show support for **Access**. For more information, see *IP Service Activator User's Guide*.

You can specify whether a rule applies to an interface's inbound or outbound traffic, or traffic in both directions.

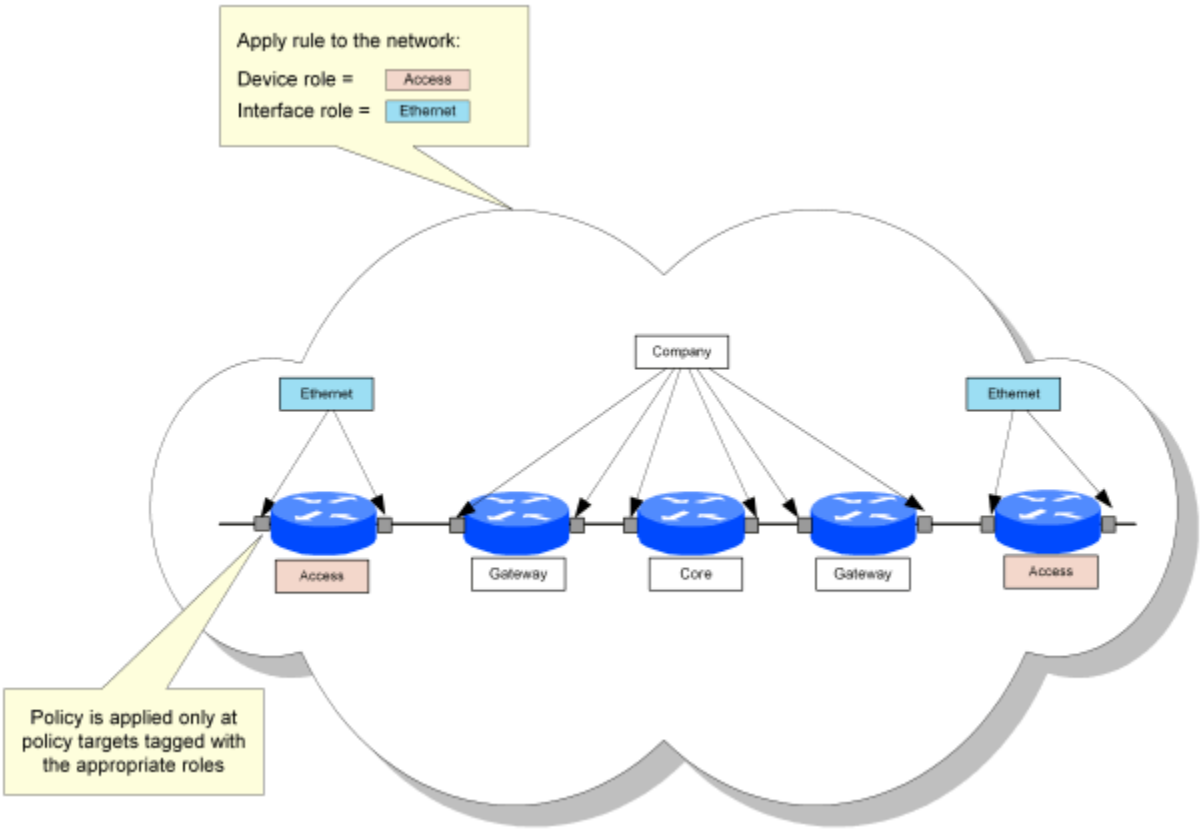
The type of traffic a rule applies to can be defined within the rule itself, based on source and destination address and traffic type. Alternatively, if you have created standalone traffic classifications, you can associate any number of classifications or classification groups with a rule. See "Setting Up a Classification" for information on defining classifications.

Using Roles in Rules

Policy rules can be created at almost any point in the network hierarchy, including domain level, or associated with a VPN, customer or site.

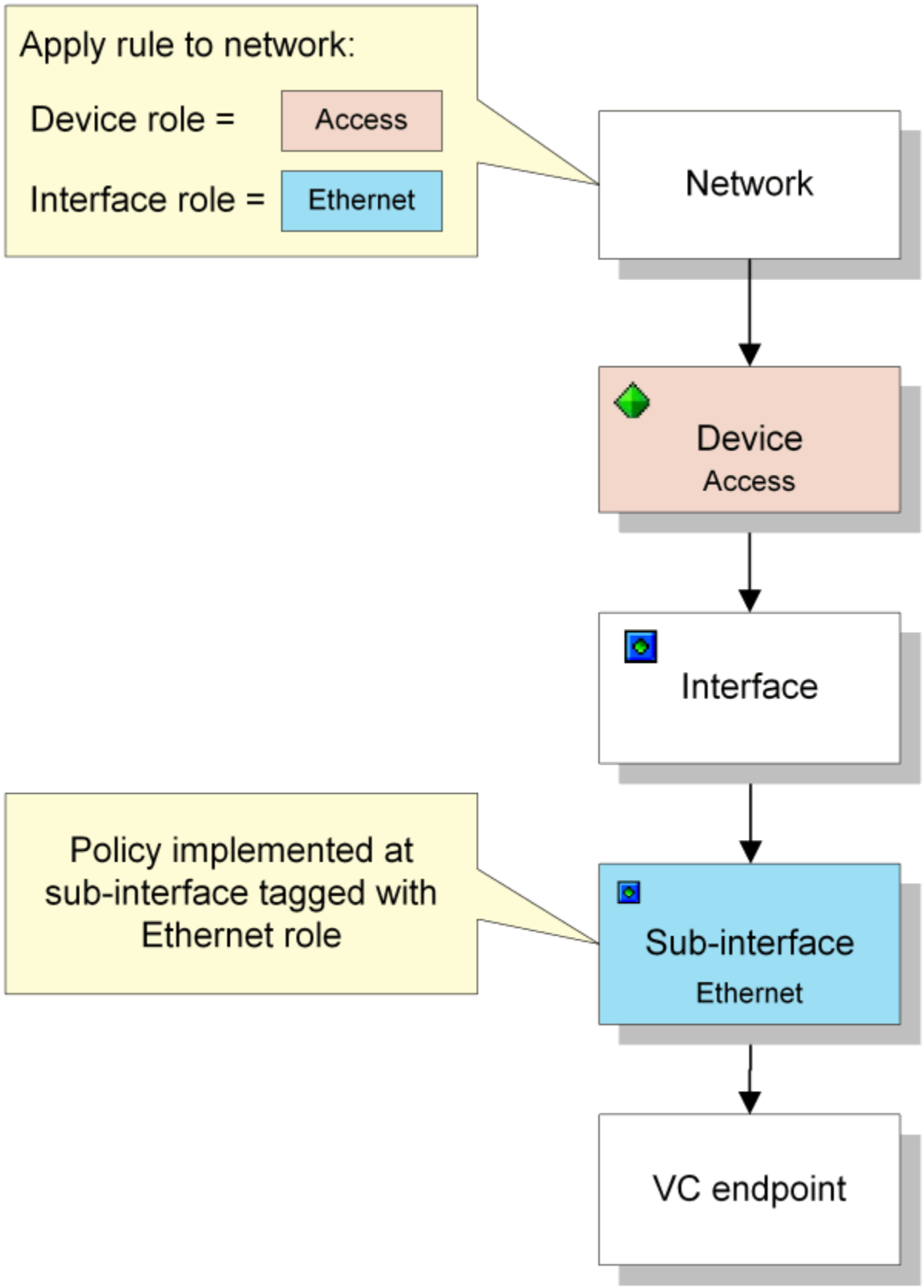
Rules are automatically inherited so that they are applied to all relevant interfaces and/or sub-interfaces on appropriate devices. You specify relevant interfaces or sub-interfaces by associating a device and interface role with the rule. The rule is only applied where the device and interface role match the roles specified in the rule. Figure 3-1 shows an example.

Figure 3-1 Roles in Rules



You can use roles to apply policy at very specific points in the network. For example, you can apply a role to a sub-interface independent of its parent interface. By associating a rule with the sub-interface role, the rule's policy is applied only at the sub-interface. See Figure 3-2 for more details.

Figure 3-2 Role Application



> **Note:**
>
> When you create a rule, there are no policy roles associated with it by default. You must associate both a device and an interface role for the rule's configuration to be applied at the appropriate points in the network. If either the device or interface role are not specified, no configuration will be applied.

Each implementation of a rule at a specific point in the network results in a concrete rule. A concrete rule is an implementation of a classification rule, policing rule or access rule that applies to a specific point in the network, i.e. at a particular interface or sub-interface. There may be several concrete rules for each parent or abstract rule. See "Checking Implemented Rules" for more information.

See "Policy Inheritance" for information on how policy is inherited in IP Service Activator.

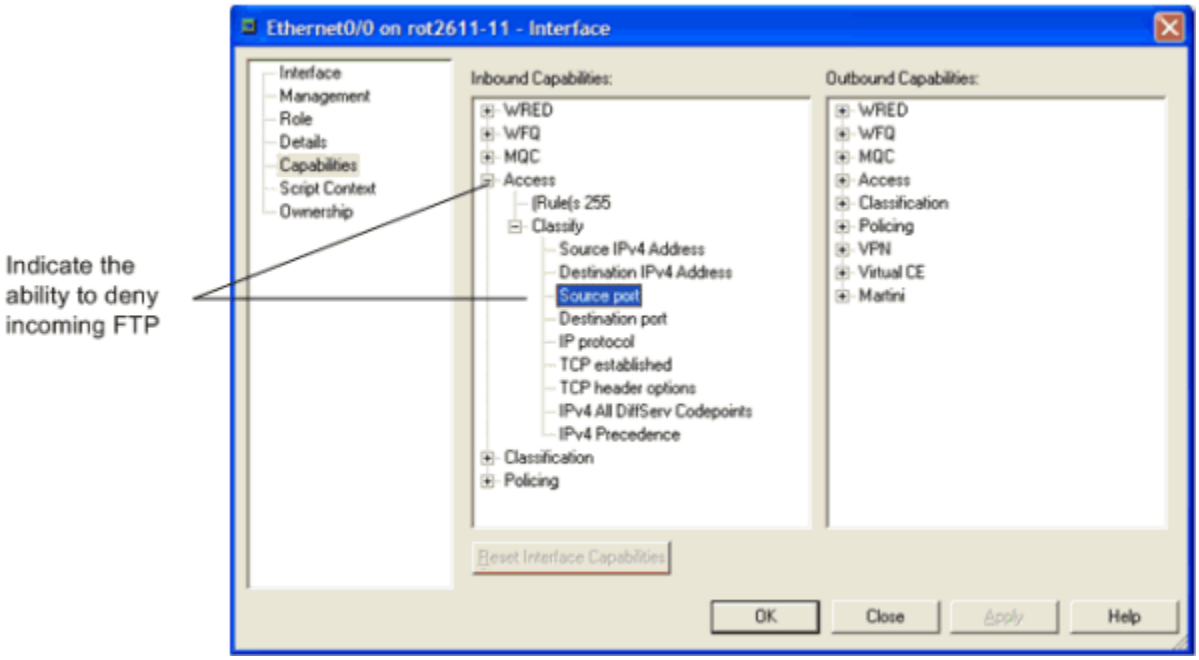
Rule Support on an Interface

The ability to install a particular type of policy rule is dependent on an interface's capabilities. These capabilities indicate:

- Whether the interface supports a particular rule type
- What traffic types the interface can classify on – effectively, which traffic classification types can be associated with a rule
- For classification and policing rules, the interface's packet marking capabilities – for example, whether the interface can mark on all DiffServ codepoints or IP Precedence bits only

For example, an access rule that denies incoming FTP traffic can only be installed on an interface whose inbound capabilities show support for **Access**, with the classification subcategory **Source port**. See Figure 3-3.

Figure 3-3 Rule Support Example



Using Roles in Rules

In order for a rule to be applied to a policy target, it must have both a device and an interface role associated with it. This role combination specifies where the rule will be applied. See "Using Roles in Policy Elements" for information on using roles in policy elements.

Classification Rules

Classification rules specify how devices identify categories of network traffic and define how they are to be treated. For example, you can use a classification rule to re-mark packets of a particular traffic classification.

For information on device-specific support for classification rules, see the applicable cartridge guide.

Packet marking can also be implemented using an MQC PHB group. See "Setting Up Class-Based Marking" for more information.

> **Note:**
>
> If a classification rule is configured on an interface using policy maps, you cannot configure an MQC PHB group on the same interface.

Create one classification rule for each classification and marking strategy you need to implement. The number of rules required will depend on the number of traffic classifications and classification groups defined. For example, if you have four different categories of traffic to be managed using two classification strategies, you should:

- Create classification groups for traffic in each of the classification strategies
- Define two classification rules, one for each classification group

Each classification rule specifies:

- The traffic to be managed and the action to be taken
- The device and interface role combination to which the rule applies

> **Note:**
>
> You must specify a device and interface role within a rule definition. The system-defined role **Any Role** can be used where the rule applies to all roles.

The actions taken can include any (or all) of the following:

- Mark IP packets with a DiffServ codepoint value
- Mark IP packets with an IP Precedence value
- Mark MPLS packets with an MPLS Experimental bit value
- Various other packet markings

> **Note:**
>
> Note that classification rules cannot use packet markings specifying settings for the Frame Relay Discard Eligible bit or ATM Cell Loss Priority bit.

Traffic can be identified by a combination of source and destination IP address or account – for example, source or destination port. The traffic affected by the rule can be defined within the rule itself or based on one or several pre-defined traffic classifications or classification groups.

Traffic Type Port Definitions support identifying traffic from TCP flags found in TCP packets.

The following TCP flags can be specified:

- Established
- ACK
- RST
- URG
- PSH
- SYN
- FIN

Further classifications based on ICMP protocol can be done using the **Messages** drop-down menu. This menu is enabled only when **ICMP** is selected as IP protocol on the Port Traffic property page.

These are the available ICMP protocol options:

- EchoRequest
- EchoReply
- TTLExceeded
- Unreachable
- Redirect
- TimeExceeded
- PacketTooBig
- SourceQuench
- AdministrativelyProhibited

The ICMPv6 protocol is used for IPv6 traffic.

These are the available ICMPv6 protocol options:

- EchoRequest
- EchoReply
- Unreachable
- Redirect
- TimeExceeded
- PacketTooBig

ICMP protocol options are enabled only if ICMP is selected as IP protocol on Port Traffic property page.

Optionally, classification rules can be made conditional on a date or time.

You can copy an existing classification rule to other policy targets and update values for multiple roles. See "Copying Rules" and "Updating Multiple Rules" for more information.

Setting Up a Classification Rule

To set up a classification rule:

1. Select the object to which the rule applies.

   You can apply a classification rule to any policy target.
2. Right-click and select **Add Classification Rule**.
3. On the Classification Rule property page, enter values including **Name**, **Quality of Service**, **Direction**, and **Rule Status**.
4. Under Classification either specify that the rule applies to traffic defined within the rule or to one or several pre-defined classifications or classification groups.
5. To set a guaranteed bandwidth level to be assigned to the traffic, select the **Guarantee** check box and enter a value (in Kbits/s).
6. If the traffic classification to which the rule applies is defined within the rule, select the Classification property page and specify the source and destination points between which the rule is applied.

7. If the rule applies to one or more pre-defined traffic classifications or classification groups, select the Classification property page and select the relevant classifications or classification groups.

> **Note:**
>
> The **Local Classification** check box indicates if classification is defined within the rule or by a classification or classification group. Select IPv4 or IPv6 from the list provided next to Local Classification. If selected, details of the source/destination and traffic type are set up on the rule's Classification page. If cleared, one or more predefined classifications or classification groups can be selected on the Classification page.

8. Select the Role property page and select the device and interface roles to which the rule applies.

   You must specify both a device and an interface role. The system-defined Any Role can be used to apply the rule to any device or interface tagged with a role.

9. On the Marking property page, specify how the rule is to mark packets by selecting the **Packet Marking** with which identified packets are to be marked.

10. If you want the classification rule to apply at a particular date or time, select the Date and Time property page.

    You can select from any previously set up date and time template listed in the Name combo box. Alternatively, you can select Local from the combo box and enter details directly of the date and time that the policy is to apply.

    The **Address Type** field accommodates both IPv4 and IPv6 addresses. Local or global classifications must be set for Ipv4 or IPv6 based on requirement.

11. Click **OK** to close the dialog box, and save the rule.

For complete dialog box and property page descriptions, see IP Service Activator online Help. See "Checking Implemented Rules" for details of how to check the implemented rules.

For details on vendor support for PHB group properties, see the vendor-specific cartridge guide.

Policing Rules

Policing rules specify one or more traffic classes to be policed, their bandwidth allocation and the action to take for traffic that conforms to or exceeds the specified bandwidth. For example, traffic that exceeds the bandwidth requirements can be dropped or re-marked with a lower DiffServ codepoint.

Policing rules can be associated with any policy target.

Policing can also be implemented using an MQC PHB group. See "Setting Up Class-Based Policing" for more information.

Depending on how your system is configured, you may need to create one or a number of policing rules for each traffic class to be managed. By grouping traffic classes into traffic classification groups, you may be able to minimize the number of

rules required. See "Setting Up a Classification" for information on defining traffic classifications and classification groups.

Each policing rule specifies the traffic to be policed and the action to be taken.

Traffic to be policed can be identified by a combination of source and destination IP address or account and traffic type – for example, source or destination port. The traffic class to be policed can be defined within the rule itself or based on one or more pre-defined traffic classifications or classification groups.

The following bandwidth requirements can be set:

- Committed rate permitted
- Normal burst size permitted
- Excess burst size permitted

The committed rate can be specified on its own or in combination with normal burst size and excess burst size.

For Cisco devices there are certain behaviors where parameters (such as CAR) are rounded off by IP Service Activator. For more information, see the applicable cartridge guide.

IP Service Activator configures an ACL to identify the traffic policed by the rule. By default, IP Service Activator generates the ACL name/number but you can override this and specify a name/number.

Optionally, policing rules can be made conditional on a date or time.

To set up a policing rule:

1. Select the object to which the rule applies.

   You can apply a policing rule to any policy target.
2. Right-click and select **Add Policing Rule** from the pop-up menu.
3. On the Policing Rule property page, enter details including **Name**, **Bandwidth Requirements**, and **Direction** for the rule.
4. Under Classification select the **Local Classification** check box to specify source/destination and traffic type within the rule or clear it to associate the rule with one or several pre-defined classifications or classification groups.
5. If you wish to specify the name/number of the ACL generated for the policing rule, select **Value** under Access Control List and specify a value.
6. If the traffic class to which the rule applies is defined within the rule, select the Classification property page and specify **Source**, **Destination**, and **Traffic Type**.
7. If the rule applies to one or more pre-defined traffic classifications or classification groups, select the Classification property page and select the relevant classifications or classification groups.
8. Select the Role property page and select the device and interface roles to which the rule applies.

   You must specify both a device and an interface role. The system-defined Any Role can be used to apply the rule to any device or interface tagged with a role.
9. On the Action property page, define the action to be taken for conforming and non-conforming traffic choosing from **Drop**, **Transmit**, **Continue** and **Re-Mark as** in the Conform Action and Exceed Action panels.

Re-marked packets may be treated differently at subsequent routers.

> **Note:**
>
> Policing rules cannot use packet markings specifying settings for the Frame Relay Discard Eligible bit or ATM Cell Loss Priority bit. For Re-Mark and Continue to work correctly, you need to set up several policing rules in a logical sequence.

10. If you want the rule to apply at a particular date or time, select the Date and Time property page.

    You can select from any previously set up date and time template listed in the Name combo box. Alternatively, you can select **Local** from the combo box and enter details directly of the date and time that the policy is to apply.

11. Click **OK** to close the dialog box, and save the rule.

See "Checking Implemented Rules" for details about how to check the implemented rules.

Access Rules

Access rules (or filters) are used to provide network security by explicitly denying or permitting access by identified traffic.

Traffic can be identified by a combination of source and destination IP address or account and traffic type – for example, source or destination port. The traffic affected by the rule can be defined within the rule itself, or based on one or more pre-defined traffic classifications.

Depending on how your system is configured, you may need to create one or several access rules for each traffic class to be managed. By grouping traffic classes into traffic classification groups, you may be able to minimize the number of rules required. See "Setting Up a Classification" for information on defining traffic classifications and classification groups.

The identified traffic can be denied or permitted access. Each rule can apply to inbound traffic only, outbound traffic only or both.

Optionally, access rules can be made conditional on the date or time.

To set up an access rule:

1. Select the object to which the rule applies.

   You can apply an access rule to any policy target.

2. Right-click and select **Add Access Rule** from the pop-up menu.

   The Access Rule dialog box opens.

3. Enter an identifying name for the rule.

4. Under ACL type, specify whether **Named** or **Numbered** ACls are to be generated. Enter a value in the appropriate field or select **Generate** to use a system generated name or number.

5. Select or clear the **Management rule override** check box to avoid automatic creation of ACL rules. ACL rules are automatically generated to assure SNMP and Telnet access from IP Service Activator to the CE.
6. On the Access Rule property page of the Access Rule dialog box, select from the following options:
   - **Permit** or **Deny** the identified traffic
   - Log (All) Enables / Disables Cisco ACL logging

   Under Direction, specify one or both of the following:
   - **In**: Apply to inbound traffic
   - **Out**: Apply to outbound traffic

   Under Rule Status, specify one of the following:
   - **Disable**: Select to switch off the rule.
   - **Conflict**: When selected, indicates that the rule is in conflict with another rule. This is a read-only field.
   - **ID**: Internal ID number of this object; allocated automatically by IP Service Activator.
7. Enter values including **Name**, **Action (Deny, Permit)**, **Direction (In, Out)**, and **Classification**.
8. If Classification was set to Local Classification, select the Classification property page and specify the source and destination points between which the rule is applied. Otherwise, select the Classification property page and select the relevant classifications or classification groups. There is a check box to indicate if classification is defined within the rule or by a classification or classification group. Select **IPv4** or **IPv6** from the list provided next to Local Classification. If selected, details of the source/destination and traffic type are set up on the rule's Classification page. If cleared, one or more predefined classifications or classification groups can be selected on the Classification page.
9. Select the Role property page and select the device and interface roles to which the rule applies.

   You must specify both a device and an interface role. The system-defined **Any Role** can be used to apply the rule to any device or interface tagged with any role.
10. If you want the access rule to apply at a particular date or time, select the Date and Time property page.

    In the **Name** field, you can choose from any previously set up date and time template listed in the pull-down menu. Alternatively, you can select **Local** from the combo box and enter details directly of the date and time that the policy is to apply.

    The **Address Type** field accommodates both IPv4 and IPv6 addresses.
11. Click **OK** to close the dialog box.

Copying Classification, Policing and Access Rules

It is possible to quickly copy and paste Classification, Policing, and Access rules between objects in the same domain. This makes it simple to re-create the settings for a rule on another object, without having to access a lot of property pages.

To copy Classification, Policing, and Access rules:

1. Double-click on the item which has the source rule already applied to it.

2. Select the appropriate tab — **Classification Rules**, **Policing Rules**, or **Access Rules** — in the **Details** pane to show the rule to be copied.
3. Select the source rule and click the copy icon in the toolbar.
4. Double-click the target item to which you want copy the rule.
5. Ensure the appropriate tab in the Details window is still selected, and click inside the **Details** pane. The enables the **Paste** button in the toolbar.
6. Click the **Paste** button in the toolbar.

   The rule is copied to the destination object. Modify the roles and values of the newly copied rule as you wish.

Using the Deny Classification in Cisco ACLs

On Cisco devices, IP Service Activator supports the ability to process or block/ignore traffic by means of exclusion. In other words, Classification objects (classifiers) can be created which match traffic to be excluded from further processing. For example, you can define a set of criteria so that all traffic that does not match the criteria will have QoS applied and traffic that does match the criteria will not.

The exclusion capability corresponds to the creation of Cisco ACLs employing the deny keyword. When Cisco ACLs are evaluated, processing of classification statements stops when the first match is found. Therefore, the ordering of entries in IP Service Activator Classification objects is of high importance. Capabilities in the IP Service Activator user interface support the specification of entry order in these objects.

Below is an example ACL using the Deny keyword:

```
access-list 180 deny ip any any
```

The deny keyword is an instruction to block all traffic that matches the criteria in the ACL statement. In this example, the device blocks all IP-type traffic to which access-list 180 is applied.

> **Note:**
>
> If no conditions match, the software drops the packet. This is because each access list ends with an unwritten or implicit **deny** statement. That is, if the packet has not been permitted by the time it was tested against each statement, it is denied.
>
> The access list must contain at least one **permit** statement or else all packets are denied.

User Interface

The IP Service Activator user interface supports the **deny** action in Classification objects.

The Classification dialog box, Details property page, contains two radio buttons and two check boxes:

- **Include**: The traffic that matches the specified criteria in the classifier is explicitly included in the processing applied to the classifier. This selection corresponds to the **permit** keyword in Cisco ACLs.
- **Exclude**: The traffic that matches the specified criteria in the classifier is explicitly excluded in the processing applied to the classifier. This selection corresponds to the **deny** keyword in Cisco ACLs.
- **Log**: Enables or disables Cisco ACL logging. Headers of packets affected by the access rule are stored in the routing engine and can be displayed using the **show log** command.

> **Note:**
>
> Enabling ACL logging may negatively affect router performance. Processor power may be used to perform the logging and log files may impact available disk space.

- **Fragments**: When selected, non-initial packet fragments are included for matching. This selection corresponds to the Fragments parameter in Cisco ACLs.

Updating Multiple Rules

You can update several rules simultaneously. The rules must be defined at the same point in the network – that is, you must be able to list and select them in the Details pane for a given policy target.

You can apply a new date and time template to any rule. For classification rules, you can also re-specify the packet marking to be applied.

To update multiple rules:

1. Double-click on the relevant object – any policy target – from the hierarchy tree or the topology map.

   The configuration that applies at the selected level is listed in the **Details** pane - select the relevant tab.
2. Select several abstract rules whose values you want to set.

   Abstract rules are displayed on a white background. If a rule has a gray background, it has been inherited from a higher point in the hierarchy indicated by the Level column.
3. From the pop-up menu select **Properties**.

   The Classification Rule dialog box opens. It contains a subset of the property pages that are available for a single rule.

   > **Note:**
   >
   > If you have included a concrete rule in the selection, no property pages are displayed on the Classification Rule dialog box. Deselect the concrete rule to display the dialog box correctly.
4. Select the relevant tabs and specify the values you wish to apply.

> **Note:**
>
> Only user-defined templates are available for selection on the Date and Time property page when updating multiple rules. You can only apply the default Local setting to individual rules.

5. Click **OK**.

   The values are applied and the new values displayed in the rule list.

Copying Rules

You can copy one or more rules from one policy target to another. Rules may already be applied to the target object. To prevent naming conflicts, the copied rule is named as follows:

- If there is no naming conflict between the copied and the existing rules, the rule is copied to the target object with the same name.
- If the copied rule conflicts with an existing rule name, the rule is copied with the text **Copy of** preceding the rule name. If subsequent copies are made, the copy number is incremented – that is, **Copy (n) of** where n is the copy number.

Some of the values associated with the rule may need to be edited after copying. For example, a different date and time template may need to be selected.

You cannot copy classification rules from one domain to another.

> **Note:**
>
> Editing the values associated with a copied rule may result in two rules of the same name that have different values.

To copy rules using menu commands:

1. List an object's rules in the details pane and select one or more rules to be copied.
2. From the **Edit** menu, select **Copy**.
3. Select the target object, and from the **Edit** menu select **Paste**.

To copy rules using drag and drop:

1. List an object's rules in the details pane.
2. Open a new window for the target object and from the **Window** menu select **Tile**.
3. List the relevant rules for the target object in the details pane. Ensure that there is space at the end of the rule list.
4. Select one or more rules to be copied from the source object and drag them to the target object's details pane.

You must drag the rules on to white space in the target window.

Implementing Rules

As you create rules through the user interface they are queued in the current transaction. Depending on your user access level, you may be able to commit the transaction immediately, or save it in a pending state for checking and committing by a supervisor. The policy defined by a rule is not implemented until the transaction it forms part of is committed.

For information on transactions, see *IP Service Activator Concepts*.

Checking Implemented Rules

After you have propagated rules to devices throughout the network, you can check how and where the rules have been implemented.

Viewing Implemented Rules

At any one time, a number of rules may be listed for a policy target – particularly as rules can be applied to various levels of both the logical and the physical hierarchy and applied via a process of inheritance. See "Policy Inheritance" for information on inheritance.

The listed rules may have originated at a higher point in the hierarchy. IP Service Activator uses color to indicate whether the rule is abstract or concrete.

Note that you can also view summary information for rules (see "Viewing System Statistics and Statistic Summary Information") as well as searching for concrete rules by type and status.

For information on locating concrete policy elements and what to do if concrete rules are not created, see *IP Service Activator User's Guide*.

To view the rules that apply to an object:

1. Double-click on the relevant object – any policy target – from the hierarchy tree or the topology map.

   The configuration that applies at the selected level is listed in the Details pane.

2. Select the relevant tab depending on the policy element type to view the rules that apply.

Each abstract (parent) rule is followed by a list of the concrete rules that have been created at appropriate interfaces.

If there are one or more concrete rules associated with an abstract rule, a plus-sign icon is displayed next to the rule. Click on the icon to expand or collapse the list of associated concrete rules.

For information on classification rules, access rules and policing rules, see IP Service Activator online Help.

Viewing System Statistics and Statistic Summary Information

For information on how to view system statistics and statistics summary information, see *IP Service Activator System Administrator's Guide* or IP Service Activator online Help.

For information on locating concrete policy elements and what to do if concrete rules are not created, see *IP Service Activator User's Guide*.

Managing Rules

This section discusses changing the sequence order of rules, avoiding rule conflicts, and disabling rules.

Changing the Sequence Order of Rules

At any one time, a number of rules of a specific type (classification, access or policing rules) may apply to a particular interface – particularly as rules can be applied to various different levels and applied via a process of inheritance.

The abstract and inherited rules that apply to a policy target are listed in the following order:

- Abstract rules: Rules created at the object
- Inherited rules: Rules that have been inherited from an object higher in the hierarchy

Inherited rules are further subdivided according to where the corresponding abstract rule was applied.

The order in which rules are listed in the details pane is important as this defines the order in which rules are checked against packets on that interface. The first rule that matches the packet is applied. Therefore you must ensure that rules appear in the correct order – for example, you need to ensure that a more general rule does not appear before a specific rule that would therefore never be checked.

The initial order reflects the order in which the rules were created, but you can change the order if required, by dragging and dropping rules to a new position in the list.

> **Note:**
>
> You cannot move inherited rules above abstract rules – this means that abstract rules always override inherited rules.

How Rule Conflicts are Avoided

It is potentially possible for two rules of the same type to be in conflict if there is any overlap in the defined traffic. Inadvertent conflicts may occur where rules are created at various levels (domain, customer, VPN, site, device, interface or VC endpoints). For example, an access rule defined at a high-level object might apply to all port-based traffic types, while an access rule defined at a lower-level object applies to a specific port.

Potential rule conflicts are dealt with automatically by IP Service Activator by a process of rule ordering. At each interface, IP Service Activator checks the rules in a strict sequence and rules are not applied if they would result in a conflict. Rules created at a lower level override those created at a higher level - for example, a classification rule created at a specific interface overrides one created for the whole domain. Where multiple rules apply at any one level, they are checked in their defined sequence order, which can be changed.

The priority levels are shown in Table 3-1. Lower numbers indicate higher priority.

Table 3-1 Rule Conflict Priorities

Object	Priority
Root network	15
Network	14
Domain	12
Customer	10
VPN	8
Site	6
Device	4
Interface	3
Sub-interface	2
VC endpoint	1

For example, a rule that applies to a device takes precedence over a rule applied at the domain level. In the case of PHB groups, only one PHB group can be applied to any one interface, so the highest priority PHB group in the list is applied, and others that may apply are ignored.

Disabling Rules

On the Access Rule property page, you can disable an abstract rule applied by an object by selecting the **Disable** check box in the Rule Status group.

4

Defining Standard Per Hop Behavior Groups

This chapter describes how to implement queuing and traffic shaping mechanisms in an Oracle Communications IP Service Activator network using standard Per Hop Behavior (PHB) groups. The chapter:

- Provides an overview of standard PHB groups and the queuing and traffic shaping mechanisms that can be implemented using IP Service Activator.
- Highlights points you should consider before setting up standard PHB groups.

See "Implementing and Managing Per Hop Behavior Groups " for details on implementing and managing PHB groups. See "Defining MQC PHB Groups " for information on defining MQC PHB groups.

Introduction

A PHB group provides a way of managing traffic at specific interfaces by implementing a device-specific queuing or traffic shaping mechanism. Standard PHB groups manage traffic in one of two ways:

- Class-of-service (CoS) mechanisms allow you to define different priorities or bandwidth allocations for each class of service that will be used in your network. Examples include configuring Weighted Round Robin (WRR) and Priority Queuing (PQ).
- VC mechanisms allow you to set up ATM and Frame Relay-specific traffic shaping at the VC endpoint level. These mechanisms apply to all traffic on the endpoint, irrespective of class of service.

A PHB group can be applied to a network component (such as a network, device or interface) or to a customer, site or VPN. As for any other policy element, the policy targets that a PHB group actually applies to are controlled using policy roles and the inheritance model.

Within IP Service Activator there are no restrictions on where a PHB group can be applied. For example, you can apply a WRR PHB group to a device at the network edge or in the network core.

> **Note:**
>
> IP Service Activator's ability to install a PHB group on a network object is dependent on an interface's capabilities. For example, a WRR PHB group can only be installed on an interface whose capabilities show **WRR** support. For information on checking interface capabilities, see *IP Service Activator User's Guide*.

Supported Traffic Shaping/Queuing Mechanisms

This section discusses CoS mechanisms, VC traffic shaping mechanisms, vendor support, and CoS mechanism combinations.

Class of Service Mechanisms

The following queuing and shaping mechanisms can be implemented within a standard PHB group and applied to traffic by CoS:

- WRR
- PQ
- Rate limiting/traffic shaping
- Weighted Random Early Detection (WRED)
- Weighted Fair Queuing (WFQ)

VC Traffic Shaping Mechanisms

The following per-VC traffic shaping mechanisms can be implemented within a standard PHB group:

- ATM Traffic Shaping
- Frame Relay Traffic Shaping (FRTS)

ATM traffic shaping and FRTS are applied to all traffic on the VC endpoint. They cannot be applied to selected classes of service.

Vendor Support

Table 4-1 summarizes device type support for each class of service mechanism.

Table 4-1 Device Type Support

Mechanism	Cisco	Juniper M-series	Juniper E-series
WRR	Y	Y	N
PQ	Y	N	N
Rate Limiting	Y	Y	N
WRED	Y	Y	N
WFQ	Y	Y	N
ATM Traffic Shaping	Y	N	N
FRTS	Y	N	N

Note:

If you apply FRTS to Frame Relay interfaces on distributed platforms, such as 75xx VIP-based devices, IP Service Activator configures Distributed Traffic Shaping (DTS) rather than FRTS. Alternatively, you can apply FRTS to Frame Relay interfaces on distributed platforms using an MQC PHB group. See "Defining MQC PHB Groups " for more information.

Class of Service Mechanism Combinations

Table 4-2 shows the CoS mechanism combinations that are permitted in a standard PHB group.

Table 4-2 Standard PHB Group CoS Mechanism Combinations

CoS	WRR	WFQ	PQ	WRED	Rate Limiting	ATM TS	FRTS
WRR	Y	N	N	N	Y	N	Y
WFQ	N	Y	N	Y	N	N	Y
PQ	N	N	Y	N	Y	N	Y
WRED	N	Y	N	Y	N	N	N
Rate Limiting	Y	N	Y	N	Y	N	N
ATM TS	Y	Y	Y	Y	Y	Y	N
FRTS	Y	Y	Y	Y	N	N	Y

WRR and Priority Queuing are mutually exclusive, but on some devices you can implement rate limiting in conjunction with a queuing mechanism.

On Cisco devices, you can implement Low Latency Queuing (LLQ) on a Frame Relay interface by selecting Priority Queuing for class-based WFQ in combination with FRTS or you can use an MQC PHB group.

Table 4-3 shows the combinations of QoS actions permitted in an MQC PHB group.

Table 4-3 MQC PHB Group QoS Combinations

QoS	LLQ	CB-WFQ	SR Police	TR Police	Shape	Mark	Congestion	Nest	RTP Compression
LLQ	*	N	Y	Y	N	Y	Y	Y	Y
CB-WFQ	N	*	Y	Y	Y	Y	Y#	Y	Y
SR Police	Y	Y	*	N	Y	Y	Y#	Y	Y
TR Police	Y	Y	N	*	Y	Y	Y#	Y	Y
Shape	N	Y	Y	Y	*	Y	Y	Y	Y
Mark	Y	Y	Y	Y	Y	*	Y#	Y+	Y
Congestion	Y	Y#	Y#	Y#	Y	Y#	#	Y#	Y#
Nest	Y	Y	Y	Y	Y	Y+	Y#	+	Y+
RTP Compression	Y	Y	Y	Y	Y	Y	Y#	Y+	*

> **Note:**
>
> Y – Combination of the two QoS actions is allowed
>
> * – Can be selected on its own
>
> # – Requires Shape, LLQ, and/or CB-WFQ to be selected except for the default CoS
>
> + – Requires any combination of Shape, SR/TR Police, CB-WFQ, LLQ
>
> N – Combination of the two QoS actions is not allowed

Before Setting Up a Standard PHB Group

This section outlines the points you need to consider before setting up a standard PHB group.

Selecting the Queuing or Traffic Shaping Mechanisms

The decision as to which queuing or traffic shaping mechanism to use depends on the policy you want to implement and the capabilities of the router. Since the available techniques are often specific to the device type, operating system and interface, consult the relevant vendor's documentation for your specific device(s).

IP Service Activator reports the capabilities of each interface. Ensure the interface is reported by IP Service Activator to support the desired operation. For information on checking an interface's capabilities, see *IP Service Activator User's Guide*. For more information about supported capabilities, consult the router documentation.

You must set up a standard PHB group for each different queuing mechanism you want to implement.

Deciding Where to Apply the Standard PHB Groups

A standard PHB group defines a queuing or shaping mechanism that can be used at various points in the network. For example, a PHB group might be used to manage the traffic going into the core network or to maintain the prioritization set up at the network edge throughout the core network.

PHB groups are implemented on the inbound and/or outbound interfaces of the routers to which they are applied. However, they are created as templates within a domain and can be applied to various points throughout the network.

A PHB group, applied to devices and interfaces sharing the same role on the root level network, will also automatically apply to all relevant interfaces throughout the network. In accordance with IP Service Activator's policy inheritance model, a locally defined PHB group overrides a PHB group defined at a higher level. Because IP Service Activator can only apply one concrete PHB group to an interface, a locally defined PHB group will take precedence over the inherited PHB group.

See "Policy Inheritance" for more information on inheritance.

Using Roles in PHB Groups

Every PHB group must have a device and interface role associated with it. The roles you associate with a PHB group specify the policy targets to which the queuing mechanism will apply. See "Using Roles in Policy Elements" for information on using roles in policy elements.

Depending on the roles that you assign to policy targets, it is possible to apply policy only at very specific points in the network. For example, you can apply a role to a sub-interface independent of its parent interface. By associating a PHB group with the sub-interface role you can apply policy only at the sub-interface.

Importing Policy Files

IP Service Activator provides sample PHB groups and policy rules in policy files located in the SamplePolicy directory. See "Importing QoS-related Policy Files" for information on loading these policy files.

> **Note:**
>
> When you create a PHB group there are no policy roles associated with it by default. You must associate both a device and an interface role for the PHB group's configuration to be applied at the appropriate points in the network. If either the device or interface role are not specified, no configuration will be applied.

Setting Up a Standard PHB Group

When setting up a standard PHB group you must specify:

- The classes of service and/or VCs that are to be controlled by the PHB group.
- The roles that define the policy target of the PHB group.
- The queuing mechanism to be used, and any specific parameters that need to be set. This will depend on the mechanisms available on the devices to which the PHB group will be applied.

For complete dialog box and property page descriptions, see IP Service Activator online Help.

Setup and Application of PHB and MQC PHB Groups as Separate Operations

PHB groups can be created and stored as definitions within the object model. These PHB groups are visible under the **Policy** tab, but until they are applied to an object, they exist only as definitions and have no effect. Defined PHB groups are instantiated when they are applied to a target object in the object model. The normal rules of roles and inheritance apply to the target object and its sub-objects in the hierarchy.

An overview of the steps follows:

1. Right-click the **PHB Groups** folder and create a new PHB group.

2. Configure the PHB group and commit the transaction.
3. Display the target object in the Details pane.
4. Display the PHB group in the hierarchy pane.
5. Drag the PHB group onto the target object.
6. Commit the transaction.

This procedure applies to both PHB and MQC PHB Groups.

Setup and Application of PHB and MQC PHB Groups as a Combined Single Operation

You can combine the creation of the PHB Group definition and the instantiation of that PHB Group definition onto a target object into one operation.

An overview of the steps follows:

1. Right-click the target object and create a new PHB group.
2. Configure the PHB group and commit the transaction.

The PHB group definition is shown in the **Policy** tab.

This procedure applies to both PHB and MQC PHB Groups.

Setting Up a Standard PHB Group

To set up a standard PHB group:

1. Do one of the following:
   - On the **Policy** tab, select the **PHB Groups** folder.
   - Select a target object — a network component, device, interface, customer, site, or VPN.
2. Right-click on the folder or target object and select **Add PHB Group** from the pop-up menu.

   The PHB Group dialog box opens.
3. Enter values including **Name**, **Configured Name**, and **Direction**.
4. If a Virtual Circuit-based mechanism is to be applied, select **ATM** or **FRTS**.

   Note that these techniques are applied to all traffic on the VC, not per class of service. You can configure FRTS in conjunction with WRR, Priority Queuing, or CB-WFQ for finer control of traffic prioritization and queuing.
5. For CoS mechanisms, specify the classes of service to be controlled by this PHB group.

   Click on the check box associated with the desired CoS Mechanism.
6. Select the CoS queuing mechanism(s) that the PHB group will apply. See "Class of Service Mechanism Combinations" for more information.

   Click **Apply** to apply the changes before setting specific details of the selected CoS mechanisms.

7. Select the Role property page and select the device and interface roles to which the PHB group applies.

   You must specify both a device and an interface role. The system-defined Any Role can be used to apply the PHB group to any device or interface tagged with a role. See "Using Roles in PHB Groups" for information on using roles in PHB groups.

8. Select the appropriate property page(s), depending on the mechanism(s) selected and set the appropriate parameters. For details of configuring each mechanism, see the appropriate description:
   - WRR – "Setting up Weighted Round Robin"
   - PQ – "Setting up Priority Queuing"
   - Rate Limiting/Traffic Shaping – "Setting Up Rate Limiting "
   - WFQ – "Setting Up Weighted Fair Queuing"
   - WRED – "Setting Up Weighted Random Early Detection"
   - FRTS – "Setting Up Frame Relay Traffic Shaping"
   - ATM Traffic Shaping – "Setting Up ATM Traffic Shaping"
9. Click **OK** to close the dialog box and save the PHB group.

Setting up Weighted Round Robin

Weighted Round Robin (WRR) is a mechanism for allocating bandwidth to queues so that higher priority applications have more bandwidth than lower priority applications when the network is congested. Custom Queuing in Cisco devices is an implementation of WRR.

For complete dialog box and property page descriptions, see IP Service Activator online Help.

To set up WRR:

1. Select the WRR property page on the PHB Group dialog box.
2. Select the **Class of Service** and set **Weight** and **Packet limit** values.
3. Click **Apply** before changing another value. The specified weight is converted to a bandwidth percentage.
4. Repeat steps 2 to 3 for each class of service to be set up.

Setting up Priority Queuing

Priority Queuing specifies that each packet is to be placed in one of a number of queues according to its priority. Packets on the highest-priority queue are transmitted first; when that queue is empty, packets on the next-highest queue are transmitted, and so on.

For complete dialog box and property page descriptions, see IP Service Activator online Help.

To set up Priority Queuing:

1. Select the Priority Queuing property page on the PHB Group dialog box.
2. Selecting each CoS in turn, specify the **Priority** that will be applied (High, Medium, Normal or Low).
3. Click **Apply** before changing another value.

4. Repeat steps 2 to 3 for each class of service to be set up.

Setting Up Rate Limiting

Rate limiting, or traffic shaping, constrains specific outbound traffic to a particular bandwidth. It is commonly used to control access to the core network. It can be used to regulate the flow of traffic in order to avoid the congestion that can occur when transmitted traffic exceeds the access speed of the remote interface.

For complete dialog box and property page descriptions, see IP Service Activator online Help.

To set up Rate Limiting:

1. Select the Rate Limiting property page on the PHB Group dialog box.
2. Choose the **Class of Service** and set the **Average rate**, **Burst rate**, and **Burst interval**.
3. Click **Apply** before changing another value.
4. Repeat steps 2 to 3 for each class of service to be set up.

Setting Up Weighted Random Early Detection

Weighted Random Early Detection (WRED) is a variant of the RED mechanism, which drops packets randomly in times of congestion. WRED drops packets at specified thresholds. Different thresholds can be specified according to the IP Precedence or DiffServ codepoint of the packet. A minimum threshold level defines the queue size at which packets start to be dropped and a maximum threshold level defines the queue size at which a specified number of packets are dropped.

Applying WRED avoids congestion and is commonly used in the network core.

Normally, the WRED implementation on the device calculates default values for the minimum and maximum threshold settings for each interface, depending on the buffering capacity and speed of the interface.

To take advantage of this, use the **As default** setting. It is possible to override the defaults and set specific threshold values in the PHB, if required.

An MQC PHB group configured with congestion avoidance can use the WRED settings configured in a standard PHB group. The standard PHB group must only have WRED configured, can have any CoS associated with it that is not linked to a classification and must be linked to at least one packet marking. See "Setting Up Congestion Avoidance" for more information.

For complete dialog box and property page descriptions, see IP Service Activator online Help.

To set up WRED with default values:

1. Select the WRED property page on the PHB Group dialog box.
2. Ensure the **As default** check box is selected.
3. Click **Apply** or **OK**.

To set up WRED with specific values for an interface:

1. Select the WRED property page on the PHB Group dialog box.

2. Clear the **As default** check box.
3. Select **Explicit Congestion Notification**, if required.
4. Choose the **Class of Service** for which you want to set specific parameters.
5. Specify the **Min threshold**, **Max threshold**, and **Drop probability**.
6. If necessary, amend the default **Weight Factor** – an exponent weight factor used to calculate the average queue size. The range is 1 to 16, the default is 9.
7. Click **Apply** before changing another value.
8. Repeat steps 3 to 6 for each class of service to be set up.

You can configure WRED in conjunction with Class-based WFQ to define the drop strategy. See "Setting Up Weighted Fair Queuing" for more information.

Setting Up Weighted Fair Queuing

Weighted Fair Queuing (WFQ) is a queuing algorithm used for congestion management.

There are two types of WFQ:

- Flow-based: Used by default on all serial interfaces less than 2 Mbits/s on Cisco routers. A flow is identified as all packets with the same source IP address, destination IP address and source or destination TCP or UDP port. WFQ allocates an equal share of the available bandwidth to each flow.
- Class-based WFQ (CB-WFQ): Only supported on a restricted set of Cisco routers. It allows you to allocate a particular bandwidth to a particular class of service. Each class is allocated to a particular queue according to its bandwidth. A traffic class allocated a higher bandwidth has a higher priority than a traffic class allocated less bandwidth.

On Cisco routers, for interfaces that support WFQ you can either specify that flow-based WFQ is applied, or select CB-WFQ and set specific parameters for each class of service.

CB-WFQ can also be implemented on Cisco devices using an MQC PHB group. "Setting Up Class-Based Weighted Fair Queuing" for more information.

On Cisco devices, by default, flow-based queuing is applied and no parameters can be set. Since there may be very large numbers of individual flows, and one queue per flow, this is process-intensive, and is not recommended for fast interfaces.

For details on vendor support for PHB group properties, refer to the vendor-specific cartridge guide.

For complete dialog box and property page descriptions, see IP Service Activator online Help.

To set up flow-based WFQ:

1. Select the WFQ property page on the PHB Group dialog box.
2. Ensure the **Class Based** check box is cleared.
3. Click **OK**. Flow-based WFQ is configured on the appropriate interfaces using default parameters.

To set up CB-WFQ:

1. Select the WFQ property page on the PHB Group dialog box.
2. Select the **Class Based** check box.

3. Specify how the **Weight** field is interpreted by selecting **Interpret Weight** as either **Kbps** or **Percent**.

   Kbps specifies that values are entered directly.

   Percent specifies values as a percentage of available bandwidth.

4. Choose the **Class of Service** for which you want to set the weighting parameters.

5. Specify the **Weight**. This value specifies the weighting to be allocated to the selected class of service, either a Kbps value or a percentage, as specified above. By default, all classes are allocated equal weighting. Bandwidth values can be entered as exact values in kbits/s or as percentage values. If kbps is selected, weights entered must be in the range:

   For Low priority queues: 8 - 2 000 000

   For High priority queues: 32 - 155 000

   Choose a Queue Priority, of High if the traffic is directed to the CB-WFQ strict priority queue. Priority queuing for CB-WFQ (PQ CB-WFQ or LLQ) is particularly relevant to delay-sensitive data, such as voice traffic where it reduces jitter. You can include any number of Classes of Service in the priority queue.

   For Frame Relay traffic, you can set the Frame Relay Discard Eligibility (DE) bit for specific classes of service considered to be of lower priority. To set the DE bit for a particular class, select the **Set DE** check box.

6. Select the Drop Strategy by choosing one of the following options from the drop-down list:

   - **Default** - drop packets according to the device default.
   - **Tail Drop** - apply tail drop. A queue depth limit can be specified, and so can the units.
     - **Limit** - maximum queue depth in packets, if Tail Drop is selected as the Drop Strategy.
     - **Units** - cells, default, microseconds, milliseconds, packets

     > **Note:**
     >
     > If the Queue Priority is **High**, then the drop strategy must be set to **default**.

   - **Default WRED** - apply WRED to the queue, using the default WRED parameters.

     Any parameters entered on the WRED property page are ignored. Note that you must have selected WRED on the PHB Group property page.

   - **WRED** - apply WRED to the queue and set specific parameters on the WRED property page (see Configuring WRED). The Min Threshold, Max Threshold and Drop Probability parameters can be set per codepoint. For example if there are two codepoints in a class of service, two queues are configured, each of which can have independent WRED settings. The Weight Factor can be set per class of service.

7. Click **Apply** before changing to another class of service.

8. Repeat steps 3 to 7 for each class of service to be set up.

> **Note:**
>
> For information on monitoring the class maps that are configured for a CB WFQ PHB group, see *IP Service Activator Network and SLA Monitoring Guide*.

Setting Up ATM Traffic Shaping

Traffic shaping specifies a queuing mechanism to limit surges that can congest a network. Data is buffered and then sent into the network in regulated amounts to ensure that the traffic will fit within the promised traffic envelope for the particular connection.

For complete dialog box and property page descriptions, see IP Service Activator online Help.

To set up ATM Traffic Shaping

1. Select the ATM property page on the PHB Group dialog box.
2. In the field **VC class name** select **Generated** to use a system generated VC class name. To manually specify a name, type the name in the field. The maximum length of the name is 126 characters.
3. Select the **Service Category**.
4. Set the appropriate parameters including **PCR**, **SCR MBS** and **MCR**.
5. Specify appropriate values in **Hold queue depth** and **Transmit ring buffer** limit.
6. Click **OK**.

Setting Up Frame Relay Traffic Shaping

Frame Relay Traffic Shaping (FRTS) delays excess traffic using a queuing mechanism to hold packets and shape the flow when the data rate of the source is higher than expected. FRTS is sometimes used to eliminate bottlenecks in Frame Relay networks that have high-speed connections at the central site and low-speed connections at branch sites. A rate enforcement is configured to limit the rate at which data is sent on the VC at the central site.

FRTS is applied at VC level and can be combined with PQ, WRR, CB-WFQ or WRED applied at the VC or sub-interface. This allows for finer control over traffic prioritization and queuing.

You can configure FRTS to use information contained in the BECN (Backward Explicit Congestion Notification) and FECN (Forward Explicit Congestion Notification)-tagged frames received from the network. These features throttle traffic dynamically when congestion occurs.

The FRTS PHB group also allows you to apply FRF.12 fragmentation to traffic, either in conjunction with traffic shaping or independently. FRF.12 is a Frame Relay standard that allows long data frames to be fragmented into smaller pieces and interleaved with real-time frames. This means that real-time voice and non real-time data frames can be carried together on lower speed networks without causing excessive delay to the real-time traffic.

> **Note:**
>
> FRTS with FRF.12 cannot be used in combination with WRR or Priority Queuing.

You can implement LLQ on a Frame Relay interface by selecting FRTS in combination with CB-WFQ. For information on support for LLQ by Cisco devices, refer to the vendor-specific cartridge guide.

For complete dialog box and property page descriptions, see IP Service Activator online Help.

To set up FRTS:

1. Select the FRTS property page on the PHB Group dialog box.
2. To configure FRF.12, select the **FRF.12** check box and set the required **Fragment size**.
3. To configure traffic shaping, select the **Shaping** check box and set the parameters including **CIR**, **Min CIR**, **Bc**, and **Be**. You can configure **Inbound** and **Outbound** parameters independently, for vendor specific devices.
4. Select the **BECN Adapt** check box if you want to monitor for Frame Relay frames that have the BECN (Backward Explicit Congestion Notification) bit set.
5. Select the **FECN Adapt** check box if you want to monitor for Frame Relay frames that have the FECN (Forward Explicit Congestion Notification) bit set.
6. In the **Hold queue depth**, specify the maximum number of packets that can be stored in the traffic-shaping queue for a Frame Relay PVC. Select **Device default** to specify the default value for that particular device.
7. Click **OK**.

Distributed Traffic Shaping

If you apply FRTS to Frame Relay interfaces on distributed platforms, such as 75xx VIP-based devices, IP Service Activator configures Distributed Traffic Shaping (DTS) rather than FRTS. Like other traffic shaping mechanisms, DTS buffers excess traffic and regulates the rate at which packets are sent into the network, setting a Committed Information Rate (CIR) a Committed Burst (Bc) and an Excess Burst rate (Be).

Although the same parameters are configured for DTS, note that the permitted parameter ranges are different from those for FRTS. Table 4-4 shows the DTS parameters and ranges.

Table 4-4 DTS Parameters and Ranges

Parameter	Range
CIR	1 - 45 000 000
Min CIR	1000 - 45 000 000
Bc	300 - 16 000 000
Be	0 - 16 000 000

To configure DTS on Frame Relay Interface (7500):

1. Enable distributed Cisco Express Forwarding (dCEF) with the following command:

   ```
   router(config)#ip cef distributed
   ```

2. Ensure that the Frame Relay interface is enabled for distributed switching.

Before configuring DTS on frame relay interface (7500 series) through PHB FRTS, make sure that the following option elements are set as specified below for that device-ios combination:

```
<cartridge.cisco.qos.trafficShapingOnFRInterface>dts</
cartridge.cisco.qos.trafficShapingOnFRInterface>

<cartridge.cisco.qos.interface.frtsCommand>false</
cartridge.cisco.qos.interface.frtsCommand>
```

> **Note:**
>
> If the "cartridge.cisco.qos.interface.frtsCommand" parameter is not set as **false**, the "frame-relay traffic-shaping" command will be configured at interface level causing the device to rollback.

5

Extending IP Service Activator with Configuration Policies

This chapter explains how configuration policies extend the capabilities of Oracle Communications IP Service Activator.This chapter includes the following:

- An overview of configuration policies.
- Loading and accessing configuration policies.
- Customizing the organization of configuration policies in the GUI.
- Adding configuration policy files to Policy Types.
- Exporting policy files from Policy Types.
- Applying configuration policies.
- Applying configuration policies at the device level.

About Configuration Policies

Configuration policies extend the services supported by IP Service Activator. They are applied through the Configuration Policy functionality of the IP Service Activator GUI.

Configuration policies are used to add a variety of services to IP Service Activator and can be applied to object model targets at various points in the object hierarchy, depending on the nature of the service.

You can access configuration policies through the **Add Configuration Policy** context menu item for Customer, Site, Network, Device, Interface or Sub-interface objects. The information gathered through the HTML interface on the Configuration Policy dialog box is configured on devices through the Network Processor and appropriate underlying cartridge support.

> **Note:**
>
> IP Service Activator will not prevent you from applying configuration policies to objects in the object model that do not support them. You can confirm the appropriate targets a configuration policy by referring to its detailed field-level description topic in IP Service Activator online Help.

Obtaining and Creating Configuration Policies

A large number of ready-to-use configuration policies are provided with IP Service Activator and can be used as-is for various purposes.

Alternatively, you can use the IP Service Activator SDK to create and customize configuration policies as well as a service cartridge to support the implementation of the services that the configuration policy provides.

Getting More Information About Configuration Policies

For detailed information about particular configuration policies, including descriptions of all fields and ranges supported on the HTML input screen, see IP Service Activator online Help.

For details on how to use the IP Service Activator SDK to create configuration policies, see *IP Service Activator SDK Configuration Policy Extension Developer Guide*. Additional concepts including the integration of configuration policies with service cartridges are also described.

Configuration Policy Groupings

For easier access, available configuration policies are grouped by functionality in sub-folders of the **Policy Types** folder in the **Policy** tab. This hierarchy is also used to organize available configuration policy choices when choosing from the **Add Configuration Policy** pop-up menu.

When **.policy** files are created, information is included which dictates their initial sub-folder organization when they are loaded into IP Service Activator.

These sub-folders include:

- **Interface**: Contains interface-oriented configuration policies
- **Service**: Contains configuration policies for particular modelled services
- **Unclassified**: Contains miscellaneous configuration policy not oriented to a modelled service

There may be additional sub-folders in the hierarchy as well. These can be from custom configuration policies that have been loaded or from your own **Policy Type** sub-folder customizations.

> **Note:**
>
> The menu hierarchy in which configuration policies are presented when you right-click on a target object and select **Add Configuration Policy** matches the hierarchy of the sub-folders and configuration policies in the **Policy Type** folder in the **Policy** tab. When you customize the organization of configuration policies in the **Policy Type** folder, this also affects the menu organization.

Viewing and Customizing the Organization of Configuration Policies

You can set permissions to configuration policies on their Ownership property page. Denied permission can be selected on the Ownership property page for users who must not access specific configuration policies. For more information, see *IP Service Activator User's Guide*.

To view the configuration policies currently loaded into IP Service Activator:

1. On the Global Setup window, double-click a Domain from the Hierarchy pane to open it.
2. Select the **Policy** tab.
3. Expand the **Policy Types** folder.
4. Explore the hierarchy by expanding sub-folders to see which configuration policies are available.

To create a new configuration policy sub-folder:

1. Right-click on the parent folder and select **Add Folder**.

   The Policy Type Folder dialog box is displayed.
2. On the Policy Type Folder property page, enter a value for the **Name**.
3. Optionally, select the Ownership property page and specify user permissions for the folder.
4. Click **OK**.
5. Commit the transaction.

   The new folder is created in the Policy Types hierarchy.

To move a configuration policy, drag it from the source to the target folder under the **Policy Types** folder hierarchy and commit the transaction. There are restrictions on which folders particular configuration policies can be placed, based on their functional grouping. If a configuration policy can't be placed in a particular folder, you will not be able to drag and drop it to that location.

> **Note:**
>
> Once you move a configuration policy from its original location, do not reload it.

To delete a configuration policy from the GUI:

1. Right-click on the target configuration policy and select **Delete**.
2. Commit the transaction.

   The target configuration policy is deleted.

To delete a configuration policy sub-folder:

1. Right-click on the target folder and select **Delete**.
2. Commit the transaction.

   The target folder and its contents are deleted.

> **Note:**
>
> When you delete a configuration policy subfolder, its contents and any sub-folders and their contents are also deleted.

Applying Configuration Policies

Configuration policies are applied to various types of target objects in the object model, depending on their function and design. See "Applying Configuration Policies at the Device Level" for information on device-level configuration policies.

Applied configuration policies employ the normal IP Service Activator concepts of inheritance and roles. In order for a configuration policy to be successfully applied it must match a device and interface role and create a concrete at the interface, sub-interface or VC object level.

> **Note:**
>
> Configuration policies must be installed before you can use them in the GUI. See *IP Service Activator Administrator's Guide* for details.

To apply a configuration policy:

1. Click either the **Service** or **Topology** tab.
2. Locate the Customer, Site, Network, Device, Interface or Sub-interface target.
3. Right click the target, and select **Add Configuration Policy...** from the pop-up menu and choose the desired configuration policy from the cascading menu.

   The Configuration Policy dialog box displays the properties of a selected Configuration Policy, which allows the entry of either a set of raw XML commands, or an HTML-based entry form to collect information which is then converted to XML.
4. Provide the required information in the HTML-based entry form.
5. Click **OK**.
6. Commit the transaction.

For complete details on the fields in each configuration policy and the ranges of values that can be entered, see the individual configuration policy topics in IP Service Activator online Help.

Disabling Applied Configuration Policies

The **Disable** check box disables a configuration policy that is provisioned at the device level and applied to numerous interfaces through inheritance. This will disable the policy for all the interfaces it has been applied to.

Checking the **Disable** check box at the interface level disables the configuration policy only from the currently selected interface.

Applying Configuration Policies at the Device Level

Some configuration policies are designed to apply device-level commands (that is, commands that are not applied in the context of an interface). You can define

configuration policies to apply either at the device or interface level. For a device level policy, only the device role has to match.

To apply configuration policies:

1. Create a new interface role called **Device Policy**.
2. Set the **Device Policy** role on the selected interface on each device (for example, Loopback0).
3. Apply the desired device-level configuration policy to the device and on the Role property page of the Configuration Policy dialog, set the configuration policy interface role to **Device Policy**.

General Device-Level Configuration Policies

A number of general use configuration policies are provided with IP Service Activator that are applied at the device-level. These are organized into the **Policy Types > Service > General** hierarchy. These configuration policies place specific data on the device, or configure particular resources on the device that may be required for other services. They are not used to configure a modelled service by themselves.

See "Applying Configuration Policies at the Device Level" for details on applying configuration policies at the device level.

When you load the **GeneralPolicyTypes.policy** file, the general usage configuration polices loaded include the following:

- Banner
- IP Pools
- Key Chain
- Prefix List
- SNMP Community
- SNMP Host
- Static Route
- User Authentication
- User Data

The function of most of these configuration policies is self-evident from their name. The Banner configuration policy configures MOTD type banners on devices, and most of the other policies configure data in accordance with their name. For complete details on the fields included in each configuration policy, see its topic in IP Service Activator online Help.

User Authentication Configuration Policy

This configuration policy can be used to configure additional separate local user accounts on the device, rather than having to perform this task manually. Using the configuration policy has the advantage that the account data is maintained in IP Service Activator, rather than having to be configured and maintained manually.

see the appropriate cartridge guides to determine device support for this policy.

> **Note:**
>
> Within the IP Service Activator system, the password for accounts configured with the User Authentication configuration policy is not protected.

User Data Configuration Policy

This configuration policy is unique in that it is not intended to configure any service or configuration on the device and has no pre-defined purpose. The use of the User Data configuration policy is to provide a system-integrated method of attaching free form user data to objects which are modelled in IP Service Activator. The data is stored as name/value pairs, making it easier to process or manage this information outside IP Service Activator, through the OJDL API for example.

When you apply the User Data configuration policy to an object, it must be done in such a way that no concrete is generated. The network processor will generate errors if a concrete is created.

When you apply the configuration policy to a target, before you commit the transaction:

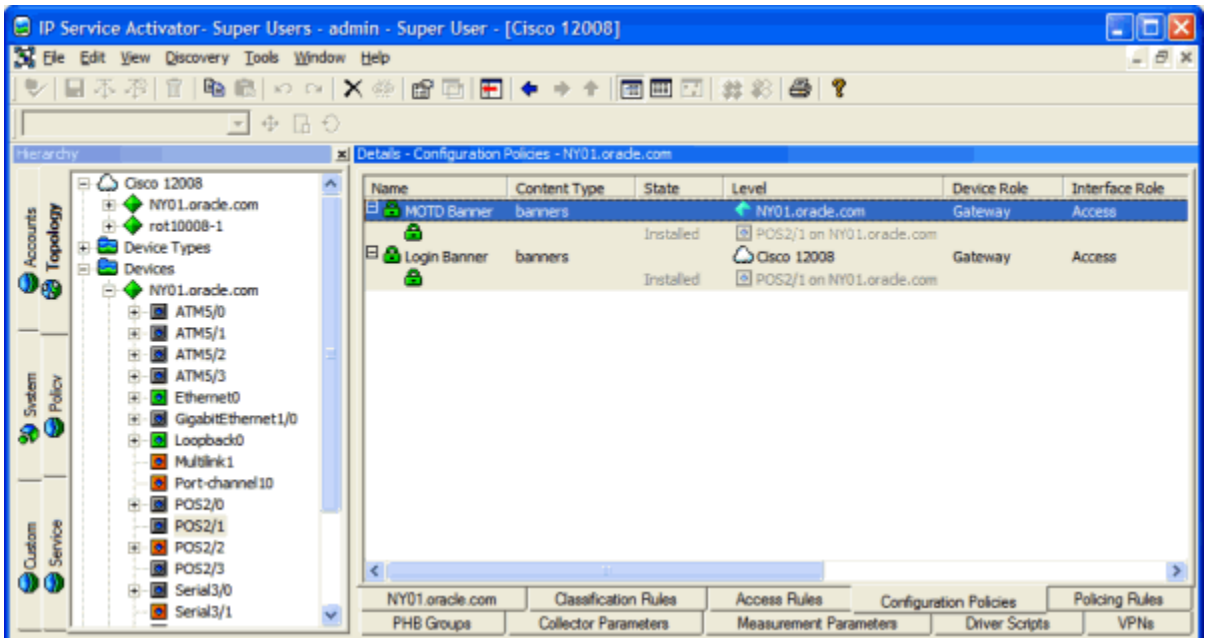
- Ensure that no roles are specified for the configuration policy.
- check the **Disable** check box in the **Rule Status** pane of the Configuration Policy property page of the Configuration Policy dialog box.

Using Collection-Based Configuration Policies

Some configuration policies such as Static Route and Banner allow for multiple definitions either within the same policy definition, or across multiple policy instances on the same device. This allows for the creation of groups of definitions that may be defined at different levels in the policy inheritance hierarchy.

For example, a general banner policy can be defined at the Network level with a common login and incoming banner definition that would apply to all devices, while a separate MOTD (message of the day) banner could be defined specifically at the device level. See Figure 5-1 for an example of banners.

Figure 5-1 Banner Example



Each collection based policy must contain at least one valid definition. If the last definition is removed, the policy must either be disabled or deleted from the device.

QoS and Attachment Configuration Policies

Included with IP Service Activator are a number of configuration policies to extend the QoS capabilities of IP Service Activator on various devices.

In cases where IP Service Activator does not support the exact QoS mechanism you need, or for whatever reason, you choose not to use IP Service Activator's QoS provisioning capabilities, you can use attachment configuration policies to attach the QoS configuration elements already configured your router to a service or interface within IP Service Activator.

For complete details on the fields and controls in specific configuration policies, see IP Service Activator online Help.

Vendor Cartridge Support for Various QoS Configuration Policies

For details on specific vendor support for this configuration policy, see the appropriate vendor-specific Cartridge guide.

Overview of Attachment QoS Policies

Attachment QoS policies allow you to use IP Service Activator to link existing QoS configuration elements pre-existing on devices with targets in the object model.

The qosCosAttachment configuration policy allows you to create references to existing QoS (quality of service) and/or CoS (class of service) policies on interfaces or PVCs on Cisco devices.

Overview of Vendor-Specific QoS Policies

The supplied vendor-specific QoS policies provide additional QoS capabilities on various vendors' equipment.

QoS Configuration Policies

Various configuration policies provide the ability to configure additional QoS elements on various platforms.

catOSPolicingRule: CatOS does not support MQC PHBs. This configuration policy enables policing-type QoS on these devices.

Installation of QoS and Attachment Configuration Policies

Configuration policies must be installed before they can be applied to target objects. Before using the complementary QoS configuration policies you must load the following **.policy** files:

- **CiscoCatOSQoSPolicyTypes.policy**
- **CiscoIOSQoSPolicyTypes.policy**
- **FoundryIronWareQoSPolicyTypes.policy**
- **ExtensionPackCPolicyTypes.policy**

For complete details on how to install configuration policies, see *IP Service Activator System Administrator's Guide*.

Role-based Inheritance

As with other configuration policies, IP Service Activator's role-based inheritance rules apply to QoS and attachment configuration policies. The inheritance model enables policy defined at a high level, such as the domain or network, to be inherited to lower level objects, such as devices and interfaces. Roles enable you to group devices and interfaces by, for example, customer and service package, and create policies targeted at that group. Policies can be directed towards specific groups of devices and interfaces.

For details on roles, see *IP Service Activator User's Guide*.

Attachment QoS Configuration Policies

Attachment QoS policies allow you to use IP Service Activator to link existing QoS configuration elements on devices with targets in the object model.

There may be cases where IP Service Activator does not support the QoS capabilities you want to implement. Or, you may prefer to define QoS configurations outside of IP Service Activator.

On new installations, there may be a significant investment in QoS configuration already on existing devices that you don't want to reproduce in the IP Service Activator object model.

In these cases, you can use IP Service Activator to apply QoS configurations defined on devices to interfaces on those devices through the use of an attachment configuration policy. One advantage of this approach is that IP Service Activator will not remove the QoS configuration from the device, even when it is unlinked from targets in the object model.

qosCosAttachment

This configuration policy allows you to create references to QoS (quality of service) and/or CoS (class of service) policies on interfaces or PVCs, primarily on Cisco devices.

The QoSCosAttachment configuration policy allows you to use predefined QoS policy on a device in a manner similar to a template and attach it to target interfaces. A single QoS definition can be attached to multiple interfaces. For example, if you provide the name of the policy map, IP Service Activator maintains the link between the interface and the defined policy map. In the interface, IP Service Activator issues configuration commands to link the policy map to the interface.

> **Note:**
>
> You can link both a QoS and a CoS with one instance of this configuration policy.

Vendor-Specific QoS Configuration Policies

This section describes vendor-specific configuration policies that extend the QoS capabilities of IP Service Activator.

Cisco QoS Configuration Policies

The following sections describe the possible Cisco QoS configuration policies.

CatOSPolicingRule

This configuration policy allows you to create a Layer 2 QoS aggregate policer with ACL configuration for IP, MAC and IPX traffic types on an Ethernet interface or VLAN. At least one classification must be declared as part of the policy definition. This configuration policy is supported for the Cisco CatOS cartridge only.

This policy is applied to interfaces and VLANs, with one policy per target. CatOS doesn't support MQC PHBs. This configuration policy enables policing-type QoS on these devices.

6

Implementing and Managing Per Hop Behavior Groups

This chapter describes how to implement and manage both standard and MQC Per Hop Behavior (PHB) groups in Oracle Communications IP Service Activator. This chapter:

- Describes how to set up and manage PHB groups
- Explains how to implement PHB groups and understand the information that IP Service Activator displays for implemented PHB groups

Implementing a PHB Group

This section discusses how to associate PHB groups with policy targets and how to commit transactions.

Associating a PHB Group with a Policy Target

If you set up a PHB group from the Policy tab, you can apply it to the appropriate points in the network by dragging and dropping. A PHB group can be applied to any policy target – that is, a network component, a customer, site or VPN. To apply a PHB group to a policy target:

- With the PHB group displayed in the hierarchy pane and the target object displayed in the Details pane, drag the PHB group onto the target object.

To remove a PHB group from a policy target:

1. Double-click on the policy target.

   IP Service Activator lists the configuration associated with the policy target in the details pane.

2. In the Details pane, select the **PHB Groups** tab and select the PHB group to be removed.

   PHB groups applied to the policy target are listed on a white background, PHB groups applied at a higher point in the hierarchy are listed on a gray background.

3. From the PHB group's pop-up menu, select **Unlink**.

Committing the Transaction

As you define PHB groups, they are added to the current transaction. Depending on your user access level, you may be able to commit the transaction immediately, or save it in a pending state for checking and committing by a supervisor. The policy implemented by a PHB group is not implemented until the transaction it forms part of is committed.

Checking Implemented PHB Groups

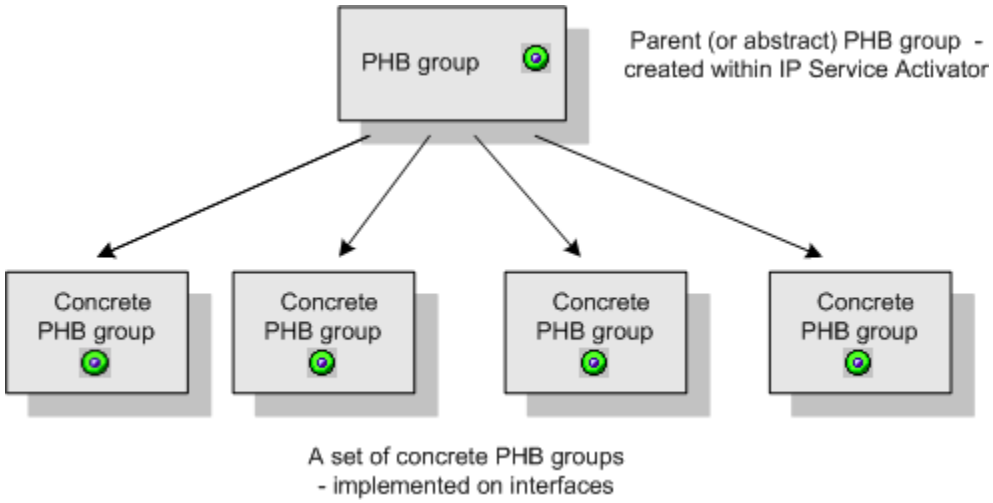
Once you have propagated PHB groups to devices throughout the network, you can check how and where PHB groups have been implemented.

Abstract and Concrete PHB Groups

A concrete PHB group is an implementation of a defined PHB group that applies to a specific point in the network, that is, at a particular interface, sub-interface or VC endpoint. Each abstract or parent PHB group set up can result in a number of concrete PHB groups. See Figure 6-1.

For more information on abstract and concrete policy elements, see *IP Service Activator Concepts*.

Figure 6-1 PHB Groups



PHB Group Status

A concrete PHB group may have the following status:

- Inactive – the PHB group has been applied to an interface but has not yet been propagated to proxy agents.
- Active – the PHB group has been propagated to a proxy agent but is not installed on a device at present.
- Conflict – the PHB group fails validation – for example, the action performed by a PHB group is not supported by an interface.
- Rejected – the proxy agent failed to install the PHB group and it has been discarded.
- Installed – the PHB group has been successfully installed on the designated device.

Viewing Implemented PHB Groups

Once you have created PHB groups you can check the points at which they apply.

To view the points at which a PHB group has been implemented:

- On the **Policy** tab, select the relevant PHB group and double-click the **Report View** button.

  The points at which the selected PHB group applies are listed in the Details pane.

Each abstract (parent) PHB group is followed by a list of the concrete PHB groups that have been created at appropriate interfaces. The background color of a PHB group indicates where it was created.

At any one time, a number of PHB groups may be listed for a network component, customer, site or VPN – particularly as PHB groups can be applied to various levels of both the logical and the physical hierarchy and applied via a process of inheritance. See "Policy Inheritance" for information on inheritance.

To view the PHB groups that apply to an object

1. On the **Topology** tab, double-click on the relevant policy target.
2. Select the **PHB Groups** tab in the Details pane.

The listed PHB groups may have originated at a higher point in the hierarchy. IP Service Activator uses color to indicate whether the PHB group is abstract or concrete. For more information on abstract and concrete policy elements, see *IP Service Activator User's Guide*.

Note that, in addition to viewing the concrete PHB groups that apply to a specific object, it is also possible to perform a system-wide search to locate concrete PHB groups by state.

If no concrete PHB groups are listed for an abstract PHB group, check the following:

- The correct device and interface roles have been associated with the PHB group and assigned to the relevant policy targets – see "Using Roles in Policy Elements".
- Devices to which the PHB group should apply are managed.

For more information, see *IP Service Activator User's Guide*.

> **Note:**
>
> IP Service Activator applies only one concrete PHB group to an interface. An abstract PHB group that has been applied at a lower level in the hierarchy overrides any PHB groups that have been applied at a higher level. A concrete standard PHB group that configures FRTS or ATM traffic shaping can be installed on an interface that has a concrete MQC PHB group whose mechanisms do not conflict with the standard PHB group.

Information Displayed About PHB Groups

Click on the **PHB groups** tab to view relevant PHB groups. Table 6-1 shows the PHB group details.

Table 6-1 PHB Group Information

Heading	Description
Name	Name of the PHB group.
State	Current status of the concrete PHB group.
Level	For abstract PHB groups, the level at which the PHB group was created (the name of the domain, VPN, site, device, interface or VC endpoint). For concrete PHB groups, the object on which the PHB group is installed.
Type	Either PHB Group or MQC PHB Group.
Device Role	Name of the matched device role to which the PHB group is applied.
Interface Role	Name of the matched interface role to which the PHB group is applied.
Direction	Direction of traffic affected by PHB group - Inbound, Outbound or Both.
WRR	True if Weighted Round Robin is applied, otherwise False.
WRED	True if Weighted Random Early Detection is applied, otherwise False.
PQ	True if Priority Queuing is applied, otherwise False.
WFQ	True if Weighted Fair Queuing is applied, otherwise False.
Rate Limiting	True if Rate Limiting is applied, otherwise False.
FRTS	True if Frame Relay Traffic Shaping is applied, otherwise False.
ATM Traffic Shaping	True if ATM Traffic Shaping is applied, otherwise False.
ID	The internal ID number by which the concrete PHB group is identified.

Changing the Evaluation Order of PHB Groups

The abstract and inherited PHB groups that apply to a policy target are listed in the following order:

- Abstract PHB groups – PHB groups applied at the object
- Inherited PHB groups – PHB groups that have been applied to an object at a higher level in the hierarchy and inherited to the lower-level object

Inherited PHB groups are further subdivided according to where the corresponding abstract PHB group was applied. For example, PHB groups inherited from devices are grouped together.

The order in which PHB groups are listed in the details pane is important – the first PHB group that appears in the list is applied. IP Service Activator applies only one concrete PHB group to any interface. Therefore, you need to ensure that PHB groups appear in the correct order.

The initial order reflects the order in which the PHB groups were created. You can change the order if required, by dragging and dropping PHB groups to a new position in the list.

7

Defining MQC PHB Groups

This chapter describes how to define Modular QoS CLI (MQC) policies for Cisco devices using MQC PHB groups in Oracle Communications IP Service Activator. This chapter:

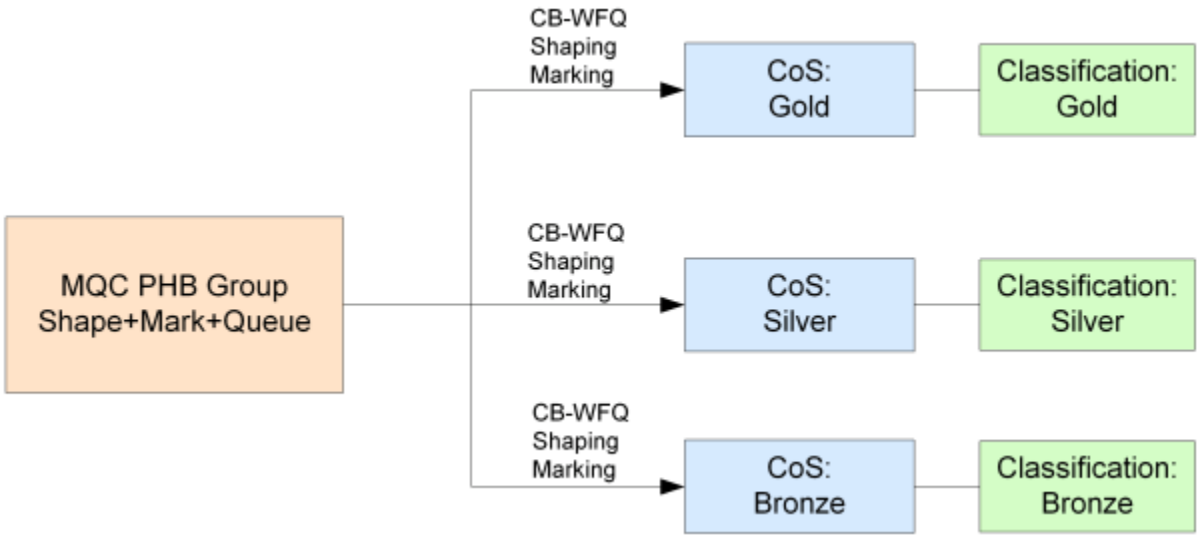
- Provides an overview of MQC PHB groups and the traffic management mechanisms that can be implemented using IP Service Activator.
- Highlights points you should consider before setting up MQC PHB groups.
- Describes how to set up and manage MQC PHB groups.
- Explains how to implement MQC PHB groups and understand the information that IP Service Activator displays for implemented MQC PHB groups.

> **Note:**
>
> See "Defining Standard Per Hop Behavior Groups " for information on defining standard PHB groups. See "Implementing and Managing Per Hop Behavior Groups " for details on implementing and managing PHB groups.

Introduction

MQC PHB groups allow you to implement Cisco's simplified configuration of policy mechanisms and actions for traffic queuing, shaping, policing, congestion avoidance and re-marking on the interfaces of Cisco routers and switches. You can specify several different QoS mechanisms for different classes of service associated with the same MQC PHB group. An MQC PHB group defines the QoS policy that may be used at various points in the network. For example, an MQC PHB group might be used to manage the traffic going into the core network or to maintain the prioritization set up at the network edge throughout the core network.An MQC PHB group may be applied to one or more classes of service that are based on a classification or classification group. The classification may be defined by factors such as source and/or destination IP address or account and traffic type. A number of classes of service may be linked to an MQC PHB group and one or more different mechanisms applied to each one. Figure 7-1 gives an example.

Figure 7-1 MQC PHB Groups



Within the MQC PHB group definition, you can specify the order in which packets are evaluated against each CoS's match criteria to ensure that packets have the correct mechanism applied to them.

See "Nesting MQC PHB Groups" for information about nesting MQC PHB groups.

An MQC PHB group is configured as a policy map and implemented at an interface as a service policy.

An MQC PHB group can be applied to a network component such as an interface or a VC endpoint, a customer, site or VPN.

Supported Traffic Management Mechanisms

The following traffic management mechanisms can be implemented within an MQC PHB group and applied to traffic by class of service:

- Low Latency Queuing (LLQ): Assigns a traffic class to a strict priority queue with a guaranteed maximum bandwidth during congestion.
- Class-based Weighted Fair Queuing (CB-WFQ): Assigns a traffic class to a queue with a priority based on a guaranteed minimum bandwidth during congestion.
- Class-based Policing: Specifies and enforces conditions that define the maximum inbound and outbound bandwidth of a traffic class, packets that exceed the conditions can be dropped or re-marked.
- Class-based Shaping: Specifies and constrains the maximum outbound bandwidth of a traffic class, outbound packets that exceed the conditions are delayed.
- Class-based Marking: Marks packets to allocate a priority status or class.
- Congestion avoidance (Queue limit and/or WRED): Defines how packets are discarded during congestion.

Before Setting Up an MQC PHB Group

This section outlines the points you need to consider before setting up an MQC PHB group.

Deciding Which QoS Actions to Select

The choice of which QoS action to use depends on the QoS policy you want to implement and the capabilities of the router. The available techniques are often specific to the device type, operating system and interface. You may find that some QoS mechanisms can only be implemented on some devices using standard PHB groups. We recommend you consult Cisco's documentation for your specific device. (MQC PHBs are specific to Cisco devices.)

IP Service Activator reports the capabilities of each interface and you should ensure that a QoS action is supported before attempting to configure it. For information on checking an interface's capabilities, see *IP Service Activator User's Guide*. For more information about supported capabilities, consult the router documentation.

Defining Classes of Service

Before creating an MQC PHB group, you need to ensure you have specified the classification parameters for identifying traffic by setting up classes of service. MQC PHB groups operate on one or more classes of service defined by a classification or classification group. See "Setting Up a Classification" for information on defining a classification or classification group. See "Setting Up Traffic Types" for information on defining traffic types.

> **Note:**
>
> You can associate a CoS defined by a classification or classification group and/or a packet marking with an MQC PHB group. However, the MQC PHB group only operates on the traffic defined by a classification or classification group – packet markings are ignored. If you wish to define a traffic class that is characterized by a packet marking, you must create a packet marking traffic type and associate it with a classification.

Check Capabilities

Before setting up MQC PHB groups, you need to know the capabilities of the policy targets to which you intend to apply policy. Check the Capabilities property page on relevant interfaces if necessary.

Deciding Where to Apply MQC PHB Groups

MQC PHB groups are implemented on the inbound and/or outbound interfaces of the routers to which they are applied. They are created as templates either within a domain or at device level. If created at the domain level, they are applied to various points throughout the network through inheritance so that they are applied to interfaces tagged with the appropriate role. However, an MQC PHB created at device level will apply only to that device's interfaces.

A system of inheritance applies – see "Policy Inheritance" for more information.

The higher the number of devices encompassed by the scope of the MQC PHB, the higher the computational load. It is recommended that you apply MQC PHBs at as close a level to the objects to which they apply. For example, if an MQC PHB is intended to apply to only one device, apply it at that device, rather than at the domain level. You can apply the same MQC PHB in more than one place as needed.

If an MQC PHB group applies to all devices and interfaces that share the same role it can be applied to the root level network and will automatically apply to all relevant interfaces throughout the network.

> **Note:**
>
> IP Service Activator applies only one concrete MQC PHB group to an interface. If you apply an MQC PHB group to the root level network, a concrete MQC PHB group is only created on an interface tagged with the appropriate role if there is no concrete MQC PHB group already installed on that interface. However, a concrete standard PHB group that configures FRTS or ATM traffic shaping can be installed on an interface that has a concrete MQC PHB group that is configured with other QoS mechanisms.

Using Roles in MQC PHB Groups

Every MQC PHB group must have a device and interface role associated with it. The roles you associate with an MQC PHB group specify to which policy targets the queuing mechanism will apply.

Depending on the roles that you assign to policy targets, it is possible to apply policy only at very specific points in the network. For example, you can apply a role to a sub-interface independent of its parent interface. By associating an MQC PHB group with the sub-interface role, you can apply a QoS policy only at the sub-interface.

See "Using Roles in Policy Elements" for information on using roles.

> **Note:**
>
> When you create an MQC PHB group there are no policy roles associated with it by default. You must associate both a device and an interface role for the MQC PHB group's configuration to be applied at the appropriate points in the network. If either the device or interface role are not specified, no configuration will be applied.

Setting Up an MQC PHB Group

You can set up and apply MQC PHB groups as two separate operations or as one combined operation just as you can with PHB groups.

See "Setup and Application of PHB and MQC PHB Groups as Separate Operations" and "Setup and Application of PHB and MQC PHB Groups as a Combined Single Operation" for more information.

To set up an MQC PHB group:

1. Do one of the following:
   - On the **Policy** tab, select the **MQC PHB Groups** folder.
   - Select a target object — a network component, customer, site or VPN.
2. Right-click on the folder or target object and select **Add MQC PHB Group** from the pop-up menu.

   The MQC PHB Group dialog box opens.

   Enter values including Name, Configured Name, Description, and Direction.
3. Select a CoS so that it is highlighted and its check box is checked.
4. Select one or several QoS actions that you want to associate with the selected CoS including **LLQ**, **Default WFQ**, **CB-WFQ**, **SR Police**, **TR Police**, **Shape**, **Mark**, **Congestion**, **Nest**, **RTP Compression**.

   > **Note:**
   >
   > See MQC PHB QoS Action Combinations in IP Service Activator online Help for a table indicating which combinations of QoS actions are allowed.

5. Repeat steps 4 to 6 for each CoS that you want to use.
6. Click the **Apply** button to apply the changes.

   To remove all QoS actions associated with a CoS, click on the CoS to clear its check box.
7. Select the Role property page and select the device and interface roles to which the MQC PHB group applies.

   > **Note:**
   >
   > You must specify both a device and an interface role. The system-defined Any Role can be used to apply the MQC PHB group to any device or interface tagged with a role. See "Using Roles in MQC PHB Groups" for more information.

8. Select the appropriate property page(s), depending on the QoS actions selected, and set the appropriate parameters. For details of configuring each QoS action, see the appropriate description:
   - Matching – "Specifying Evaluation Order"
   - LLQ –"Setting Up Low Latency Queuing"
   - CB-WFQ – "Setting Up Class-Based Weighted Fair Queuing"
   - Policing – "Setting Up Class-Based Policing"
   - Policing action – "Setting Up a Policing Action"
   - Shaping – "Setting Up Class-Based Shaping"
   - Marking – "Setting Up Class-Based Marking"
   - Congestion avoidance – "Setting Up Congestion Avoidance"

- Nesting – "Nesting MQC PHB Groups"
- RTP compression – "RTP Header Compression"

9. Click **OK**.

Specifying Evaluation Order

The classes of service that are associated with an MQC PHB group are listed on the MQC PHB group's Classify property page. The order in which these appear is significant. The order can be changed using the controls in the MQC Order pane.

The position of a CoS in the list can affect which QoS actions are applied to a packet.

Packets are evaluated against the classes of service listed in the MQC Order pane in sequence. When a packet matches a class of service, the appropriate QoS actions are applied and no further matching is performed.

For example, Bronze and Gold classes of service may include the same destination address in their match criteria but have different QoS actions applied to them. They are listed in the order shown above. If both CoS's match criteria is Match Any, a packet with the relevant destination address will be matched against the Bronze CoS and no further evaluations made. The packet therefore only has the QoS actions applied to it that have been defined for the Bronze CoS, and is never evaluated against the Gold CoS.

> **Note:**
>
> The match criteria for a CoS is defined by the classification or classification group that is linked to the CoS. See "Setting Up a Classification" for information on defining a classification or classification group.

To specify match order:

1. Select the Classify property page in the MQC PHB Group dialog box.

   All classes of service that you selected on the PHB Group page are listed in the MQC Order list.

2. If required, change the position of a CoS in the MQC Order list by selecting a CoS and clicking the up or down arrows to move it up or down the list.
3. Save your settings by clicking **Apply**.

Re-ordering classes within IP Service Activator policies sends the correct configuration to the router, but some Cisco IOSs do not show the correct order on subsequent 'show run' commands. The router does not return any errors. There is no indication that the configuration has not been accepted by the router.

For problematic IOSs, the best work-around is to unlink the entire policy map, re-order the classes and then re-link the policy map. This will ensure that the correct ordering is applied to the router.

The following IOSs have been tested:

Table 7-1 Class Re-Order Tests

IOS Version	Class re-order successful on router
12.3(3)	Yes
12.2(19c)	No
12.2(15)T10	Yes
12.2(12i)	No
12.2(8)T	No
12.3(11)T	No

Setting Up Low Latency Queuing

You use Low Latency Queuing (LLQ) to assign a strict priority to a CoS to allow delay-sensitive traffic to be given priority over less delay-sensitive traffic during congestion.

The operation of LLQ is identical to Class-Based Weighted Fair Queuing (CB-WFQ) except that LLQ has a strict priority queue.

You allocate a guaranteed bandwidth - a proportion of the output interface bandwidth - to one or more classes of service. When congestion occurs, each traffic flow is placed in its own queue. If there is only one flow of a particular CoS, it will be allocated all of the user-specified bandwidth for that CoS. If there are several flows of the same CoS, each flow queue is allocated an equal proportion of the user-specified bandwidth for that CoS. For example, if a CoS is allocated 60% of the output interface bandwidth, and there are three flows of the same CoS, each flow queue is allocated 20% of the output interface bandwidth.

During congestion, each queue is serviced in turn by a scheduling mechanism that forwards a number of bits from each packet in proportion to the queue's allocated bandwidth. For example, if there are two CoS queues allocated bandwidth of 40% and 20%, each time a queue is serviced, twice as many bits are taken from a packet in the CoS queue allocated 40% bandwidth than bits taken from a packet in the CoS queue allocated 20% bandwidth.

If a CoS is not using its allocated bandwidth, the unused bandwidth is shared by the other classes of service.

During congestion, packets belonging to a CoS that is assigned LLQ are always allowed to be transmitted before packets of a CoS that is assigned CB-WFQ. However, any incoming packets of a traffic class assigned LLQ that exceed the allocated bandwidth will be dropped.

Multi-Level Priority Queuing

This allows you to configure multiple priority queues for multiple traffic classes by specifying a different priority level for each of the traffic classes in a single service policy map. You can configure multiple service policy maps per router. Having multiple priority queues enables the router to place delay-sensitive traffic, for example, voice traffic, on the outbound link, before delay-insensitive traffic. As a result, high priority traffic receives the lowest latency possible on the router.

In the MQCPHB Group object, LLQ bandwidth type holds a value for representing priority levels. The actual weight attribute of the MQCPHB holds the value of “level" (valid range of 1 to 4; 1 being the highest priority and 4 being the lowest priority) when the bandwidth type is set to “level".

Restrictions and conditions for using multi-level priority queues:

- The bandwidth and priority level commands cannot be used in the same class, within the same policy map. These commands can be used in the same policy map, however.
- The shape and priority level commands cannot be used in the same class, within the same policy map. These commands can be used in the same policy map.
- Within a policy map, you can give one or more classes priority status. The router associates a single priority queue with all of the traffic enabled with the same priority level and services the high level priority queues until empty before servicing the next level priority queues and non-priority queues.
- You cannot specify the same priority level for two different classes in the same policy map.
- You cannot specify the priority command and the priority level command for two different classes in the same policy map. For example, you cannot specify the priority bandwidth-kbps or priority percent percentage command and the priority level command for different classes.
- When the priority level command is configured with a specific level of priority service, the queue-limit and random-detect commands can be used if only a single class at that level of priority is configured.
- You cannot configure the default queue as a priority queue at any priority level.
- To convert a single-level (flat) service policy with multiple priority queuing configured to a hierarchical multi-level priority queuing service policy, you must first detach the flat service policy from the interface using the no service-policy command, and then add a child policy map to it.

For complete dialog box and property page descriptions, see IP Service Activator online Help.

To set up LLQ:

1. Select the Queue property page in the MQC PHB Group dialog box.

   The classes of service that you selected with LLQ on the PHB Group page appear in the QoS Queue area.
2. Select a CoS and set the following parameters.
3. Select or clear the check box Maximum reserved bandwidth to enable/or disable this capability. If enabled specify a new value if required. Cisco devices have a default maximum reserve bandwidth value of 75 percent that is designed to leave sufficient bandwidth for overhead traffic. You can alter this by entering a percentage value.
4. Select a bandwidth option from the **Interpret LLQ Weight as** list (**Absolute Bandwidth**, **Percentage of Bandwidth**, **Percentage of Remaining**, **Default**, **Level**).
5. Specify the **Queue Weight or Level** value.

   If you are changing the settings of several classes of service in the MQC PHB group, use the **Modify** button to apply the changes to each CoS.
6. Specify a value in **LLQ burst** in bytes. Select **Device default** to specify the default value for that particular device.
7. Specify the **Fair-queue** values to configure fair-queuing.

8. Select the next CoS in the list and repeat this procedure.
9. Save your settings by clicking **Apply**.

Setting Up Class-Based Weighted Fair Queuing

Use Class-Based Weighted Fair Queuing to assign a priority to a CoS based on bandwidth.

You allocate a minimum bandwidth - a proportion of the output interface bandwidth - to one or more classes of service. When congestion occurs, each traffic flow is placed in its own queue. If there is only one flow of a particular CoS, it will be allocated all of the user-specified bandwidth for that CoS. If there are several flows of the same CoS, each flow queue is allocated an equal proportion of the user-specified bandwidth for that CoS. For example, if a CoS is allocated 60% of the output interface bandwidth, and there are three flows of the same CoS, each flow queue is allocated 20% of the output interface bandwidth.

During congestion, each queue is serviced in turn by a scheduling mechanism that forwards a number of bits from each packet in proportion to the queue's allocated bandwidth. For example, if there are two CoS queues allocated bandwidth of 40% and 20%, each time a queue is serviced, twice as many bits are taken from a packet in the CoS queue allocated 40% bandwidth than bits taken from a packet in the CoS queue allocated 20% bandwidth.

If a CoS is not using its allocated bandwidth, the unused bandwidth is shared by the other classes of service.

The operation of CB-WFQ configured using MQC PHB and standard PHB groups is identical.

For complete dialog box and property page descriptions, see IP Service Activator online Help.

To set up CB-WFQ:

1. Select the Queue property page in the MQC PHB Group dialog box.

   The classes of service that you selected with CBWFQ on the PHB Group property page appear in the **QoS Queue** area.
2. Select a CoS and set the required parameters.
3. Select a bandwidth option from the **Interpret CBWFQ Weight as:** list (**Absolute Bandwidth**, **Percentage of Bandwidth**, **Percentage of Remaining**).
4. Specify the **Queue Weight** value.

   If you are changing the settings of several classes of service in the MQC PHB group, use the modify button to apply the changes to each CoS.
5. Specify the **Fair-queue** values to configure fair-queuing.
6. Select the next CoS in the list and repeat steps 3 to 4.
7. Save your settings by clicking **Apply**.

Setting Up Class-Based Policing

You can use class-based policing to specify and enforce the maximum bandwidth allocated to a specified traffic class transmitted from or received by an interface. Bandwidth is enforced by either dropping or re-marking packets that exceed and/or violate their user-specified conditions. Packets are dropped less aggressively by allowing packets that occasionally exceed the committed information rate as bursts to be transmitted if those burst sizes are within the user-specified conditions.

You specify the maximum rate and burst size(s) that define the conditions to which a packet is required to conform. These values represent the policing profile of the CoS and are specified on the Police property page.

For single rate policing, a conform condition indicates that a packet stream's information rate is within the specified Committed Information Rate (CIR). An exceed condition indicates that a packet stream's information rate is above the specified CIR. A violate condition indicates that a packet stream's burst size is above the specified Committed Burst Size (CBS) and Excess Burst Size (EBS).

For two-rate policing, a conform condition indicates that a packet stream's information rate is within the specified CIR and Peak Information Rate (PIR). An exceed condition indicates that a packet stream's information rate is within the specified PIR but above the specified CIR. A violate condition indicates that a packet stream's PIR is above the specified PIR.

The two-rate (three-color marker) policer improves bandwidth management by allowing you to police traffic streams according to two separate rates. Unlike the single-rate policer, which allows you to manage bandwidth by setting the excess burst size (be), the two-rate policer allows management of bandwidth by setting the Committed Information Rate (CIR) and the Peak Information Rate (PIR). The three-color marker distinguishes between the nonconforming traffic that occasionally bursts a certain number of bytes more than the CIR and violating traffic that continually violates the PIR allowance. Applications can use the three-color marker to provide three service levels: guaranteed, best effort, and deny. The three-color marker is useful in marking packets in a packet stream with different, decreasing levels of assurances (either absolute or relative).

You can specify the actions performed on packets that conform, exceed or violate specified conditions on the Police Action property page.

The following steps are required to configure class-based policing using an MQC PHB group:

1. Set up a policing profile for a CoS on the Police property page of an MQC PHB Group dialog box.
2. Set up policing actions for conform, exceed and violate conditions on the Policing Action property page of a PHB Policing Action dialog box.
3. Associate policing actions with a CoS on the Police Action property page of the MQC PHB Group dialog box.

> **Note:**
>
> Policing actions can be set up before setting up policing profiles.

For complete dialog box and property page descriptions, see IP Service Activator online Help.

Single rate class-based policing measures bandwidth conformance of traffic based on its Committed Information Rate, Committed Burst Size and Excess Burst Size.

To set up single rate class-based policing:

1. Select the Police property page in the MQC PHB Group dialog box.

The classes of service that you selected with SR Police on the PHB Group property page appear in the **QoS Policing** area.

2. Select a CoS so that it is highlighted.
3. Specify values fields including **CIR**, **CBS**, and **EBS**.
   - **Rate Type**: Selects the policing type. If Absolute is chosen, the additional controls express rates in absolute terms. If Percent is chosen, CIR express a rate in terms of the percentage of available bandwidth. CBS and EBS are expressed in milliseconds (ms) with a valid range of 1 to 2000.
   - **CIR**:
     - **Absolute-based**: Committed Information Rate in bits/s. Range is 8000 (8 kbits/s) to 4000000 (i.e. 8 kbits/s - 4000 Mbits/s). Default is 8000.
     - **Percentage-based**: CIR as a percentage of the interface's bandwidth. Default is 1. Range is 1 to 100%.
   - **CBS**:
     - **Absolute-based**: Committed Burst Size in bytes. Range 1 kbytes to 512 Mbytes. Default is 1 kbyte.
     - **Percentage-based**: Committed Burst Size expressed in ms.
     - **Default**: When selected, IP Service Activator defers to the device to set the actual value used for CBS. This can vary from device to device. Also, disables the EBS fields.

     When cleared, you can specify a value for CBS.
   - **EBS**:
     - **Absolute-based**: For Single Rate policing only, Excess Burst Size in bytes. Range is 1 kbyte to 512 Mbytes, the default is 1 kbyte.
     - **Percentage-based**: Excess Burst Size expressed in ms.
     - **Default**: When selected, IP Service Activator defers to the device to set the actual value used for EBS. This can vary from device to device. When cleared, you can specify a value for EBS.

   The following options, when added by the user, provide the default value in the case that the **Default** check box is checked. For complete details on options, see *IP Service Activator Cisco IOS Cartridge Guide*.
   - Percent:

     ```
     cartridge.cisco.qos.policymap.police.percent.defaultCBSValue(Default -1)
     cartridge.cisco.qos.policymap.police.percent.defaultEBSValue  (Default -1)
     ```
   - Absolute:

     ```
     cartridge.cisco.qos.policymap.police.defaultCBSValue (Default -1)
     cartridge.cisco.qos.policymap.police.defaultEBSValue (Default -1)
     ```
4. Aggregate policer name: Select to activate aggregate policing and specify the aggregate policer name in the text box.

   If you are changing the settings of several classes of service in the MQC PHB group, use the modify button to apply the changes to each CoS.
5. Select the next CoS in the list and repeat step 3.
6. Save your settings by clicking **Apply**.

Two rate class-based policing measures bandwidth conformance of traffic based on its Committed Information Rate, Committed Burst Size, Peak Information Rate and Peak Burst Size.

To set up two rate class-based policing:

1. Select the Police property page in the MQC PHB Group dialog box.

   The classes of service that you selected with TR Police on the PHB Group property page appear in the **QoS Policing** area.
2. Select a CoS so that it is highlighted.
3. Specify values including: **CIR**, **CBS**, **PIR** and **PBS**.
   - **Rate Type**: Selects the policing type. If Absolute is chosen, the additional controls express rates in absolute terms. If Percent is chosen, CIR and PIR express a rate in terms of the percentage of available bandwidth. CBS and EBS are expressed in milliseconds (ms) with a valid range of 1 to 2000. The PIR value must be equal to or larger than the CIR value.
   - **CIR**:
     - **Absolute-based**: Committed Information Rate in bits/s. Range is 8000 (8 kbits/s) to 4000000 (i.e. 8 kbits/s - 4000 Mbits/s). Default is 8000.
     - **Percentage-based**: CIR as a percentage of the interface's bandwidth. Default is 1. Range is 1 to 100%.
   - **CBS**:
     - **Absolute-based**: Committed Burst Size in bytes. Range 1 kbytes to 512 Mbytes. Default is 1 kbyte.
     - **Percentage-based**: Committed Burst Size expressed in ms.

     When cleared, you can specify a value for CBS.
   - **PIR**: For Two Rate policing only. Absolute-based: Peak Information Rate in bits/s, in the range 8 kbits/s to 4000 Mbits/s. Default is 8 kbits/sec.
   - **PBS**: For Two Rate policing only. Peak Burst Size in bytes, in the range 1 kbyte to 512 Mbytes. Default is 1 kbyte.

   If you are changing the settings of several classes of service in the MQC PHB Group, use the modify button to apply the changes to each CoS.

   The following command syntax options (singleLine/MultiLine/PercentageSyntax) are available for the police command and the desired syntax can be generated by setting the appropriate options. For complete details on options, see IP Service Activator Cisco IOS Cartridge Guide.

   ```
   cartridge.cisco.qos.policymap.police.conformAction.isSupported
   cartridge.cisco.qos.policymap.police.exceedAction.isSupported
   cartridge.cisco.qos.policymap.police.violateAction.isSupported
   ```
4. Select the next CoS in the list and repeat step 3.
5. Save your settings by clicking **Apply**.

Setting Up a Policing Action

You can specify the treatment of packets that conform to, or exceed the rate value(s), or violate the burst sizes that are specified for a CoS on the Police property page. You can specify a separate action for each of these three states. For example, you can

specify that packets that conform are transmitted, packets that exceed are re-marked and transmitted, and packets that violate are dropped. The re-marked values on the packets determine how they are treated by QoS mechanisms set up on interfaces downstream. An action can implement several types of marking.

A policing action is defined by setting up a PHB Policing Action object which can then be specified as either the conform, exceed or violate action for a CoS on the Police Action property page of the MQC PHB dialog box. You can either use default PHB policing actions or specify your own. A PHB Policing Action can be used by several MQC PHB groups.

For complete dialog box and property page descriptions, see IP Service Activator online Help.

To set up a PHB policing action:

1. On the **Policy** tab, select the **PHB Policing Action** folder.
2. Right-click and select **Add PHB Policing Action** from the pop-up menu.
3. The PHB Policing Action dialog box opens.
4. Enter a **Name** for the PHB Policing Action.
5. Select either **Drop** or **Transmit**.
6. If you select **Transmit**, specify how you want packets to be marked by selecting an action including **Set ATM CLP**, **Set FR DE**, **Set IP Marking**, and **Set MPLS Exp**. If you do not select a marking, then no marking changes are applied to the packet by the PHB Policing Action. Any original packet markings remain intact.
7. Save your settings by clicking **Apply**.

Applying a Policing Action

Apply a PHB policing action by associating it with an MQC PHB group.

To associate a policing action with an MQC PHB group:

1. Select the Police Action property page in the MQC PHB Group dialog box.

   The classes of service that you selected with SR Police or TR Police on the PHB Group property page appear in the **MQC Policing Action** area.
2. Select a CoS and set the required parameters.
3. Specify values for **Conform Action** and **Exceed Action**.

   Default **Conform Action** transmits packets without re-marking. Default **Exceed Action** drops packets.
4. Specify a **Violate Action**, or **None**.

   Default **Violate Action** drops packets. If **None** is selected for two rate policing, the default value for **Exceed Action** will be used.

   If you are changing the settings of several classes of service in the MQC PHB group, use the modify button to apply the changes to each CoS.
5. Select the next CoS in the list and repeat steps 3 to 4.
6. Save your settings by clicking **Apply**.

   Your selections for each CoS appear in the **MQC Policing Action** area.

Setting Up Class-Based Shaping

You use class-based shaping to constrain a traffic class to the committed information rate (CIR) and to delay outbound packets that exceed the CIR by placing them in a queue.

Class-based shaping allows you to configure the following:

- Average rate traffic shaping: Limits the traffic rate to the CIR (on non-Frame Relay interfaces only).
- Peak rate traffic shaping: Allows traffic rate bursts above the CIR if extra network bandwidth is available, packets may be dropped if network congestion occurs (on non-Frame Relay interfaces only).
- Adaptive generic traffic shaping for Frame Relay: Uses the Backward Explicit Network Congestion Notification (BECN) to estimate the available bandwidth and adjust the transmission rate accordingly. BECN signals may also be reflected as Forward Explicit network Congestion Notifications (FECN).
- CB-WFQ inside GTS: Places a packet that exceeds the shape parameters in a queue whose priority is based on bandwidth allocated to the CoS to which the packet belongs. CB-WFQ is configured on the Queue property page.

For complete dialog box and property page descriptions, see IP Service Activator online Help. For detailed information related to traffic shaping support, see *IP Service Activator Cisco IOS Cartridge Guide*.

Average or peak rate traffic shaping can be configured on non-Frame Relay interfaces only.

To set up average or peak rate traffic shaping:

1. Select the Shape property page on the MQC PHB Group dialog box.

   The classes of service that you selected with Shape on the PHB Group property page appear in the **MQC Shaping** area.
2. Select a CoS from the MQC Shaping area and set the required parameters.
3. Select either **Shape Average** or **Shape Peak**.
4. Specify values including **CIR**, **Bc**, and **Be**.

   If you are changing the settings of several classes of service in the MQC PHB group, use the Modify button to apply the changes to each CoS.
5. Select the next CoS in the list and repeat steps 3 to 4.
6. Specify **Number of buffers**. Select **Device default** to specify the default value for that particular device.
7. Save your settings by clicking **Apply**.

In addition to average or peak rate shaping, you can configure BECN and/or FECN adaptive shaping on Frame Relay interfaces.

To set up adaptive generic traffic shaping:

1. Select the Shape property page on the MQC PHB Group dialog box.

   The classes of service that you selected with Shape on the PHB Group property page appear in the MQC Shaping area.

2. Deselect **Default Shaping** and select either **Shape Average** or **Shape Peak**.
3. Specify values including **CIR**, **Bc**, and **Be**.
4. Specify **Number of buffers**. Select **Device default** to specify the default value for that particular device.
5. Select the **FR Extension** check box.
6. Select **BECN Adapt** and/or **FECN Adapt**.
7. Enter a minimum value for CIR in the **Min CIR** field.
8. Select the **BECN Adapt** check box if you want to monitor for Frame Relay frames that have the BECN bit set.

   Select the **FECN Adapt** check box if you want to monitor for Frame Relay frames that have the FECN bit set.

   If you are changing the settings of several classes of service in the MQC PHB group, use the **Modify** button to apply the changes to each CoS.
9. For each CoS to which you wish to apply adaptive generic traffic shaping, repeat steps 2 to 8.

   Your selections for each CoS appear in the **MQC Shaping** area.
10. Save your settings by clicking **Apply**.

Class-based shaping can be used in conjunction with CB-WFQ. This allows a packet that exceeds the shape parameters to be placed in a queue whose priority and bandwidth allocation is defined by the packet's CoS.

To set up CB-WFQ within Generic Traffic Shaping (GTS):

1. In the MQC PHB Group dialog box, select the PHB Group property page.
2. Select a CoS to which you want to apply CB-WFQ within GTS.
3. Select **CBWFQ** and **Shape**.
4. Repeat steps 2 and 3 for each CoS to which you want to apply CB-WFQ within GTS.
5. Select the Queue page.
6. For each CoS, set up CB-WFQ as described in "Setting Up Class-Based Weighted Fair Queuing".
7. Select the Shape property page.
8. For each CoS, set up GTS as described in "Setting Up Class-Based Shaping".

You can apply basic traffic shaping to Cisco 10000 devices, based on the CIR value only.

To set up basic traffic shaping:

1. Select the Shape property page on the MQC PHB Group dialog box.

   The classes of service that you selected with Shape on the PHB Group property page appear in the **MQC Shaping** area.
2. Select a CoS and select **Default Shaping** and specify a value in the **CIR** field.
3. Select the next CoS in the list and repeat step 2.
4. Save your settings by clicking **Apply**.

Setting Up Class-Based Marking

You can use class-based marking to mark packets so that they belong to a particular traffic class which can affect how the packets will be managed by QoS policies at other interfaces in the traffic path.

To set up class-based marking:

1. Select the Mark property page in the MQC PHB Group dialog box.

   The classes of service that you selected with Mark on the PHB Group property page appear in the **MQC Mark** area.
2. Select a CoS.
3. Select marking types including **Set IP Marking**, **MPLS Exp.**, **Set FR DE**, **Set ATM CLP**, **Discard Class**, **Set Trust Type**, **COS**, **COS Inner**, and **QoS Group**.

   If you are changing the settings of several classes of service in the MQC PHB group, use the **Modify** button to apply the changes to each CoS.
4. Select the next CoS in the list and repeat step 3.
5. Save your settings by clicking **Apply**.

Setting Up Congestion Avoidance

Use congestion avoidance to specify how packets are discarded when congestion occurs. During congestion, packets are queued according to their CoS. For each CoS you can specify:

- Queue limit – the maximum number of packets allowed in the queue

  and/or:
- WRED – Weighted Random Early Detection

Queue limit allows you to specify the maximum number of packets allowed in the queue. If the number of packets reaches the maximum number defined, any additional packets are dropped.

WRED is a congestion avoidance mechanism that drops packets at a specified threshold based on a calculated queue size. You set up WRED parameters on the WRED properties property page in a standard PHB group.

Before you can apply queue limit and/or WRED to a CoS, it must be identified with WRED-compliant packet marking and one of the following:

- Bandwidth allocated on the CBWFQ property page
- Bit rate specified on the Shape property page

The default CoS does not need to be assigned CB-WFQ or Shape actions, and can be classified with either WRED-compliant packet marking or source/destination IP address or protocol.

A queue limit can be applied to the default class of service for devices that support this. However, at least one class in the policy map must have a queuing feature, when a queue-limit is applied to the default class of service.

For complete dialog box and property page descriptions, see IP Service Activator online Help.

To set up congestion avoidance:

1. Select the Congestion property page in the MQC PHB Group dialog box.

   The classes of service that you selected with Congestion on the PHB Group property page appear in the **MQC Congestion** area.
2. Select a CoS.
3. To specify a Queue Limit, select either **Default** or **Value**.
4. From the **WRED Strategy** list select one of **None**, D**evice Default**, or ***Name of a standard PHB group***.
5. If you want to define drop thresholds and probability, select the **WRED Drop Profile** check box and enter the following:
   - **Min threshold** number
   - **Max threshold** number
   - **Drop probability** number
6. If you are changing the settings of several classes of service in the MQC PHB group, use the **Modify** button to apply the changes to each CoS.
7. Select the next CoS in the list and repeat steps 3 to 4.
8. Save your settings by clicking **Apply**.

Nesting MQC PHB Groups

One MQC PHB group may be nested inside another MQC PHB group. This provides a method of applying a policy to a broad range of traffic, defined by the parent MQC PHB group, and another to a subset of that range, defined by the child MQC PHB group. For example, a single shaping policy may be applied to all traffic on an interface by a parent MQC PHB group, while the child applies a queuing policy to one or more classes of service. The resulting configuration is referred to by Cisco as a **hierarchical service policy**.

Multiple levels of nesting of MQC PHB groups are allowed.

A child MQC PHB group may be nested for a CoS to which Policing, Shaping, CB- WFQ or LLQ is applied. The method for nesting MQC PHB groups is:

1. Create the child MQC PHB group.

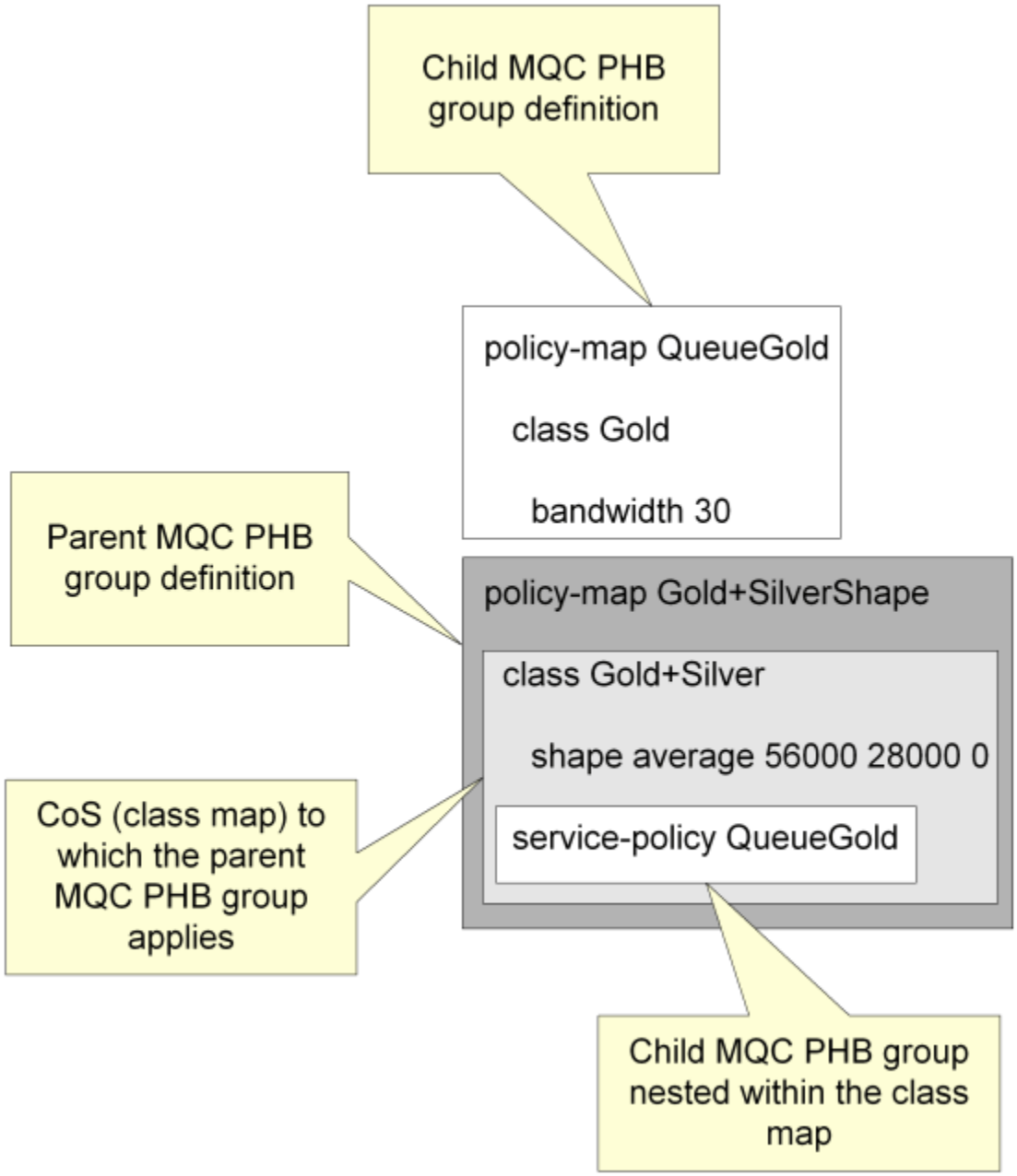
   The child MQC PHB group defines Policing, Shaping or CB-WFQ parameters for a subset of traffic handled by an interface – for example, Gold traffic.
2. Create the parent MQC PHB group.

   The parent MQC PHB group defines Policing, Shaping or CB-WFQ parameters for a broader range of traffic handled by an interface – for example, Gold and Silver traffic – and specifies a child MQC PHB group to nest for each CoS.

At command level, an MQC PHB group is configured as a policy map, and a class of service is configured as a class map. Nesting places a policy map (a child MQC PHB group) within a class map (CoS) that is part of another policy map (a parent MQC PHB group).

This is illustrated in Figure 7-2.

Figure 7-2 Nested MQC PHB



To nest MQC PHB groups:

1. Select the **Nest** tab.

   The classes of service that you selected with **Nest** and any combination of **Shape**, **SR/TR Police** or **CBWFQ** on the PHB Group property page appear in the **MQC Nesting** area.

2. Select a CoS in the **MQC Nesting** area of the parent MQC PHB group.
3. Select the child MQC PHB group from the **Nest** drop down combo box.

4. If you are nesting several MQC PHB groups, click the **modify** button to apply each selection.

   The name of the child MQC PHB group appears in the **Nest** column next to the selected CoS in the **MQC Nesting** area to indicate that the child policy map is nested within the selected class map.

5. Save your settings by clicking **Apply**.

RTP Header Compression

RTP (Real-Time Protocol) and RTCP (Real-Time Control Protocol) header compression is supported on out-going Frame Relay traffic on a per-Class-of-Service basis. It is used on relatively low-speed Frame Relay links to improve latency for Voice-over-IP traffic. For each Class of Service you can specify one nesting.

RTP Header Compression reduces the overhead on each voice packet that traverses the network. The near-constant nature of RTP and RTCP header content permits only the differences to be transmitted.

This feature is enabled in the IP Service Activator GUI by selecting the **RTP Compression** check box on the MQC PHB Group dialog box while the desired CoS is currently selected in the dialog box.

8
Example Policy Setups

This chapter provides some examples that illustrate Oracle Communications IP Service Activator's ability to apply policy at any point in the network and at any network component. This chapter:

- Demonstrates how to target policy to points in the network using roles.
- Shows how to apply policy to a VC endpoint.
- Illustrates the use of classifications and classification groups in rules.

Using Roles to Apply Policy

This example looks at QoS requirements across the core network and examines IP Service Activator's solution at one point in the network.

Requirements

The requirements are as follows:

- Provide two service packages, Premium and Basic
- Support a range of customers
- Ensure that bandwidth restrictions are applied to incoming and outgoing customer traffic
- Maintain traffic flow in the core network

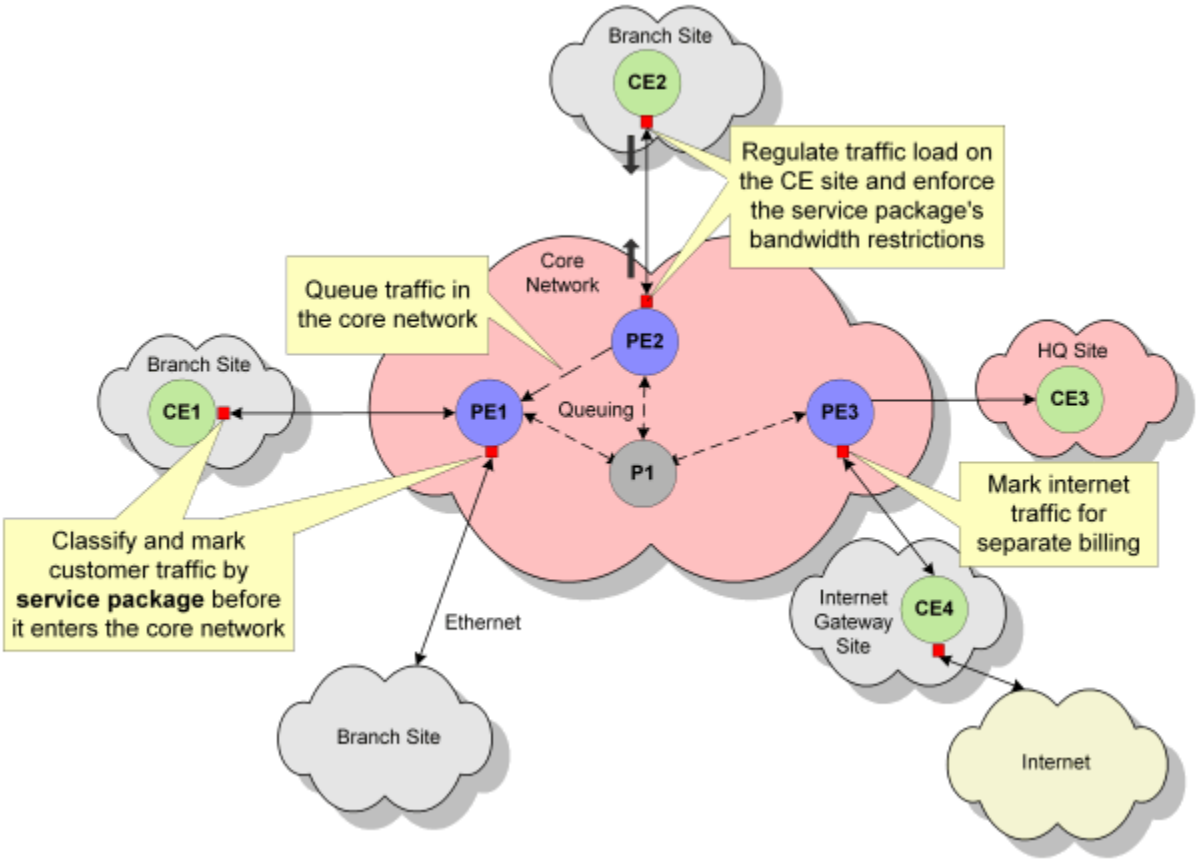
In both the Premium and the Basic service packages there are three classes of service – Gold, Silver and Bronze. The bandwidth percentage allocated to each CoS differs between service package:

- Premium traffic receives 30% Gold, 30% Silver, 40% Bronze
- Basic traffic receives 10% Gold, 40% Silver, 50% Bronze

Traffic entering the core network must be restricted to a bandwidth limit agreed on a per-customer basis. Links coming into the core differ in their bandwidth capacity.

These requirements are illustrated in Figure 8-1.

Figure 8-1 Policy Network Requirements



Solution

From the requirements, it is possible to identify three variables that affect policy:

- Service package
- Bandwidth capacity of the link
- Customer

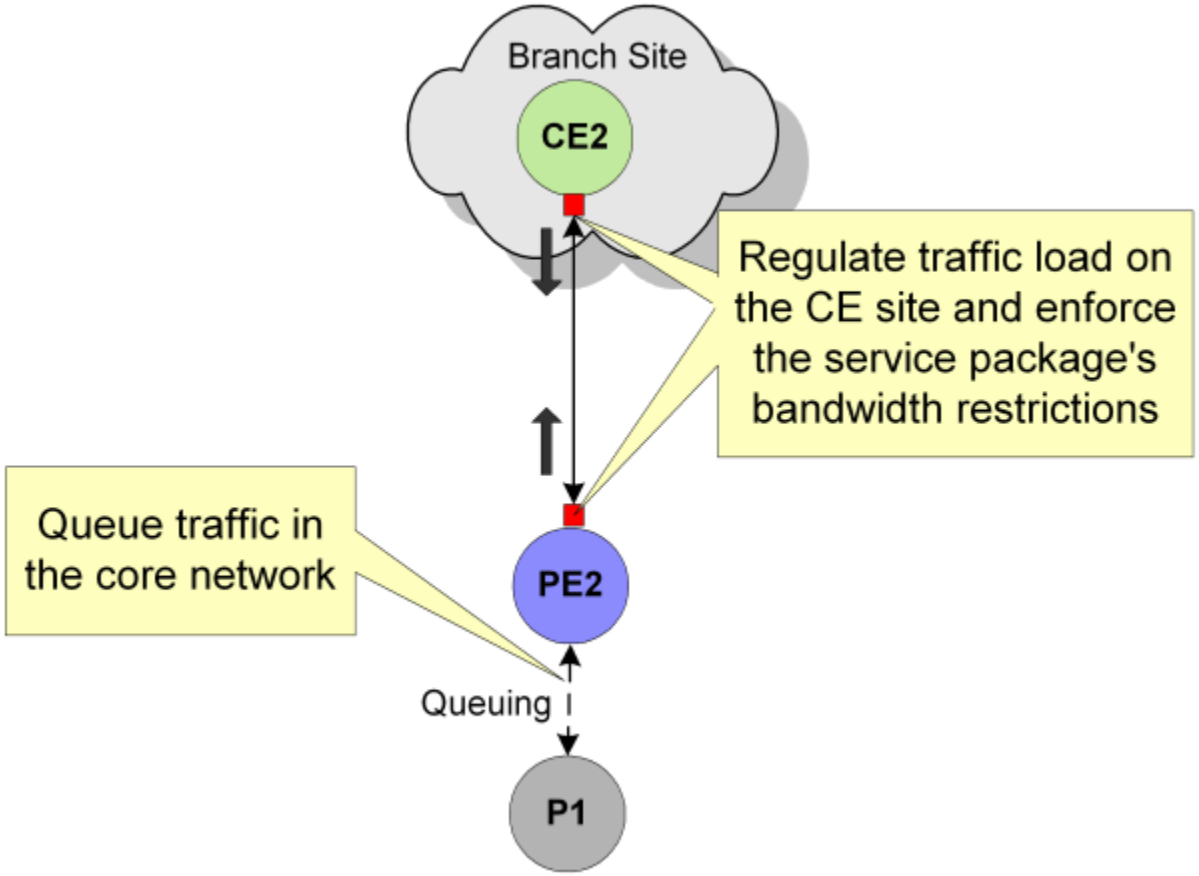
These variables dictate the roles that must be created to target policy to the appropriate points in the network. Ideally, three sets of roles would be created to support these variables. However, IP Service Activator allows a maximum of one system and/or one user-defined role to be assigned to a policy element (though you can assign one system and any number of user-defined roles to a policy target). In the roles we create, therefore, service package and bandwidth will be combined into a single role.

The roles to be defined are:

- One role per service package/link size combination
- One role per customer

The following solution, shown in Figure 8-2, focuses on a subsection of the network.

Figure 8-2 Policy Network Subsection

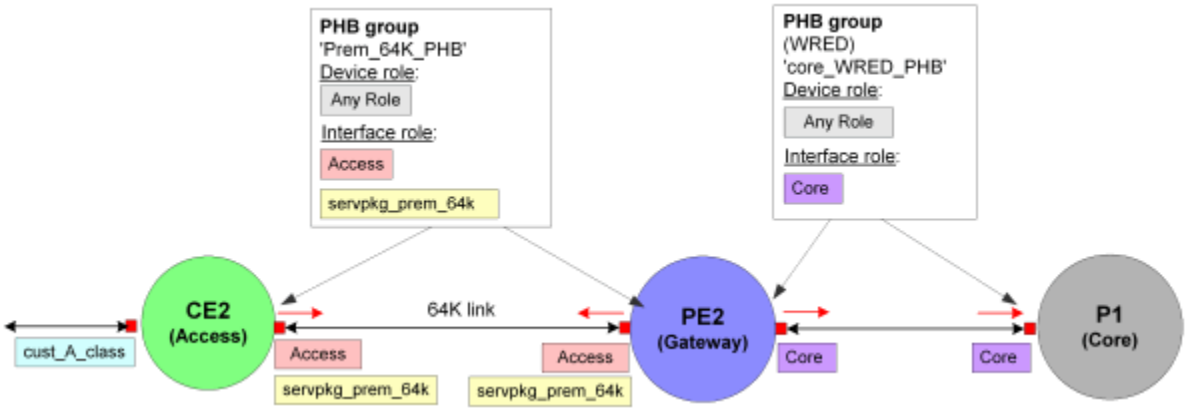


The tasks to be performed at each device can be defined as follows:

- CE2:
  - Classify customer traffic before it enters the core network
  - Police outbound traffic to enforce bandwidth restrictions, per CoS
  - Apply Class-Based-WFQ (CB-WFQ) queuing mechanism to regulate traffic flow
- PE2:
  - Police PE-CE traffic
  - Apply CB-WFQ queuing mechanism
- P1:
  - Apply WRED queuing mechanism

After creating the appropriate roles, rules and PHB groups and applying them to the network, the roles and policy applied to CE2, PE2 and P1 are illustrated in Figure 8-3.

Figure 8-3 Rule and Role Example



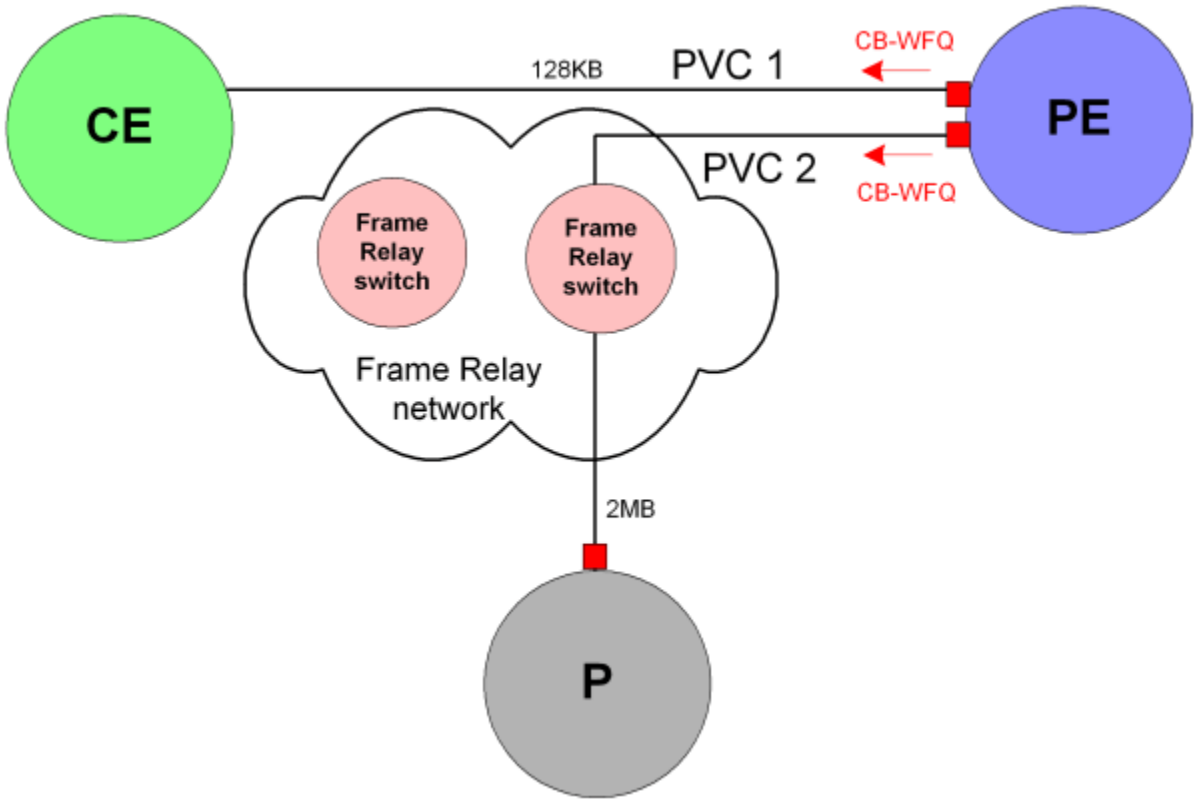
Applying Policy to a VC Endpoint

One of the advantages of IP Service Activator's role-based application of policy is the ability to assign roles to any network component, including sub-interfaces and VC endpoints. This enables you to apply policy to a sub-interface or VC endpoint independent of its parent interface.

In this example, two VC endpoints on the same device are connected to two Permanent Virtual Circuits (PVC) that have different bandwidth capacity. CB-WFQ must be applied to both PVCs, with bandwidth weight defined in Kbits/s.

Figure 8-4 presents a physical representation of the relevant network section.

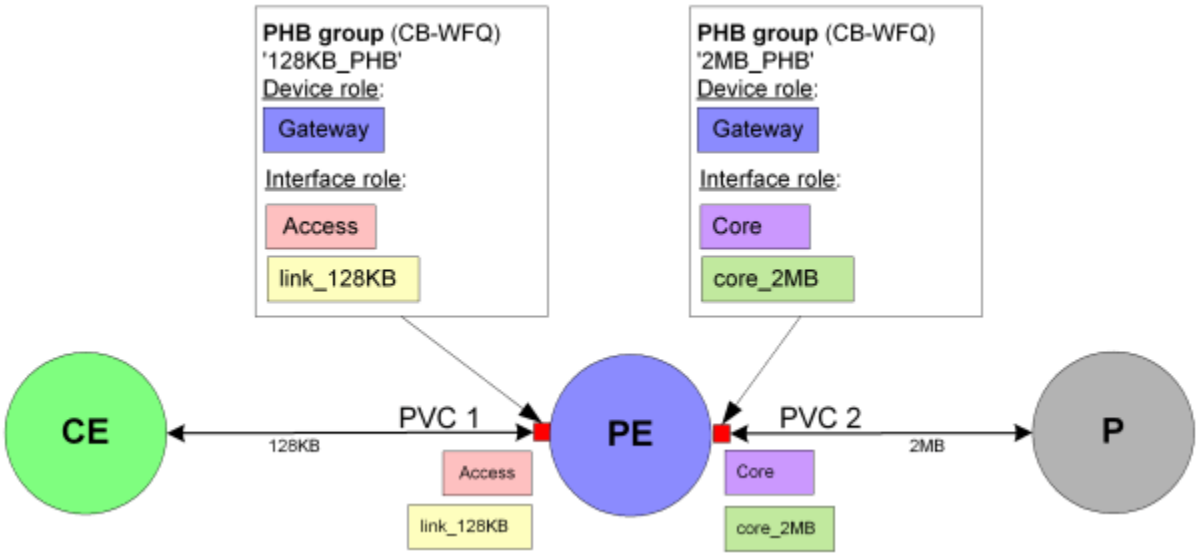
Figure 8-4 Network With Policy Applied at VC Endpoint



To take account of each PVC's bandwidth capacity, two PHB groups must be created and each PHB group targeted at the correct VC endpoint. This can be achieved by assigning a different role to each VC endpoint and associating the relevant role with the correct PHB group.

Figure 8-5 shows the logical network setup, with PHB groups defined and targeted at the appropriate VC endpoint using roles:

Figure 8-5 Logical Network Setup



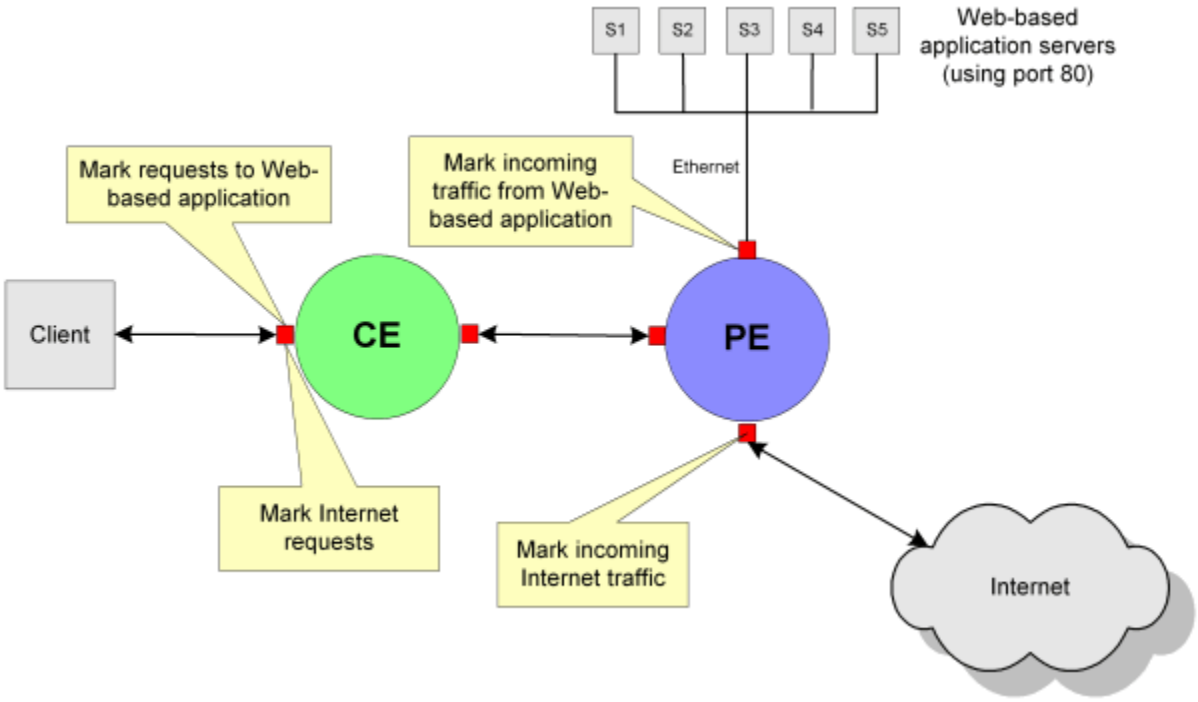
Using Classifications in Rules

A classification provides a means of categorizing traffic according to its source and destination and traffic type. You can create standalone classifications and/or group a number of classifications to form a classification group. Members of a classification group do not need to share the same source and destination point or traffic type. Classifications and/or classification groups can be associated with a rule to define the traffic to which it applies.

In this example a set of Web-based application servers supply information to employees. Employees also have Internet access. The requirement is to apply a different CoS treatment to traffic to and from the application servers and the Internet.

The network setup is shown in Figure 8-6.

Figure 8-6 Network Setup



> **Note:**
>
> Traffic originating from both the Web-based application servers and the Internet has source port number 80.

The example solution uses a classification group and a standalone classification within the classification rules that mark traffic from these sources:

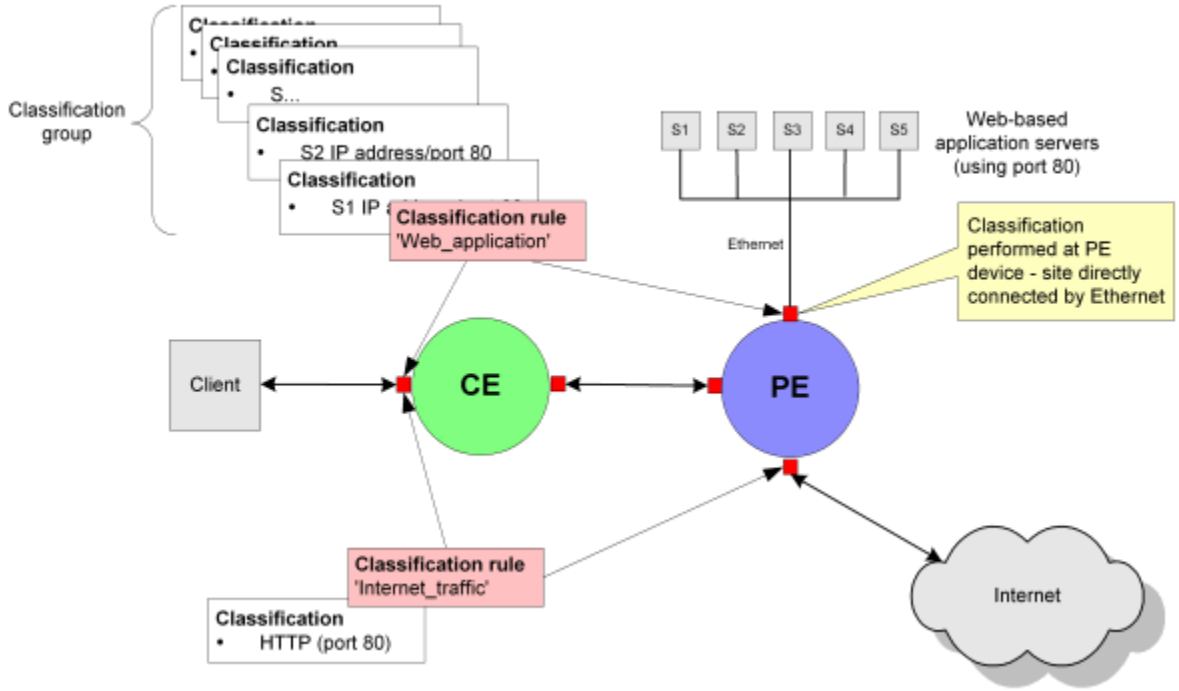
- A classification group holds five classifications that categorize traffic by IP address and port number.
- A standalone classification categorizes traffic by port number only.

The following classification rules are created:

- Web_application: Marks traffic from the Web-based application servers. This rule is associated with the classification group.
- Internet_traffic: Marks traffic by port 80 only. This rule is associated with the standalone classification.

The solution is shown in Figure 8-7.

Figure 8-7 Solution



At the CE device, rules must be applied in the following order:

- Web_application
- Internet_traffic

Rule order is significant at this point as the interface handles both Web-based application traffic and Internet traffic. Therefore, the most specific rule must be applied first (classifying by both IP address and port number) before the more general rule (port number only). If the rules are applied in the incorrect order, both Web-based application traffic and Internet traffic will be classified by the Internet_traffic rule as both use port 80.