CHAPTER 10

Layer 3 QoS

The Layer 3 QoS chapter contains the following information:

- CAR and WRED Overview
- The Workflow for CAR
- CAR Policies
- Access Lists
- CAR Policy Apply
- CAR Status
- The Workflow for WRED/DRR
- CoS Queue Group Configuration
- WRED Tx Configuration

CAR and WRED Overview

Committed Access Rate (CAR)

CAR is a policing mechanism that allows you to partition your network into multiple priority levels or classes of service. You set the IP precedence for packets entering the network. Networking devices within your network can then use the adjusted IP precedence to determine how to treat the traffic. CAR services limit the input or output transmission rate on an interface or subinterface based on a flexible set of criteria. CAR is often configured on interfaces at the edge of a network to limit traffic into or out of the network. CAR can rate limit traffic based on certain matching criteria, such as incoming interface, IP precedence, or IP access list. You configure the actions CAR will take when traffic conforms to or exceeds the rate limit. Each interface can have multiple CAR policies, corresponding to different types of traffic. For example, low priority traffic can be limited to a lower rate than high priority traffic.

Weighted Random Early Detection (WRED)

WRED is a congestion avoidance mechanism that takes advantage of TCPs (Transmission Control Protocol) congestion control mechanism. WRED drops packets selectively, prior to periods of high congestion, based on IP precedence. Packets with a higher IP precedence are less likely to be dropped than packets with a lower precedence. WRED is normally used in the core routers of a network, rather than on the edge. Edge routers assign IP precedences to packets as they enter the network. WRED uses these precedents to determine how it treats different types of traffic. All WRED processing takes place on the line card, rather than on the GRP management card. No default configuration values are supplied. You must provide values for all configurable fields. WRED also incorporates Modified Deficit Round Robin (mDRR).

You can see from the descriptions where these two mechanisms differ. CAR focuses more on classifying traffic according to QoS parameters, while WRED functions to ease network traffic and prioritize specified traffic.

MDRR Overview

Modified Deficit round Robin (MDRR) is a traffic latency control function. It allows the operators to guarantee traffic latency for differentiated flows by controlling the packet de-queuing process. Packet classification is based on IP Precedence. MDRR differs from DRR in that one of the eight available queues is designated as a low-latency queue.

There are two basic modes of operation which govern how packets arede-queued from the low-latency queue in relation to other queues. They are:

- Alternate Priority - queues are serviced by alternating between the low-latency queue & the other queues in round-robin.
- Strict Priority - low-latency queue is continually serviced to keep it empty.

MDRR in CGM

The GSR MDRR implementation uses COS Queue Groups to encapsulate the required profile. Consequently, CGM provides MDRR support via COS Queue Groups: the operator creates a COS Queue Group & uses the MDRR configuration Window to encapsulate the required parameters. The COS Queue Group is then available to be applied to any interface.

Implications of Engine Type

In CGM 2.0, there was no provision for the different engine types available on GSR line cards. Put simply, the engine type refers to different hardware architectures. From a management perspective, the engine type determines what functionality is available to the client. Currently, this only applies to Layer 3 QoS. The following is a summary of how engine type affects Layer 3 QoS:

- CAR: Supported for Engine 0, 1, and 4
- PIRC: Supported for Engine 2 (refer to “PIRC Support” section on page 10-4 for further details.)
- WRED: Supported for Engine 0, 2, and 4 (refer to “Engine Type Support for WRED” section on page 10-19 for further details.)

CGM will detect the engine type applicable to a given module (line card) and prevent operations that are not applicable.

CAR and WRED in CGM

CAR and WRED are modeled as objects in CGM. There are two types of CAR objects: CAR policies and access lists. There is one type of WRED object: CoS (Class of Service) queue groups.

When you create these objects in CGM, you can work within the Layer 3 QoS view to create, apply, delete or edit Layer 3 QoS objects. Created CAR policies are placed under the CAR Policies container in the Layer 3 QoS view. Created access lists are placed under the Access List container in the Layer 3 QoS view. Created CoS queue groups are placed under the WRED-MDRR container in the Layer 3 QoS view.

Tips Access lists are only supported within the realm of CAR and do not function as stand-alone objects.

It is important to note that Layer 3 QoS CAR and WRED objects (access lists, policies, CoS queue groups) are global, meaning they can be applied to any interface object within CGM.

The Workflow for CAR

To begin working with CAR objects, proceed as follows:

Step 1 Create and configure a CAR policy.

Step 2 Create and configure an access list (optional).

Step 3 Apply the access list to a CAR policy. Only one access list can currently be applied to a CAR policy.

Step 4 Apply the created CAR policy or access list to one or multiple interfaces. Up to twenty CAR policies can be applied to any amount of interfaces at a time.

At any given time, you also have the option to edit or delete CAR policies, change the association of CAR policies, or view the status of CAR policies on any interface.

CAR Policies

CAR policies can rate limit traffic based on certain matching criteria, such as incoming interface, IP Precedence, or IP access list. You configure the actions CAR will take when traffic conforms to or exceeds the rate limit. You can set CAR rate policies that are associated with one of the following:

- All IP traffic
- IP precedence
- MAC address
- IP access list, both standard and extended. Matching to IP access lists is more processor-intensive than matching based on other criteria.

Each interface can have multiple CAR policies, corresponding to different types of traffic. For example, low priority traffic can be limited to a lower rate than high priority traffic. With multiple rate policies, the router examines each policy in the order entered until the packet matches. If a match is not found, the default action is to transmit.

The rate policies can be independent; each rate policy deals with a different type of traffic. Alternatively, rate policies can be cascading; a packet can be compared to multiple different rate policies in succession. You can configure up to 20 rate policies on a subinterface.

The CAR Policies section covers the following areas:

- Creating a CAR Policy
- Applying an Access List to a CAR Policy
- CAR Policy Configuration Window—Detailed Description

PIRC Support

From the operator's perspective, the same workflows used for CAR will be available for the creation, application and maintenance of PIRC Policies. Specifically, the following functions are applicable to PIRC:

- Incoming only (Rx direction)
- Only one rule is allowed in a PIRC statement
- Available conform-actions are:
  - drop
  - set-prec-transmit
  - transmit
- No access-group, dscp, or qos-group matching is available; a PIRC rule matches *all* traffic inbound on that interface
- Only available exceed-actions are:
  - drop (drop packet)
  - set-prec-transmit (rewrite packet precedence and send it)
  - transmit (transmit packet)

If an attempt is made to apply a CAR policy to an engine 2 module, then the request will be refused and an appropriate error message issued to the client if an attempt is made to use CAR functionality outwith that listed above.

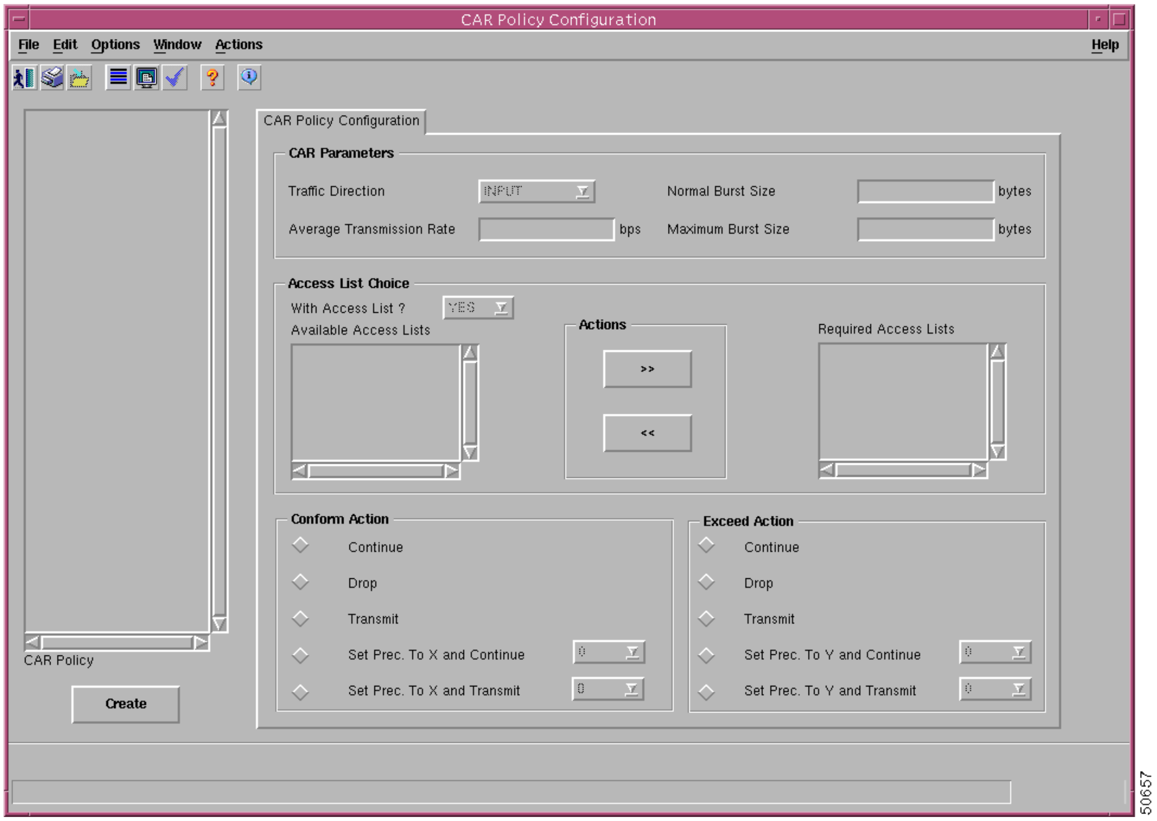
On engine 0, 1 and 4 modules, the full range of CAR functions is supported.

Creating a CAR Policy

To create a CAR policy, proceed as follows:

Step 1 In the Layer 3 QoS view, right-click on CAR Policies, then choose **CGM Management>Logical> Layer 3 QoS>CAR>Policy Configuration**. The CAR Policy Configuration window appears.

Figure 10-1 CAR Policy Configuration Window



Traffic Direction INPUT

With Access List ? YES

Step 2 Click **Create**.

Step 3 Enter a name for the CAR policy you are about to create, then click **Ok**.

A window appears, confirming if you were successful or not. The name of your new profile appears in the list box at left.

Step 4 Modify the configuration fields, as desired (see below for a detailed description of the fields within this window.)

Step 5 Click **Save** to save the changes.

Applying an Access List to a CAR Policy

Step 1 You can apply an access list to a selected CAR policy if desired (to create an access list, refer to “Access Lists.”) To apply an access list, proceed as follows:

Step 2 Select Yes in the Access List Choice area, next to With Access List?

Step 3 Available access lists appear at left. Select the access list you want to apply.

Step 4 In the Actions area, click on the right facing arrow to move the selected access list into the Required Access List.

Step 5 Click **Save** to save the changes.

CAR Policy Configuration Window—Detailed Description

The CAR Policy Configuration window has one tab, CAR Policy Configuration, with four areas:

- CAR Parameters
- Access List Choice
- Conform Action
- Exceed Action

CAR Parameters

The CAR Parameters area contains the following fields:

Traffic Direction—Choose either incoming (input) or outgoing (output) traffic.

Average Transmission Rate—Normal transmission rate based on a long term average in Mbps.

Normal Burst Size (in bytes)—Bytes allowed in a burst before some packets will exceed the rate limit. Larger bursts are more likely to exceed the rate limit.

Maximum Burst Size (in bytes)—Bytes allowed in a burst before all packets will exceed the rate limit.

Access List Choice

The Access List Choice area contains the following fields:

With Access List?—Choose yes to apply a selected access list to the selected CAR policy; choose No if you do not want to apply an access list to the selected CAR policy.

Available Access List—Pane that lists all created access lists.

Actions—Contains two arrow buttons to move access lists between the available access list and the required access list.

Required Access List—Pane that lists all access lists, which are required to be associated with the selected CAR policy.

Conform Action

The Conform Action area contains the following fields:

Continue—Evaluate the next rate-limit command.

Drop—Choose to drop the packet or not.

Transmit—Choose to transmit the packet or not.

Set Prec. To X and Continue—(numbers 0-7) Set precendence to an integer and continue.

Set Prec. To X and Transmit—(numbers 0-7) Set precendence to an integer and transmit.

Exceed Action

The Exceed Action area contains the following fields:

Continue—Evaluate the next rate-limit command.

Drop—Choose to drop the packet or not.

Transmit—Choose to transmit the packet or not.

Set Prec. To Y and Continue—(numbers 0-7) Set precendence to an integer and continue.

Set Prec To Y and Transmit—(numbers 0-7) Set precendence to an integer and transmit.

Access Lists

Access lists are supplemental to CAR policies. They enhance the abilities of a CAR policy. For example, access lists allow you to specify certain types of traffic, or certain locations where the traffic is coming from, etc. They allow you further specificity when creating your CAR policies.

The Access List section covers the following areas:

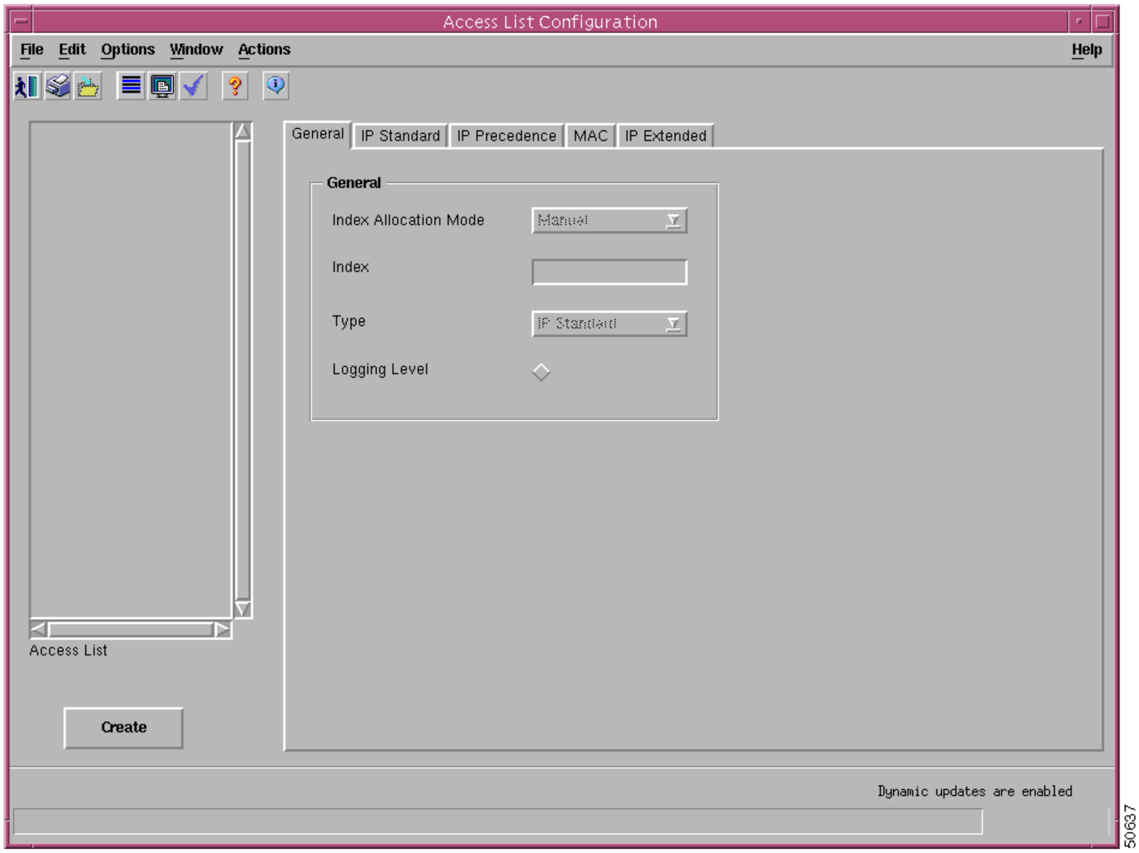
- Creating Access Lists
- Access List Configuration Window—Detailed Description

Creating Access Lists

To create an access list, proceed as follows:

Step 1 In the Layer 3 QoS view, right-click on Access List, then choose **CGM Management>Logical> Layer 3 QoS>CAR>Access List Configuration.** The Access List Configuration window appears, with the General tab displayed.

Figure 10-2 Access List Configuration—General Tab



General

Index Allocation Mode: Manual

Index:

Type: IP Standard

Logging Level: ◇

Step 2 Click **Create**.

Step 3 Enter a name for the access list you are about to create, then click **Ok**.

A window appears, confirming if you were successful or not. The name of your new access list appears in the list box at left.

Step 4 In the General tab, select the type of access list you want to create. You can also enable logging level at this time (for details, refer to the section below.)

Step 5 Modify the configuration fields in the respective tab, as desired (for a detailed description of the fields within this window, see below.)

Step 6 Click **Save** to save the changes.

Step 7 To apply an access list to a CAR policy, refer to "Applying an Access List to a CAR Policy" section on page 10-5.

Access List Configuration Window—Detailed Description

The Access List Configuration window contains one button, **Create**. The **Create** button is used to create an access list. When you click **Create**, a new access list of type IP standard is created and the next available index is assigned. The access list type can be changed and saved if desired. When the access list type is changed, the index is automatically reallocated to the next available index for the new type selected.

The Access List Configuration window contains five tabs:

- General
- IP Standard
- IP Precendence
- MAC
- IP Extended

Note that the General tab is always accessible. The corresponding tab, based on the access list type, is also accessible. Any non-relevant tabs are grayed out. The fields in all the tabs are populated with default values. The fields can be changed as desired.

General Tab

The General tab contains one area: Action.

Action

The Action area contains three fields:

Index—Identification number for an access list that is automatically generated by CGM.

Type—Lists the type of access list. Possible types include:

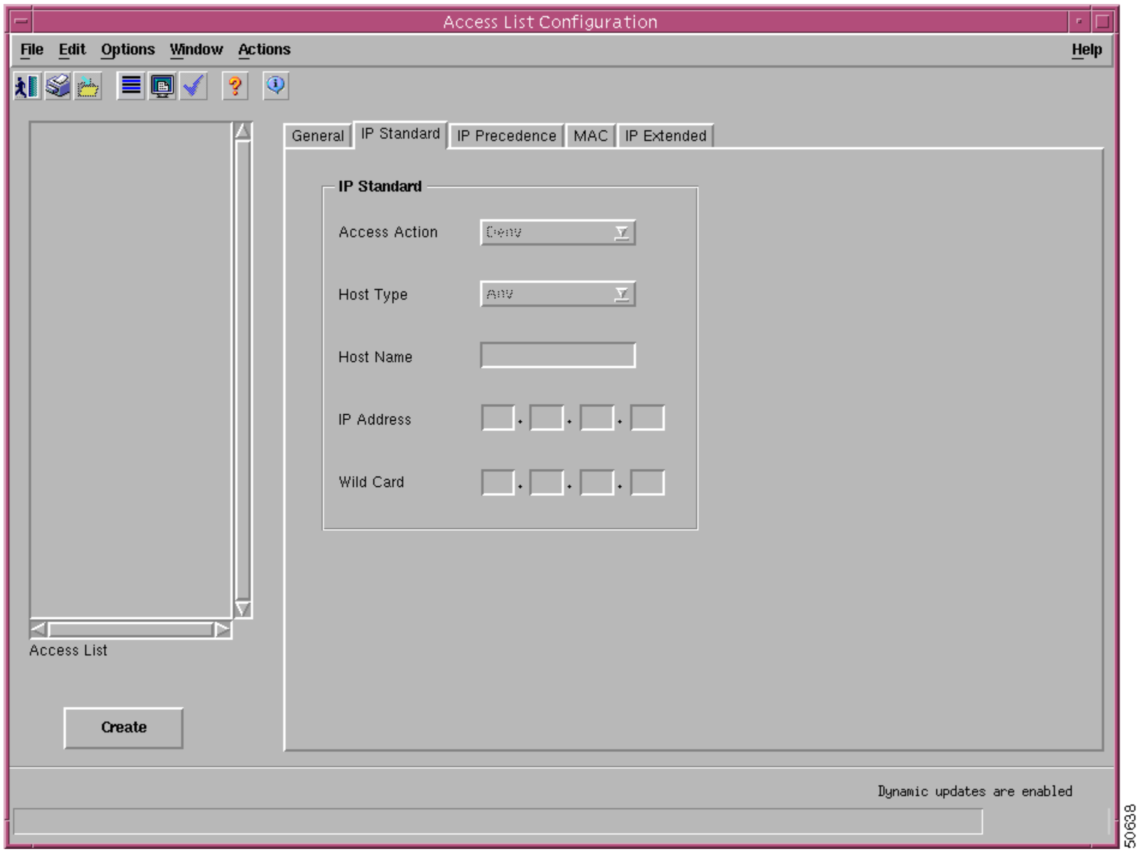
- IP Standard
- IP Precedence
- MAC
- IP Extended

Logging Level—(This field is only applicable to IP standard and IP extended access lists.) If you enable the logging level, then informational messages about the packet that matched the criteria specified in the access list will be generated.

IP Standard Tab

The IP Standard tab appears as follows:

Figure 10-3 Access List Configuration—IP Standard Tab



Access Action Deny

Host Type Any

Host Name

IP Address . . .

Wild Card . . .

Dynamic updates are enabled

The IP Standard tab contains one area: IP Standard.

IP Standard

The IP Standard area contains five fields:

Access Action—Action to be taken if the conditions are matched. This value will be either deny or permit.

Host Type—Host type indicates the hosts for which the access action are available. Possible values for this field include the following:

- Any—All hosts
- Host Name—Specified host name with wild card bits
- A.B.C.D—Specified IP address with wild card bits
- Host Hostname—Only the specified hostname
- Host A.B.C.D—Only the specified IP address

Host Name—Name of the host (or source of the packet) for which the access action is applicable.

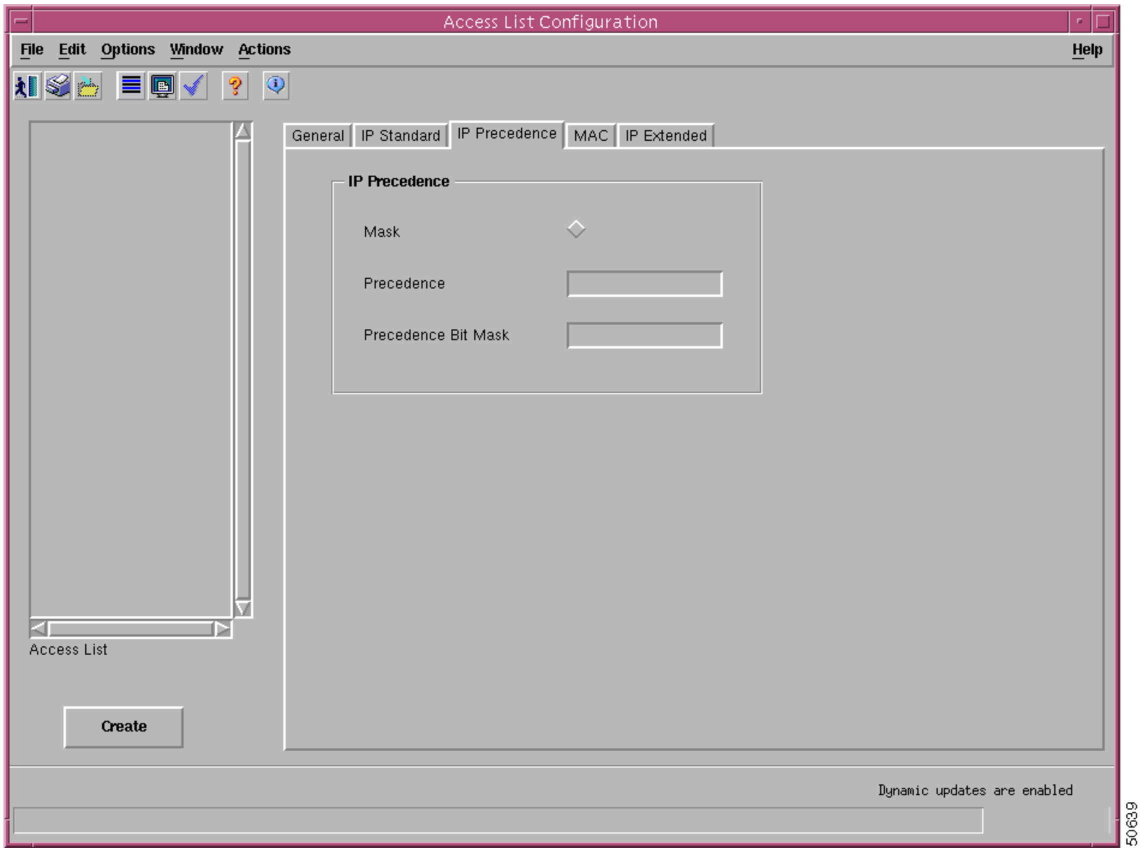
IP Address—IP address of the host (or source of the packet) for which the access action is applicable.

Wild Card—If the access action is applicable for more than one host, then this field should be used as a mask. For example, the wild card 255.255.255.255 effectively represents any.

IP Precedence Tab

The IP Precendence tab appears as follows:

Figure 10-4 Access List Configuration—IP Precedence Tab



The IP Precedence tab contains one area: IP Precedence.

IP Precedence

The IP Precedence area contains three fields:

Mask—If more than one precendence comes into the same classification, mask should be used for classification. Enabling mask enables the precedence bit mask field and disabling mask enables the precedence field to be enabled.

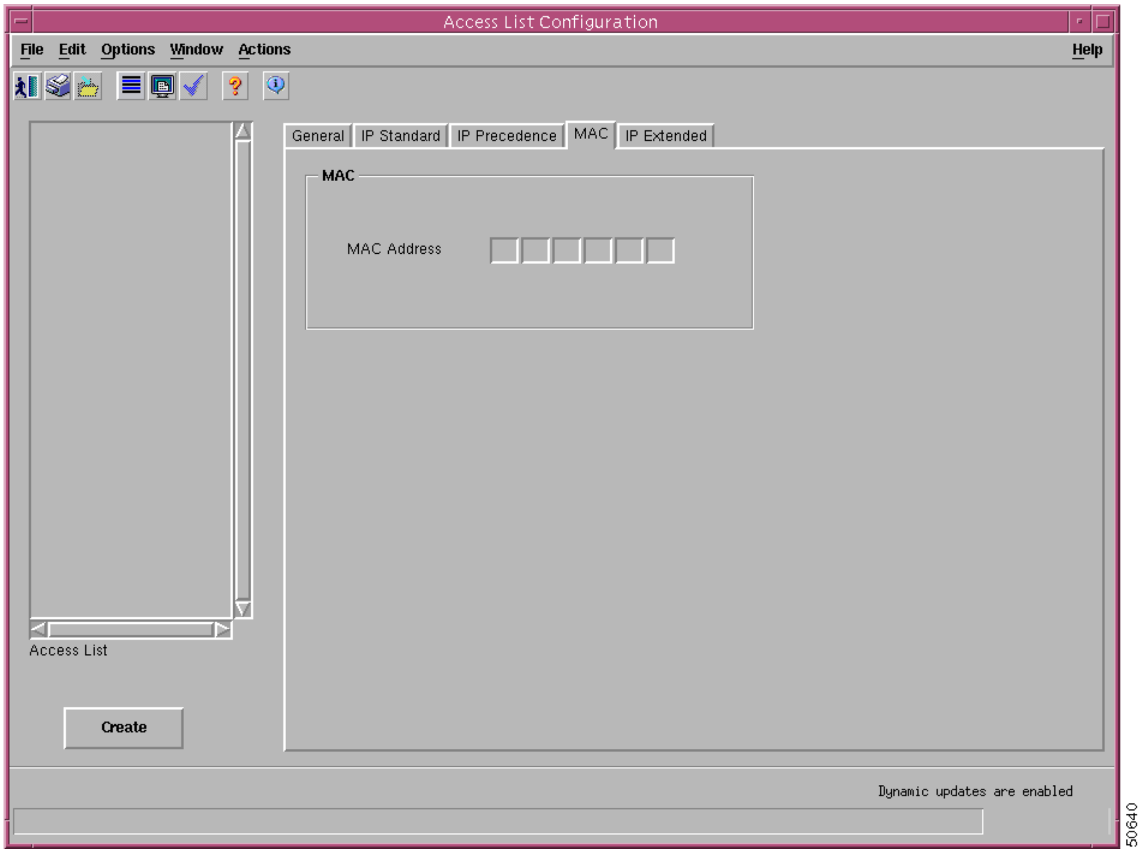
Precedence—IP precedence to be matched. Possible values are 0 - 7.

Precedence Bit Mask—If more than one precedence comes into the same classification, precedence bit mask should be used. Possible values for this field are 00-xx.

MAC

The MAC tab appears as follows.

Figure 10-5 Access List Configuration—MAC Tab



The MAC tab contains one area: MAC.

MAC

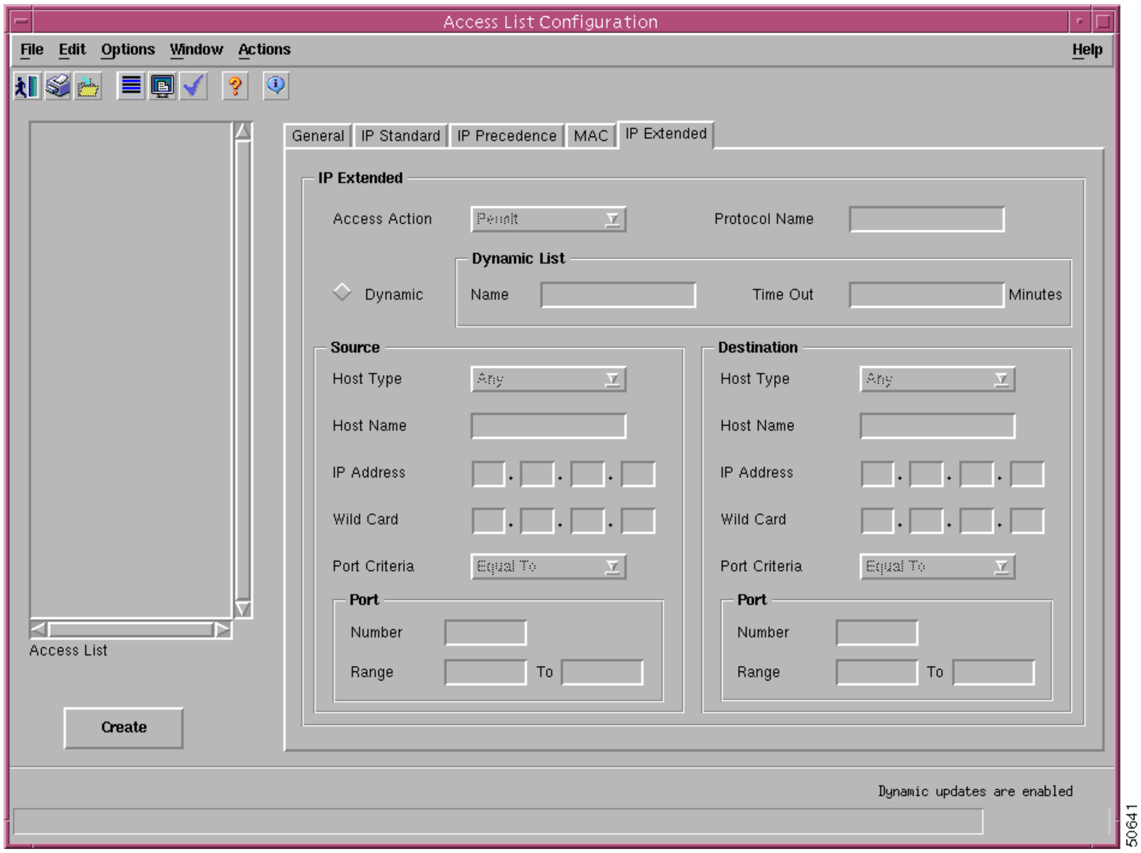
The MAC area contains one field:

MAC Address—Type in the MAC address for the packets to be classified.

IP Extended Tab

The IP Extended tab appears as follows.

Figure 10-6 Access List Configuration Window—IP Extended Tab



Access Action: Permit

Source — Host Type: Any; Port Criteria: Equal To

Destination — Host Type: Any; Port Criteria: Equal To

Dynamic updates are enabled

The IP Extended tab contains one area: IP Extended. The IP Extended area is further split into three subareas:

- Dynamic List
- Source
- Destination

IP Extended

The IP Extended area contains two fields:

Access Action—Action to be taken if the conditions are matched. Possible actions are deny and permit.

Protocol Name—Name or number of an IP protocol. Valid protocol number values are 0 - 255. Valid protocol names are as follows:

Table 10-1 Valid Protocol Names

Valid Protocol Names	
ahp	ipinip
eigrp	nos
gre	ospf
icmp	pcp

Table 10-1 Valid Protocol Names

Valid Protocol Names	
igmp	pim
igrp	tcp
ip	udp

Dynamic—Defines the selected access list to be dynamic. Dynamic access lists grant access per user to a specific source or destination host through a user authentication process. You can allow user access through a firewall dynamically, without compromising security restrictions.

Dynamic List

Name—Defines a name for the dynamic list (only available if Dynamic button is selected).

Time Out—Specifies the absolute length of time (in minutes) that a temporary access list entry can remain in a dynamic access list. The default (0) is an infinite length of time and allows an entry to remain permanently (only available if Dynamic button is selected).

Source and Destination

The Source and Destination areas contain the following fields:

Host Type—Indicates the hosts for which the access action are available. Possible values for this field include the following:

- Any—All hosts
- Host Name—Specified host name with wild card bits
- A.B.C.D—Specified IP address with wild card bits
- Host Hostname—Only the specified hostname
- Host A.B.C.D—Only the specified IP address

Host Name—Name of the host (or source of the packet) for which the access action is applicable.

IP Address—IP address of the host (or source of the packet) for which the access action is applicable.

Wild Card—If the access action is applicable for more than one host, then this field should be used as a mask. For example, the wild card 255.255.255.255 effectively represents any.

Port Criteria—Criteria to be applied on the specified port (interface) number. Possible values are as follows:

- None—Port number is insignificant
- Equal To—Equal to the port number
- Not Equal To—Not equal to the port number
- Greater Than—Greater than the port number
- Less Than—Less than the port number
- Range—Not supported

Port

The Port subarea in the Source and Destination areas contains the following fields:

Number—Port (interface) number from/to where the packet is sent or destined.

Range—Defines which port (interface) numbers will be allowed through this filter.

CAR Policy Apply

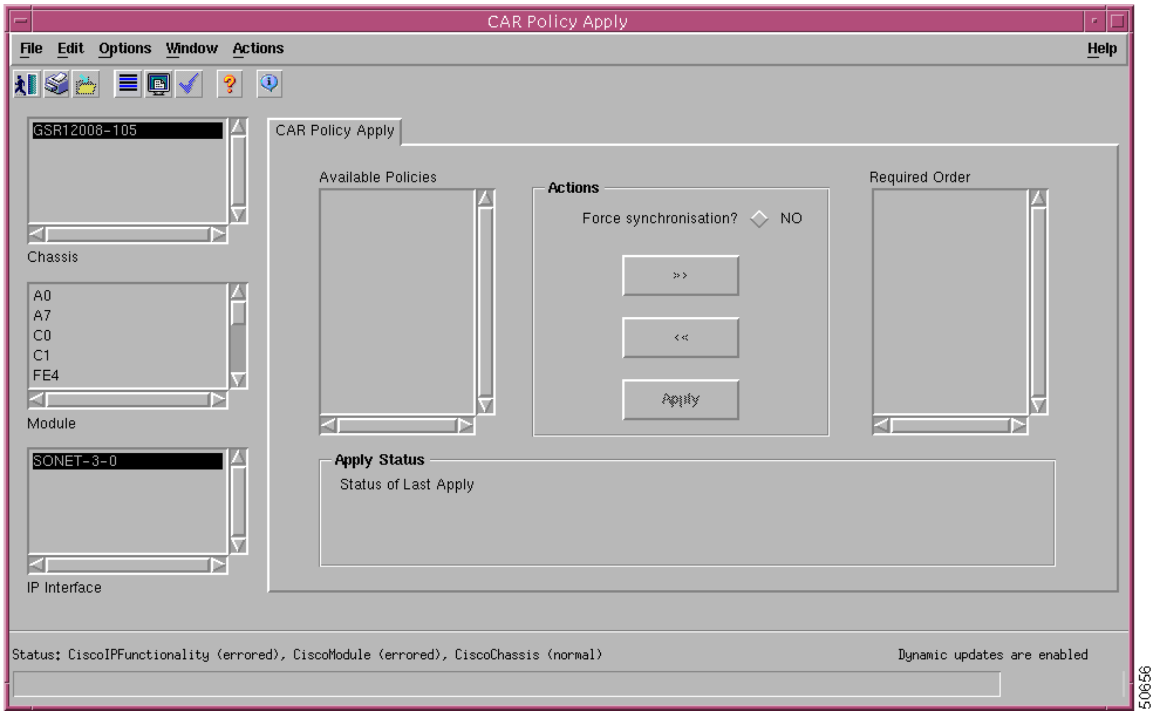
The CAR Policy Apply section covers the following areas:

- Applying CAR Policies to an Interface
- Removing a CAR Policy from an Interface
- Changing the Ordering of CAR Policies on an Interface
- Editing or Deleting a CAR Policy
- CAR Policy Apply Window—Detailed Description

Applying CAR Policies to an Interface

Step 1 Right-click on the interface you want to apply the CAR policy to, then choose **CGM Management> Logical>Layer 3 QoS>CAR>CAR Policy Apply.** The CAR Policy Apply window appears.

Figure 10-7 CAR Policy Apply Window



Chassis: GSR12008-105

Module: A0, A7, C0, C1, FE4

IP Interface: SONET-3-0

Force synchronisation? ◇ NO

Status: CiscoIPFunctionality (errored), CiscoModule (errored), CiscoChassis (normal)

Dynamic updates are enabled

Step 2 Make sure the appropriate chassis, module, and interface you want to apply the CAR policy to are selected in the list boxes at left. You can select multiple chassis, modules, or interfaces if desired.

Step 3 A pane listing available policies appears on the left. Select the policy you want to apply, and click on the right facing arrow to move that policy into the required order box at right.

Note If a CAR policy fails to be applied to an interface the Apply Status area on the CAR Policy Apply window (see Figure 10-7) is updated accordingly.

Step 4 When you have moved all the CAR policies you want to apply to the selected interface into the required order pane and you are satisfied with the ordering of those policies, click **Apply**.

If the interface is being managed, then the selected CAR policies are downloaded to the device.

For more details on the fields within this tab, refer to "CAR Policy Apply Window—Detailed Description" section on page 10-18.

Removing a CAR Policy from an Interface

To remove a CAR policies from an interface, proceed as follows:

Step 1 Within the CAR Policy Apply window (refer to Figure 10-7), ensure that the correct chassis, module, and interface are selected in the list boxes at left.

Any CAR policies that are currently applied to the selected interface appear in the required order list in the CAR Policy Apply tab. Any available CAR policies that are not being used appear in the available policies list in the CAR Policy Apply tab.

Step 2 Use the directional arrows to move CAR policies from the required order list back to the available policies list.

Step 3 Click **Apply** to apply the changes, removing the selected CAR policies from the interface.

Changing the Ordering of CAR Policies on an Interface

To change the ordering of CAR policies already applied to an interface, proceed as follows:

Step 1 Within the CAR Policy Apply window (refer to Figure 10-7), ensure that the correct chassis, module, and interface are selected in the list boxes at left.

Any CAR policies that are currently applied to the selected interface appear in the required order list in the CAR Policy Apply tab. Any available CAR policies that are not being used appear in the available policies list in the CAR Policy Apply tab.

Step 2 Use the directional arrows to move CAR policies from the required order list to the available policies list, then move the CAR policies, in the new order, back into the required order box.

Step 3 Click **Apply** to apply the new ordered CAR policies to the selected interface.

Editing or Deleting a CAR Policy

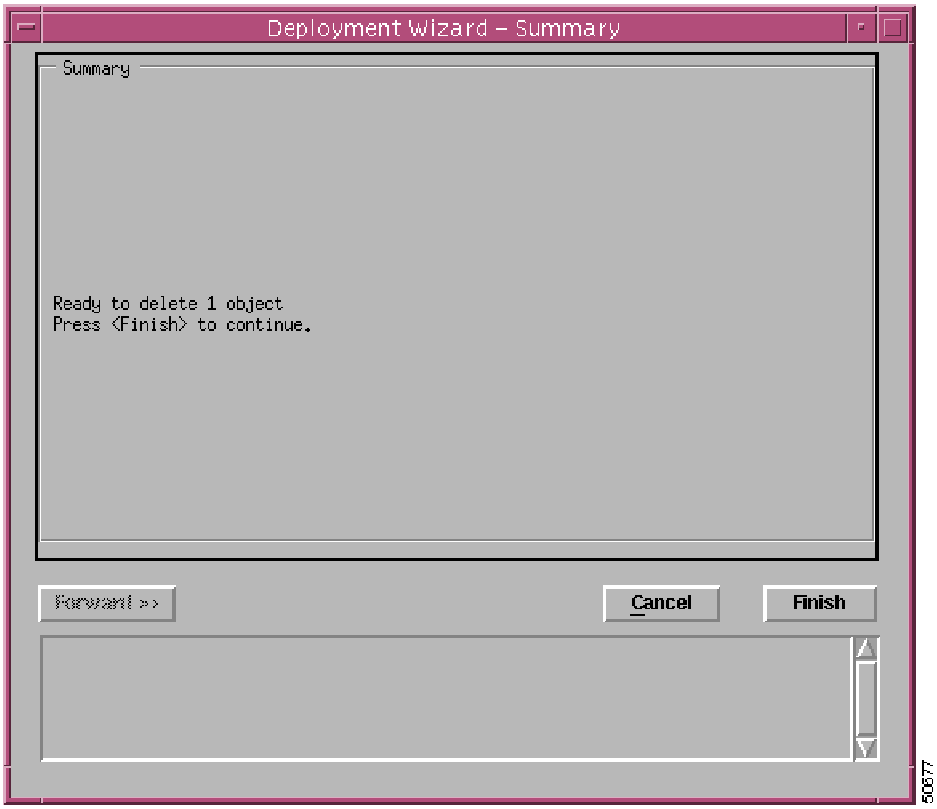
A CAR policy can only be edited or deleted if it is not currently being applied to any interfaces. Once you have applied a CAR policy to an interface, you cannot edit or delete it unless you remove it from the interface. If that CAR policy is being used by any other interfaces, you will still not be able to edit or delete the CAR policy. For this reason, it is a good idea to note down which interfaces have which CAR policies applied to them. If you keep such a list, if you later want to edit or delete the CAR policy, you can simply remove it from the interfaces that are using it, then proceed to edit the fields within the CAR Configuration window or delete the CAR policy.

To delete an existing CAR policy, proceed as follows:

Step 1 Select the CAR policies you wish to delete within the Layer 3 Qos view. Refer to the "Layer 3 QoS View" section on page 1-12 for details of the Layer 3 QoS view.

Step 2 Choose **Deployment>Delete Objects**. The Deployment Wizard appears with a summary of what will be deleted.

Figure 10-8 Deployment Wizard—Summary



```
Ready to delete 1 object
Press <Finish> to continue.
```

Step 3 Click **Finish**, and the CAR policy is deleted. If deletion fails, another interface might be currently using the CAR policy, therefore you cannot delete the object.

CAR Policy Apply Window—Detailed Description

The CAR Policy Apply window has one tab, CAR Policy Apply.

CAR Policy Apply Tab

The CAR Policy Apply tab contains two list boxes and two areas, Actions and Apply Status.

Available Policies—Lists all created CAR Policies that are available to apply to a selected interface.

Required Order—Lists all CAR policies that are applied to the selected interface.

Actions

The Actions area contains three buttons, as follows:

Right arrow button (>>)—Allows you to move CAR policies from the Available Policies list to the Required Order list.

Left arrow button (<<)—Allows you to move CAR policies from the Required Order list to the Available Policies list.

Apply—Allows you to apply the CAR policies in the Required Order list to the selected interface.

Apply Status

The Apply Status area contains one field, as follows:

Status of Last Apply—Status of the last CAR policy applied to an interface. This value can be either succeeded or failed.

CAR Status

The CAR Status section covers the following area:

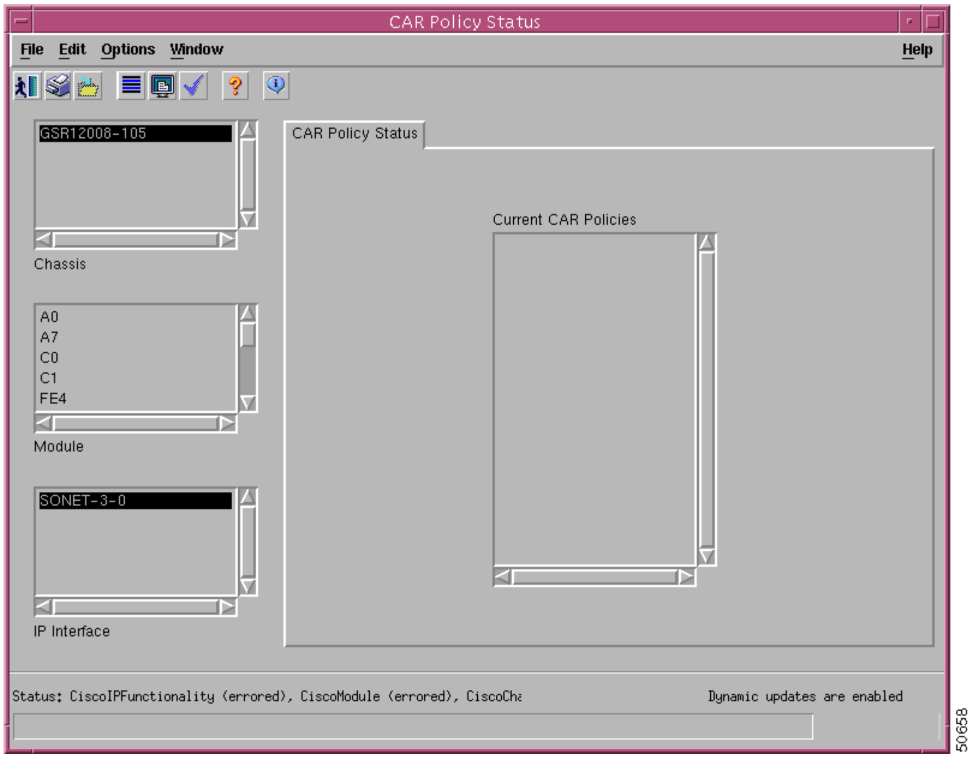
- Viewing the CAR Status

Viewing the CAR Status

The CAR Policy Status window shows you what CAR policies are currently applied to a selected interface, and in what order.

Step 1 Right-click on a selected interface, then choose **CGM Management>Logical>Layer 3 QoS>CAR> CAR Policy Status**. The CAR Policy Status window appears.

Figure 10-9 CAR Policy Status Window



Status: CiscoIPFunctionality (errored), CiscoModule (errored), CiscoCha

Dynamic updates are enabled

Step 2 Make sure the correct chassis, module, and interface are selected in the list boxes at left.

All of the current CAR policies that are applied to the selected interface appear, in numerical order, in the pane at right.

The Workflow for WRED/DRR

To begin working with WRED objects, the first step is to create and configure a CoS queue group (which includes DRR, or Distributed Round Robin). You can then apply the created CoS queue group to one or multiple interfaces. Only one CoS queue group can be applied to any amount of interfaces at a time.

At any given time, you also have the option to edit, delete, or change the association of a CoS queue group.

Engine Type Support for WRED

If an attempt is made to apply a WRED policy to an engine 1 module, then the request will be refused and an appropriate error message issued to the client. The full range of WRED functionality will be supported for engine 0, 2 and 4 modules.

CoS Queue Group Configuration

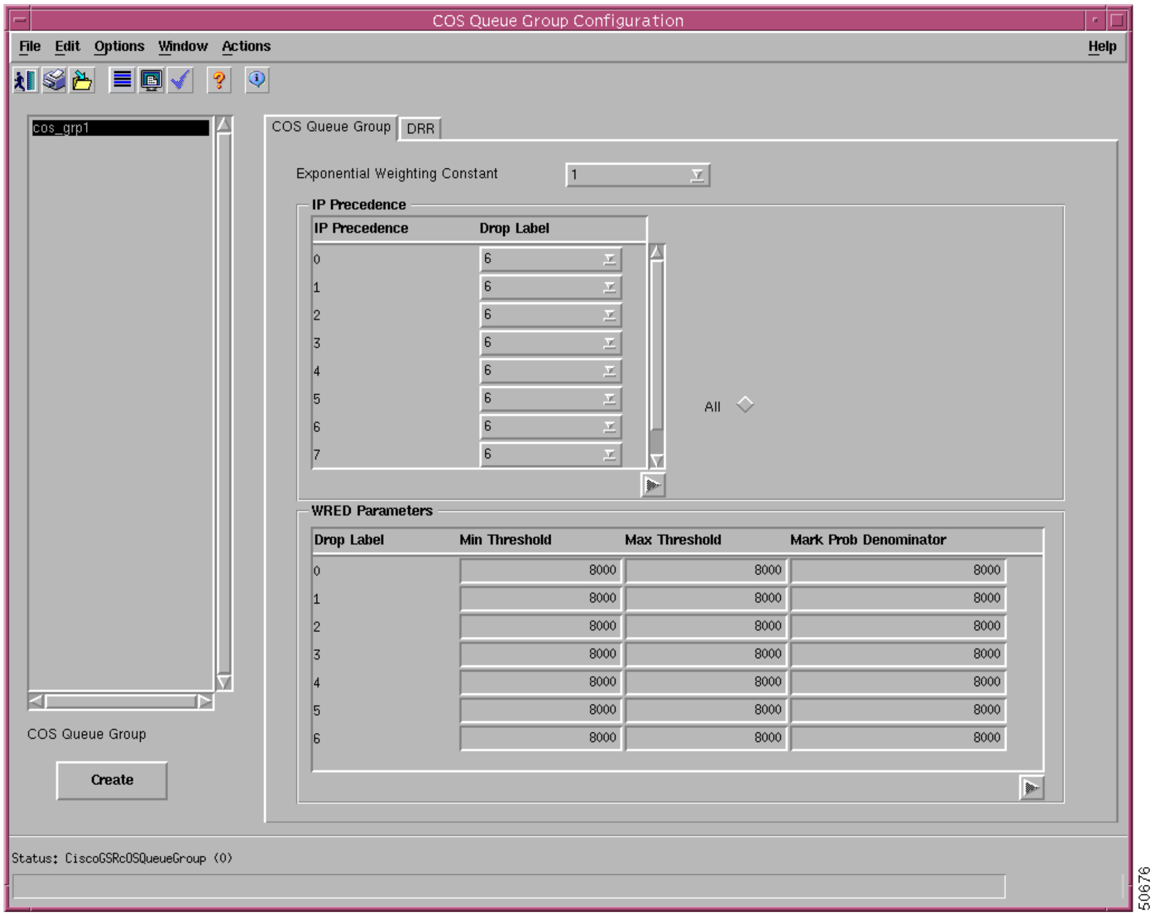
The CoS Queue Group Configuration section covers the following areas:

- Creating a CoS Queue Group Under WRED
- Editing or Deleting an Existing CoS Queue Group
- CoS Queue Group Configuration Window—Detailed Description

Creating a CoS Queue Group Under WRED

Step 1 In the Layer 3 QoS view, right-click on WRED-MDRR, then choose **CGM Management>Logical> Layer 3 QoS>WRED>CoS Queue Group Configuration**. The CoS Queue Group Configuration window appears.

Figure 10-10 CoS Queue Group Configuration Window—CoS Queue Group Tab



cos_grp1

Exponential Weighting Constant 1

IP Precedence

IP Precedence	Drop Label
0	6
1	6
2	6
3	6
4	6
5	6
6	6
7	6

All ◇

WRED Parameters

Drop Label	Min Threshold	Max Threshold	Mark Prob Denominator
0	8000	8000	8000
1	8000	8000	8000
2	8000	8000	8000
3	8000	8000	8000
4	8000	8000	8000
5	8000	8000	8000
6	8000	8000	8000

Status: CiscoGSRcOSQueueGroup (0)

Step 2 Click **Create**.

Step 3 Enter the CoS queue group name, then click **Ok**.

A window appears, confirming if you were successful or not. The name of your new CoS queue group appears in the list box at left.

Step 4 Modify the parameters in both tabs, as desired. The following section provides detailed information on the parameters in both tabs.

Step 5 Click **Save** to save the changes.

Editing or Deleting an Existing CoS Queue Group

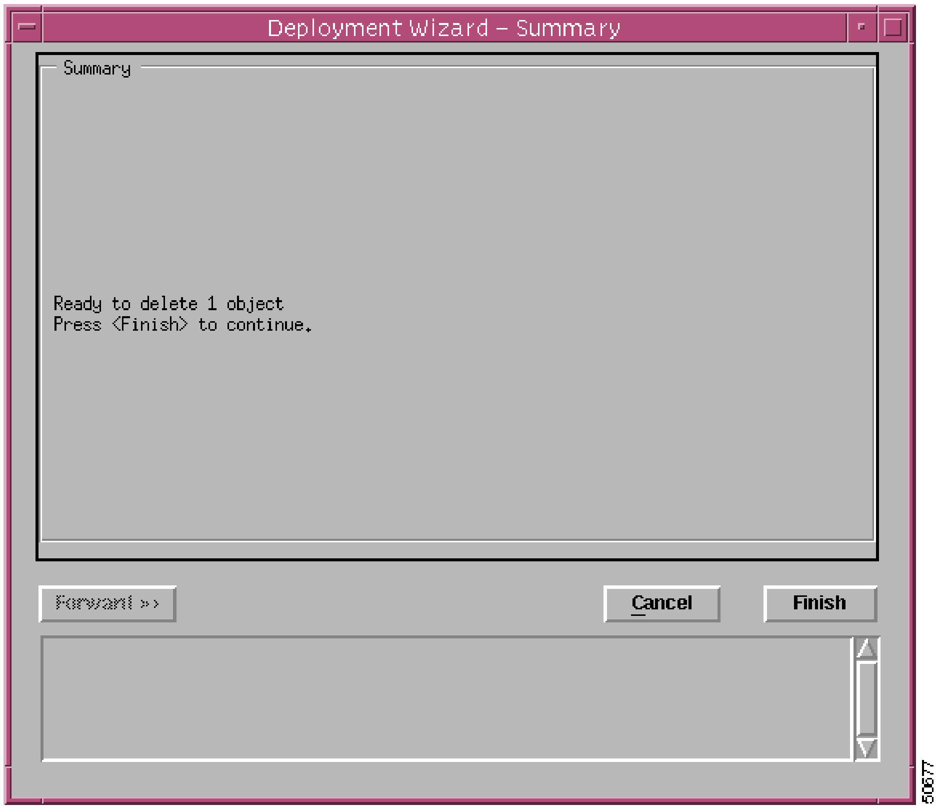
An existing CoS queue group can only be edited or deleted if it is not currently being applied to any interfaces. Once you have applied a CoS queue group to an interface, you cannot edit or delete it unless you remove it from the interface. If that CoS queue group is being used by any other interfaces, you will still not be able to edit or delete the CoS queue group. For this reason, it is a good idea to note down which interfaces have which CoS queue groups applied to them. If you keep such a list, if you later want to edit or delete the CoS queue group, you can simply remove it from the interfaces that are using it, then proceed to edit the fields within the CoS Queue Group Configuration window or delete the CoS queue group.

To delete an existing CoS queue group, proceed as follows:

Step 1 Select the CAR policies you wish to delete within the Layer 3 Qos view. Refer to the “Layer 3 QoS View” section on page 1-12 for details of the Layer 3 QoS view.

Step 2 Choose **Deployment>Delete Objects**. The Deployment Wizard appears with a summary of what will be deleted.

Figure 10-11 Deployment Wizard—Summary



Ready to delete 1 object
Press <Finish> to continue.

Step 3 Click **Finish**, and the CoS queue group is deleted. If deletion fails, another interface might be currently using the CoS queue group; therefore, you cannot delete the object.

CoS Queue Group Configuration Window—Detailed Description

The CoS Queue Group Configuration window has two tabs: CoS Queue Group and DRR (Deficit Round Robin).

CoS Queue Group Tab

In the CoS Queue Group tab, you can configure the WRED parameters and the mapping of the IP precedence to the specific WRED profile you wish to use. The CoS Queue Group tab has two areas: IP Precendence and WRED Parameters. The CoS Queue Group tab also has one outside field, as follows:

Exponential Weighting Constant—(numbers 0-15) Sets the weight used in calculating the average queue depth for this COS queue group.

IP Precedence

The IP Precendence area contains two headings: IP Precendence and Drop Label.

IP Precendence—This area allows the user to map packets that have a particular IP precendence to a WRED profile in this CoS queue group. You can map several or all precedences to the same WRED profile if you wish. By default, precendence values are mapped so that they are not dropped due to WRED.

Drop Label—Select a number, 1 - 6, which is the number of the corresponding drop label in the WRED parameters table.

WRED Parameters

The WRED Parameters area contains four headings: Drop Label, Min Threshold, Max Threshold, and Max Prob Denominator. The last three headings describe the actual WRED curve.

Drop Label—Drop label is a placeholder number for this set of WRED parameters. This is the number you map IP precedence values to.

Min Threshold—When the weighted queue average is below the minimum threshold, no packets are dropped.

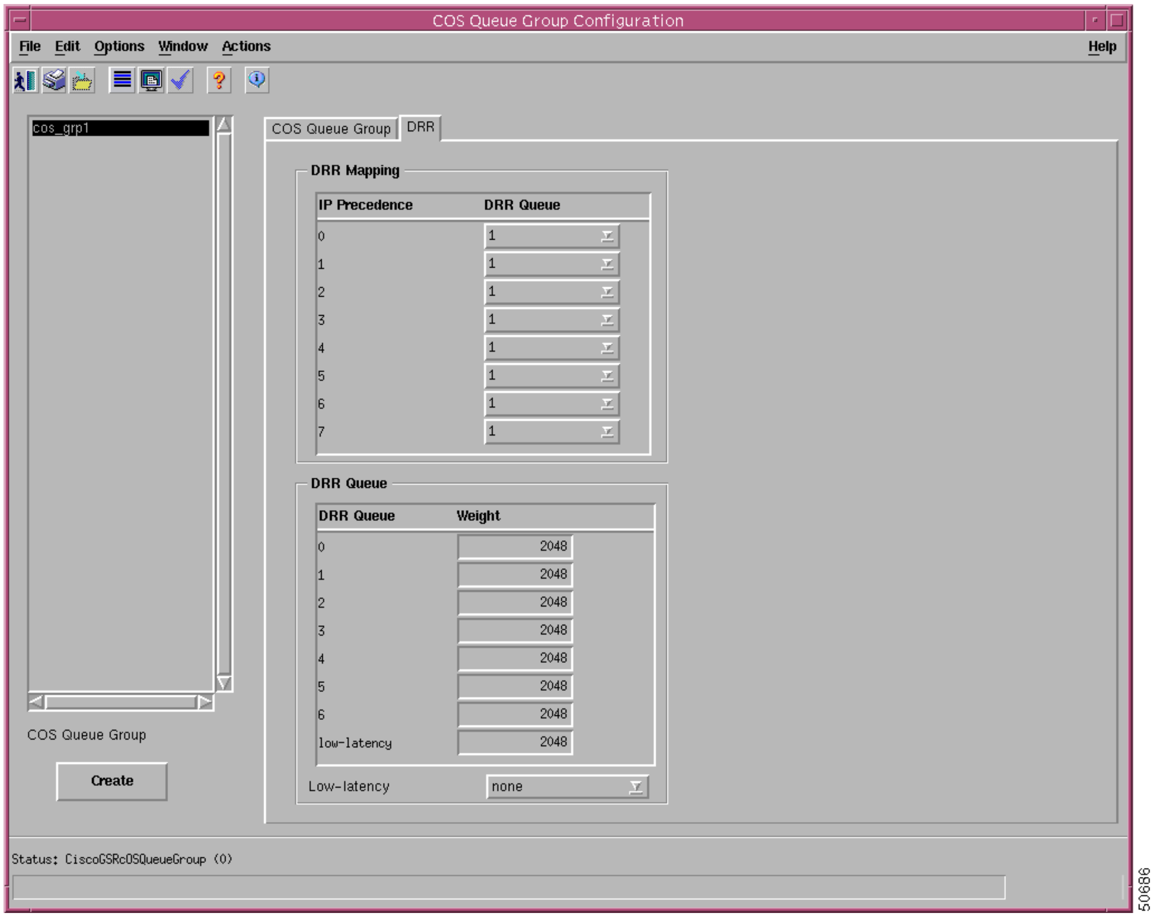
Max Threshold—When the weighted queue average is above the maximum queue threshold, all packets are dropped until the average drops below the maximum threshold.

Max Prob Denominator—When the weighted queue average is between the minimum and the maximum thresholds, the probability that the packet is going to be dropped can be calculated by a straight line from the minimum threshold (probability of drop will be 0) to the maximum threshold (probability of drop is equal to the max prob denominator).

DRR Tab

The DRR tab appears as follows:

Figure 10-12 CoS Queue Group Configuration Window—DRR Tab


COS Queue Group Configuration
File Edit Options Window Actions
Help
cos_grp1
COS Queue Group
Create
COS Queue Group
DRR
50686

DRR Mapping

IP Precedence	DRR Queue
0	1
1	1
2	1
3	1
4	1
5	1
6	1
7	1

DRR Queue

DRR Queue	Weight
0	2048
1	2048
2	2048
3	2048
4	2048
5	2048
6	2048
low-latency	2048

Low-latency none

Status: CiscoGSRcOSQueueGroup (0)

The DRR tab has two areas: DRR Mapping and DRR Queue. There is also a Low-latency field.

DRR Mapping

The DRR Mapping area allows you to map a particular IP precedence to a regular DRR queue (values 0-6 or low-latency).

DRR Queue

The DRR Queue area allows you to give a relative weight to each DRR queue.

Low-latency—Only applicable for MDRR. This value can be set to one of the following values:

Alternate priority—You must specify a weight in the DRR queue area.

Strict priority—No weight is specified.

None—If low latency is not mapped to any of the IP Precedences in the DRR Queue, then you must set the low latency to none.

WRED Tx Configuration

The WRED Tx Configuration section covers the following areas:

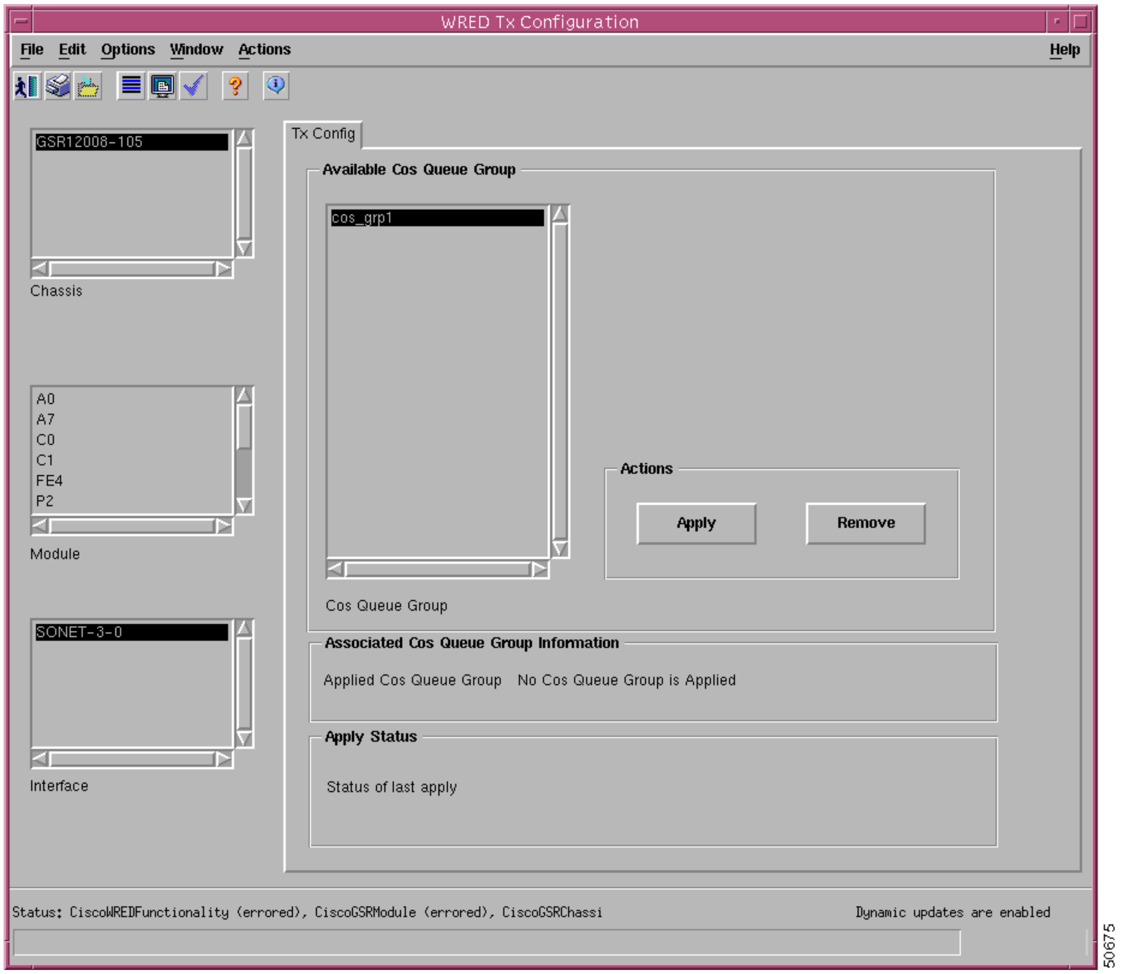
- Applying a CoS Queue Group to an Interface
- Removing a CoS Queue Group from an Interface
- Changing the Association of a CoS Queue Group
- WRED Tx Configuration Window—Detailed Description

Applying a CoS Queue Group to an Interface

To apply a CoS Queue Group to an interface, proceed as follows:

Step 1 In the Layer 3 QoS view, right-click on the desired CoS queue group, then choose **CGM Management>Logical>Layer 3 QoS>WRED>WRED Tx Configuration**. The WRED Tx Configuration window appears.

Figure 10-13 WRED Tx Configuration Window



Applied Cos Queue Group No Cos Queue Group is Applied

Status: CiscoWREDFunctionality (errored), CiscoGSRModule (errored), CiscoGSRChassi

Dynamic updates are enabled

Step 2 In the list boxes at left, choose the chassis and module that contain the interface(s) you want to apply the CoS queue group to, then choose the specific interface(s). More than one chassis, module, or interface can be selected at a time.

Step 3 Make sure the correct CoS queue group is highlighted in the Available CoS Queue Group list.

Step 4 Click **Apply**. If the interfaces are currently being managed (are commissioned), then the CoS queue group will be downloaded to the device and the status in the Associated CoS Queue Group Info area changes to on.

Note If a CoS queue group fails to be applied to an interface the Apply Status area on the WRED Tx Configuration window (see Figure 10-13) is updated accordingly.

Removing a CoS Queue Group from an Interface

To remove an applied CoS queue group from an interface, follow the steps above but, instead of clicking **Apply**, click **Remove**.

Changing the Association of a CoS Queue Group

If you want to apply a different CoS queue group to a selected interface or interfaces, you can simply follow steps 1 - 2 above, then select the new CoS queue group you want to apply, and click **Apply**. Any previously applied CoS queue groups are removed and the new CoS queue group is applied.

WRED Tx Configuration Window—Detailed Description

The WRED Tx Configuration window contains two areas:

- Available COS Queue Group
- Associated COS Queue Group

Available COS Queue Group

Available COS Queue Group—This list box displays all the available CoS queue groups. You can Apply or Remove a CoS queue group from the selected interface in this pane as well. If the selected interface has a CoS queue group applied to it, that CoS queue group will be highlighted in this box. If the selected interface has no CoS queue group applied to it, the top CoS queue group will be highlighted by default.

Apply—Once you have highlighted the CoS queue group in the Available COS Queue Group list, click Apply to apply it to the selected interface.

Remove—Once you have highlighted the CoS queue group in the Available COS Queue Group list, click Remove to remove it from the selected interface.

Associated COS Queue Group Info

Associated COS Queue Group Info—Status of the selected CoS queue group. Values can be as follows:

- On—The CoS queue group selected is applied to the interface
- Off—The CoS queue group selected is not applied to the interface
- No CoS Queue Group is Applied—No CoS queue groups have been applied to any interfaces.