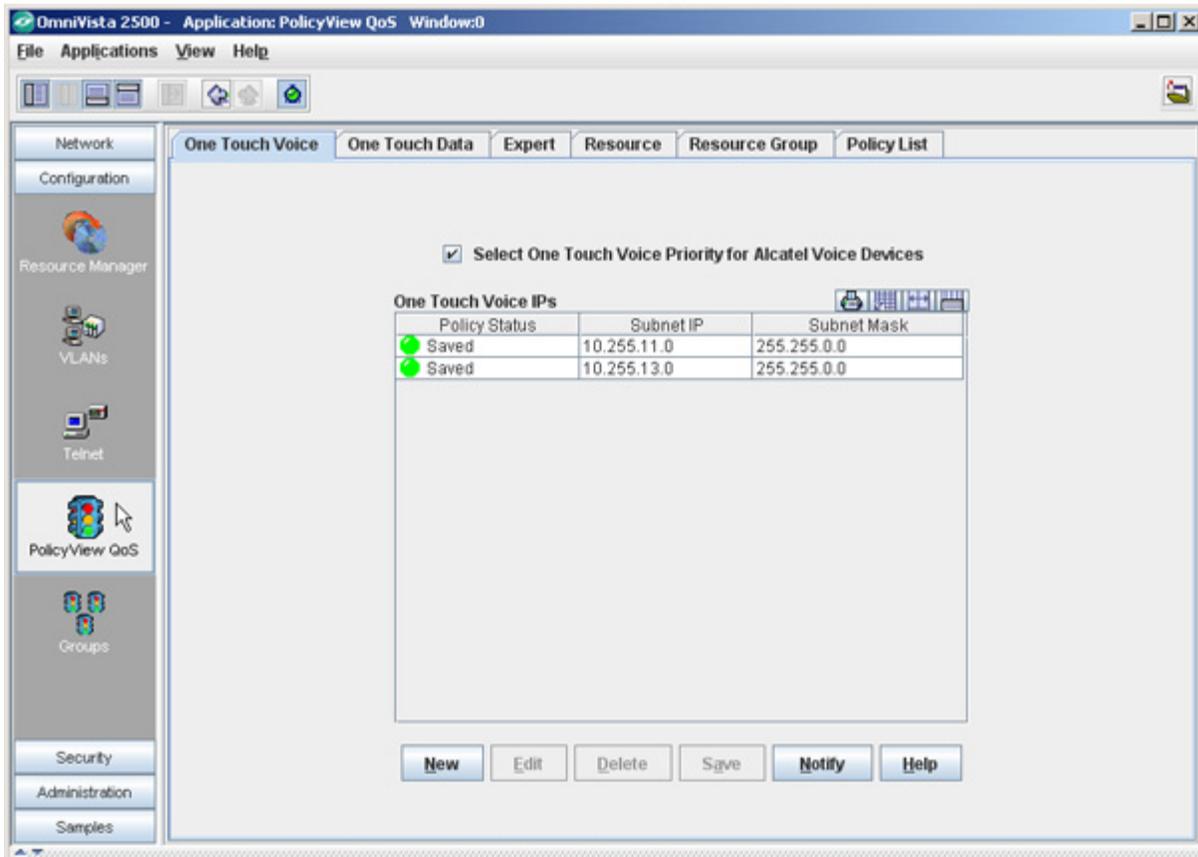


## Getting Started with PolicyView QoS

The PolicyView QoS application enables you to create Quality of Service (QoS) policies that specify QoS for network traffic. Policy rules are stored in a Lightweight Directory Access Protocol (LDAP) repository that is automatically installed with the PolicyView QoS application and resides on the same device as the OmniVista server. QoS-qualified devices in the network are notified when new or modified Policy rules are available on the LDAP repository via an SNMP interface. Software resident in the switch is responsible for retrieving the Policy rules from the LDAP repository, interpreting the Policy rules, and enforcing them on the switch.

When you first open the PolicyView QoS application, the **One Touch Voice**, **One Touch Data**, **Expert**, **Resource**, **Resource Group**, and **Policy List** tabs are displayed. Any existing devices that are configured for one touch voice mode are displayed.

### PolicyView QoS Application



PolicyView QoS provides easy, simplified "One Touch" modes that enable you to create QoS policies for voice and data traffic with minimal effort and maximum simplicity. If you use the One Touch modes to create QoS policies for your network, there is no need to understand the underlying QoS definitions and constructs. The One Touch modes enable you to create QoS policies without bothering with the normal complexity associated with QoS. All QoS policies created using One Touch modes are automatically applied to all QoS-enabled devices in the list of All Discovered Devices (Topology application).

The PolicyView QoS application also provides an "Expert" mode that enables you to create more complex QoS policies by using standard QoS constructs. QoS policies created in the Expert mode can be applied to all QoS-enabled devices in the list of All Discovered Devices or to selected QoS-enabled devices.

PolicyView QoS enables you to assign four distinct traffic priorities:

- Platinum provides the highest quality of service (and maps to a firmware priority of 7).
- Gold provides the next-highest quality of service (and maps to a firmware priority of 5).
- Silver provides the next-highest quality of service (and maps to a firmware priority of 3).
- Bronze provides the same quality of service as best effort (and maps to a firmware priority of 1).

A separate egress queue is maintained in the hardware for traffic of each priority.

## QoS Terms and Definitions

QoS policies are created by associating a "Condition" with an "Action." A condition specifies criteria that, when true, will cause traffic to flow as specified by the associated action. A condition can specify criteria such as the following (a limited example):

- A source MAC address or a source IP address or a source VLAN ID, so that the condition applies to traffic originating from that source only
- A destination MAC address or a destination IP address or a destination VLAN ID, so that the condition applies to traffic flowing to that destination only.

An action specifies the treatment traffic is to receive when the criteria specified by the condition are true. This treatment may include the priority and bandwidth to be allocated to the traffic, its minimum and maximum output rates, and the manner in which packets are tagged upon egress from the switch (if at all).

The PolicyView QoS application supports Provisioned QoS actions. By default, Provisioned QoS provides best-effort QoS in the switch. A Provisioned QoS action enables a network administrator to provide traffic with QoS other than best effort and to define the network resources, such as bandwidth and priority, to be made available to the traffic. When the criteria defined by the associated condition are true, traffic will be assigned to a queue that delivers the QoS specified by the action.

## One Touch Mode

As previously stated, PolicyView QoS provides One Touch modes that enable you to create QoS Policies for voice and data traffic with minimal effort and maximum simplicity. The One Touch Voice and One Touch Data screens are shown and described below.

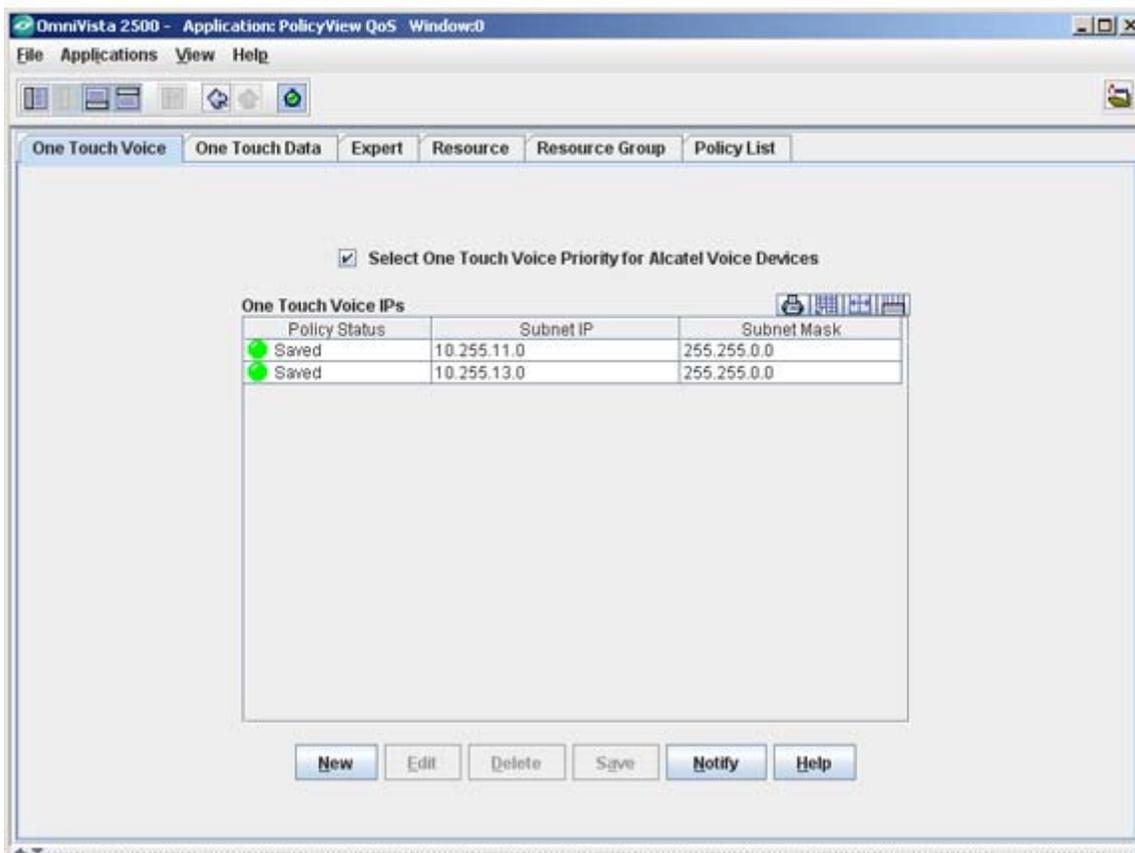
### One Touch Voice QoS

The **One Touch Voice** tab (shown below) enables you to provide Platinum QoS to all voice traffic that enters the network, and all voice traffic that originates from the network. There are two ways to apply one touch voice mode policies:

- Clicking the checkbox at the top of the window (Default) provides Platinum QoS to all voice traffic flowing to preconfigured ranges of Alcatel MAC addresses. The preconfigured MAC addresses belong to Alcatel voice devices and IP phones.
- You can also click the **New** button and enter the IP address of subnets that contain IP phones and voice devices to provide Platinum QoS to all voice traffic flowing to those subnets and all voice traffic originating from those subnets.

Click the **Save** button, to automatically create the appropriate conditions, actions, and policies. To learn more about the One Touch Voice tab, click [here](#).

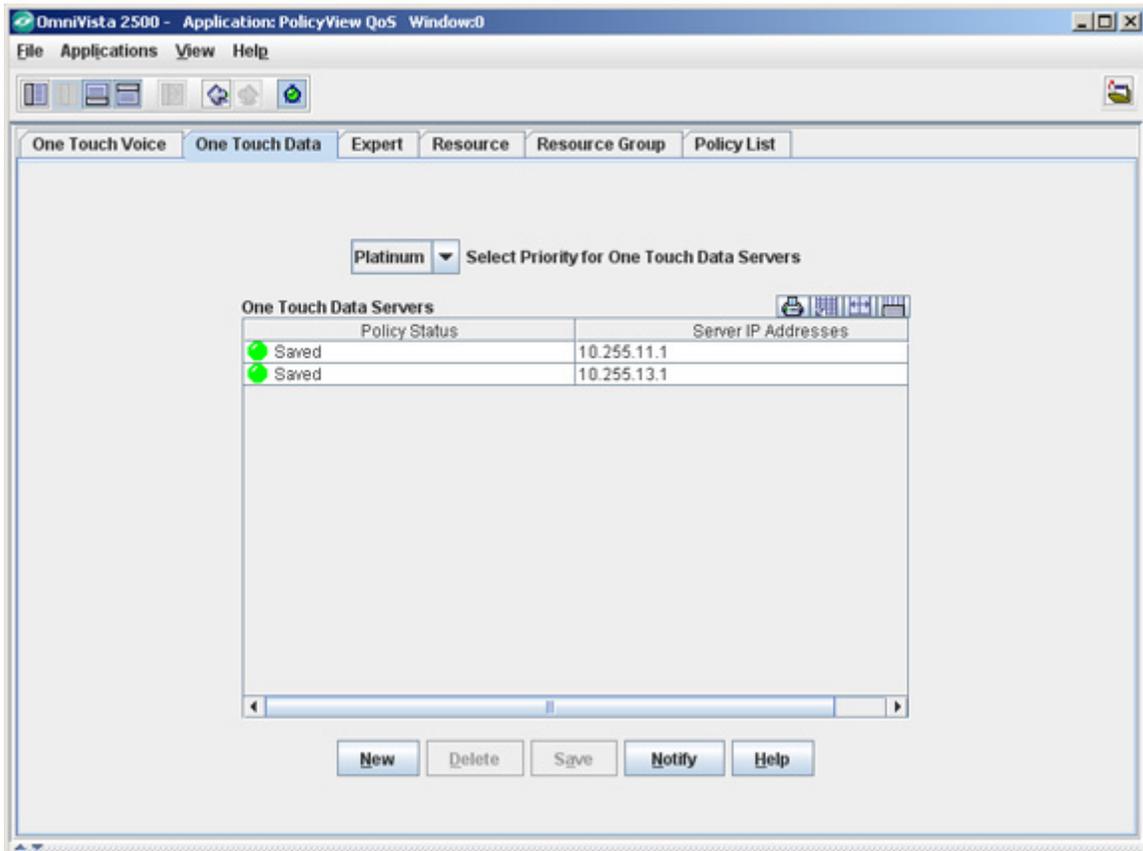
### One Touch Voice Tab



### One Touch Data QoS

The **One Touch Data** tab enables you to assign the desired quality of service - Platinum, Gold, Silver, or Bronze - to all data traffic flowing to, and all data traffic originating from, specific data servers. Set the Priority field to the desired quality of service, enter the data server's IP address (e.g., 10.255.11.242), and click the **Save** button. The appropriate conditions, actions, and policies are created automatically. To learn more about the One Touch Data tab, click [here](#).

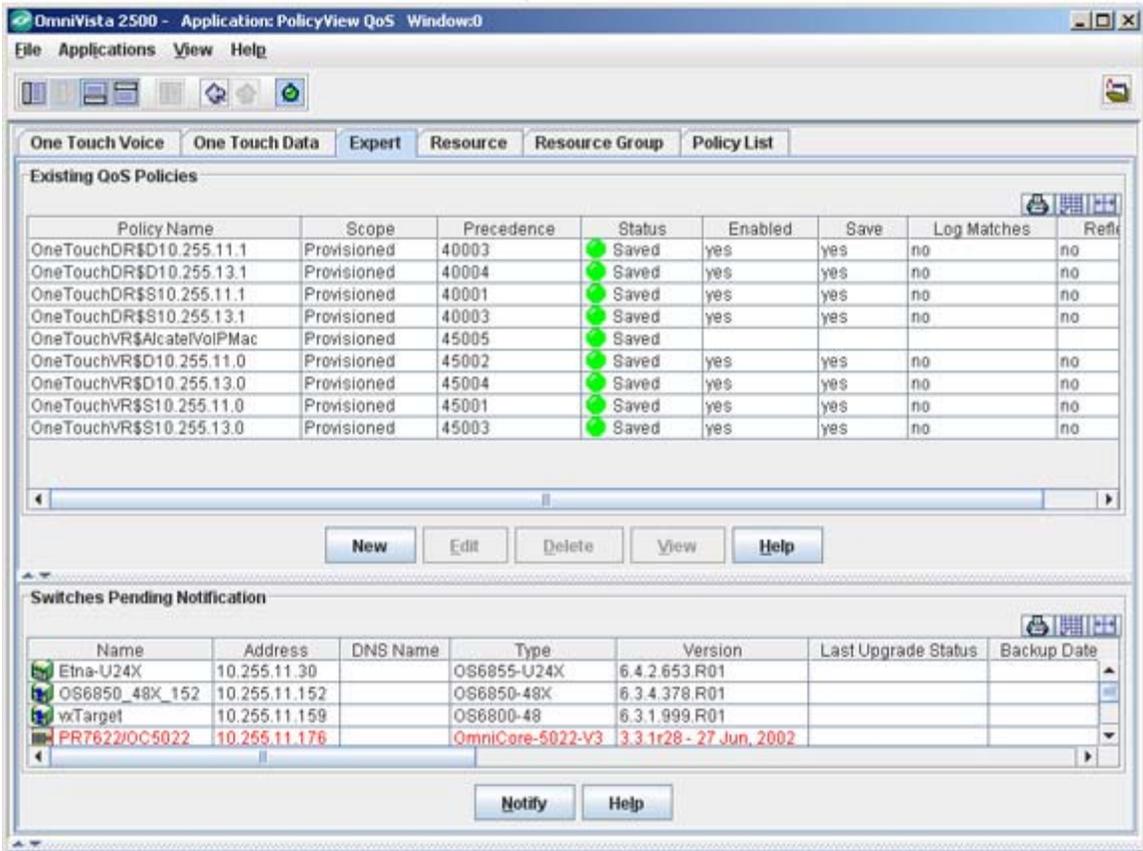
## One Touch Data Tab



## Expert Mode

In the Expert mode, conditions and actions are not created automatically; and the user defines the devices to which the policies are assigned. The Expert mode enables you to create conditions and actions manually, by specifying each individual parameter. In the Expert mode, you can create conditions that specify MAC addresses, IP address, protocols, VLAN IDs, specific DSCP or TOS values, or specific 802.1 priority values.

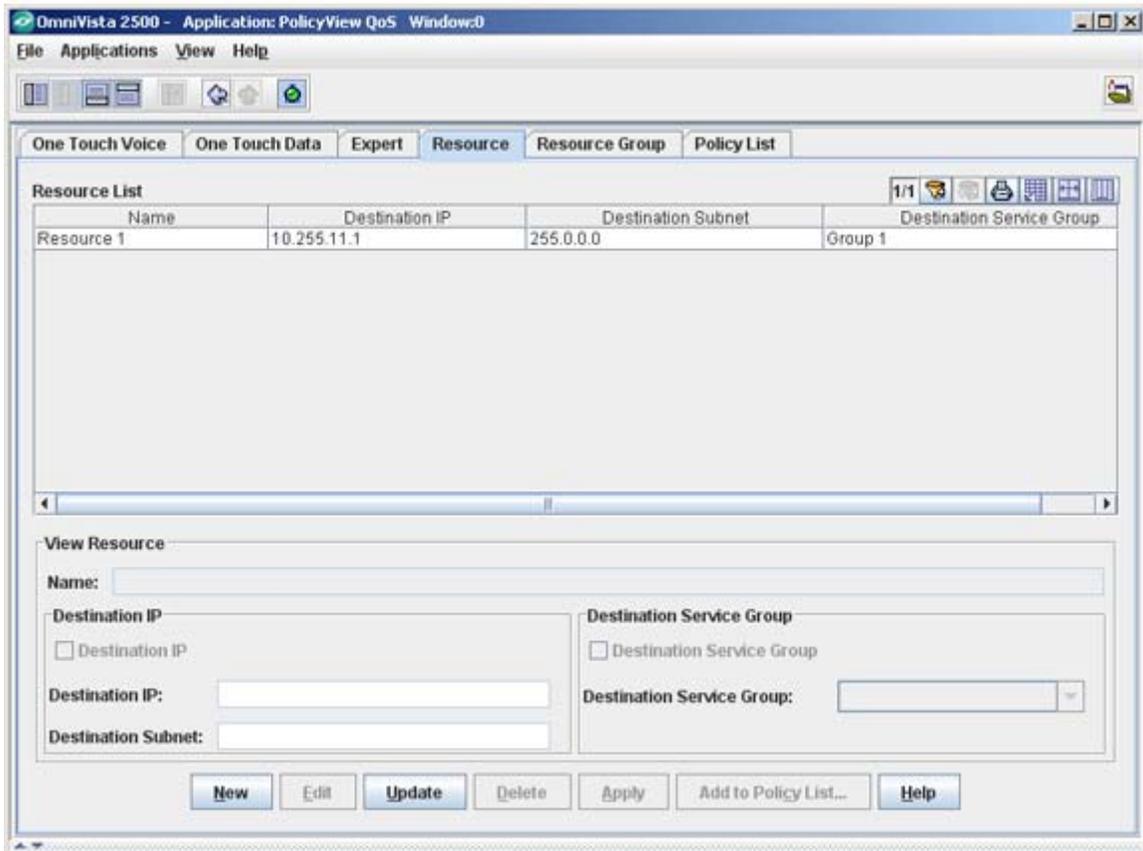
Expert Tab



**Resource**

The Resource Tab is used to create/edit system resources for QoS Policies. Although you can use Policy View QoS Expert Mode to create Policies for User Network Profiles (UNP), this can be time consuming. the Resource and Resource Group tabs can be used to quickly create resources that can be turned into Policies and added to Policy Lists.

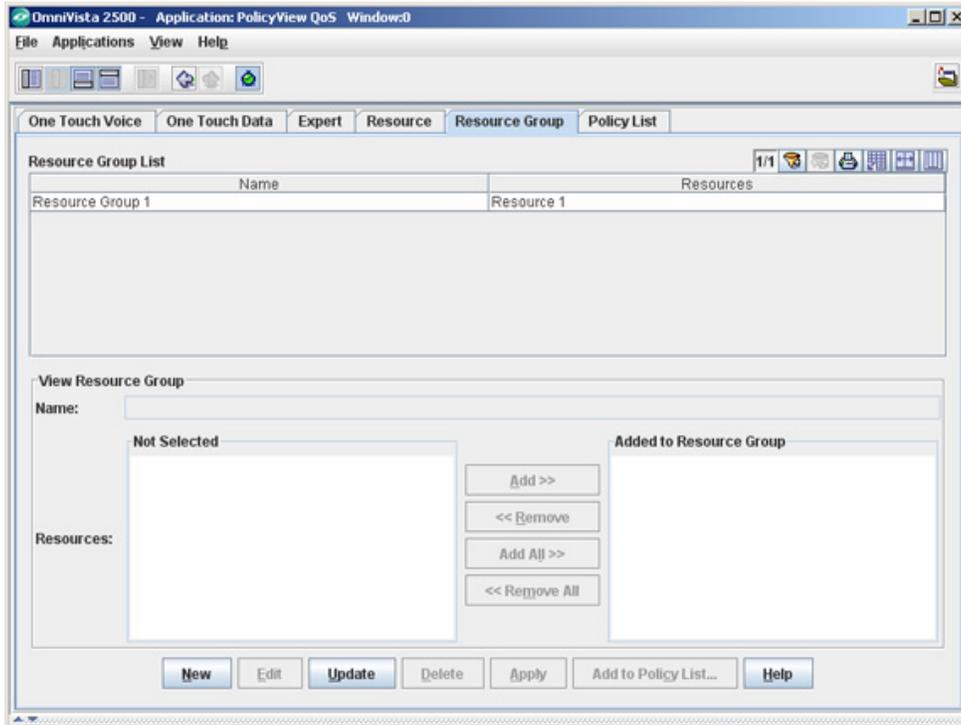
## Resource Tab



## Resource Group

The Resource Group tab is used to create/edit system Resource Groups for QoS Policies. Along with the Resource tab, the Resource Group tab can be used to quickly create Resource Groups that can be turned into Policies and added to Policy Lists.

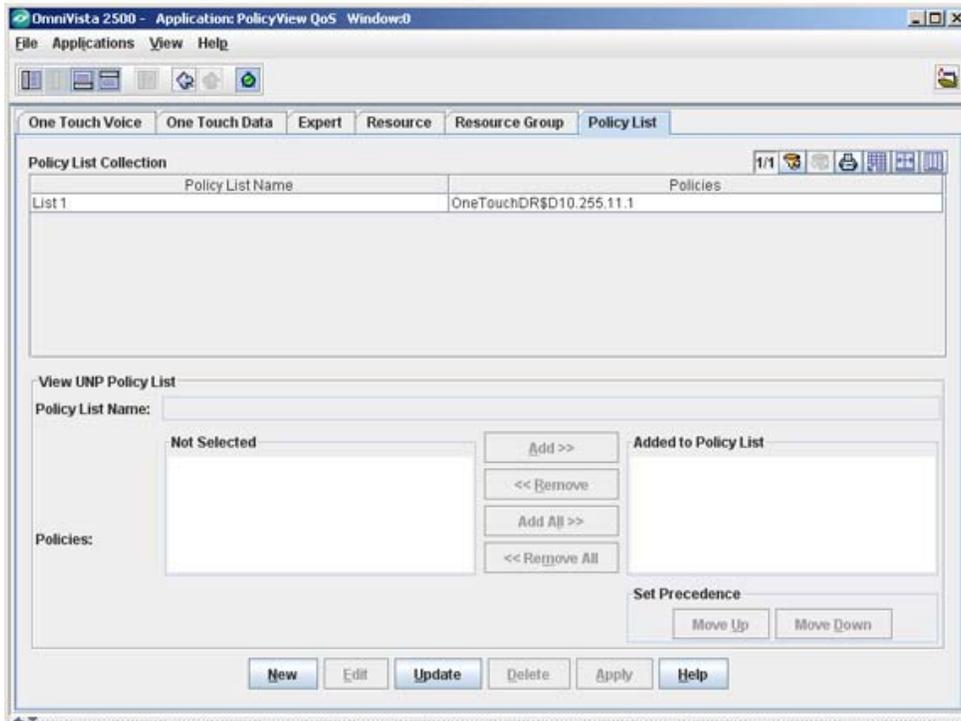
Resource Group Tab



Policy List

The Policy List tab displays a list of all policies configured for the switch. It is also used to view, create, modify and delete policy lists and assign QoS/ACL policy rules to a policy list.

Policy List Tab



## QoS-Qualified Devices

A QoS-qualified device is a device that can support the PolicyView QoS application and provisioned QoS. AOS devices are qualified devices. XOS devices are qualified devices if their flash file systems contain the policy.img file and the qos.img file. QoS-qualified devices are identified during the discovery process. The list of devices is displayed in the Expert tab.

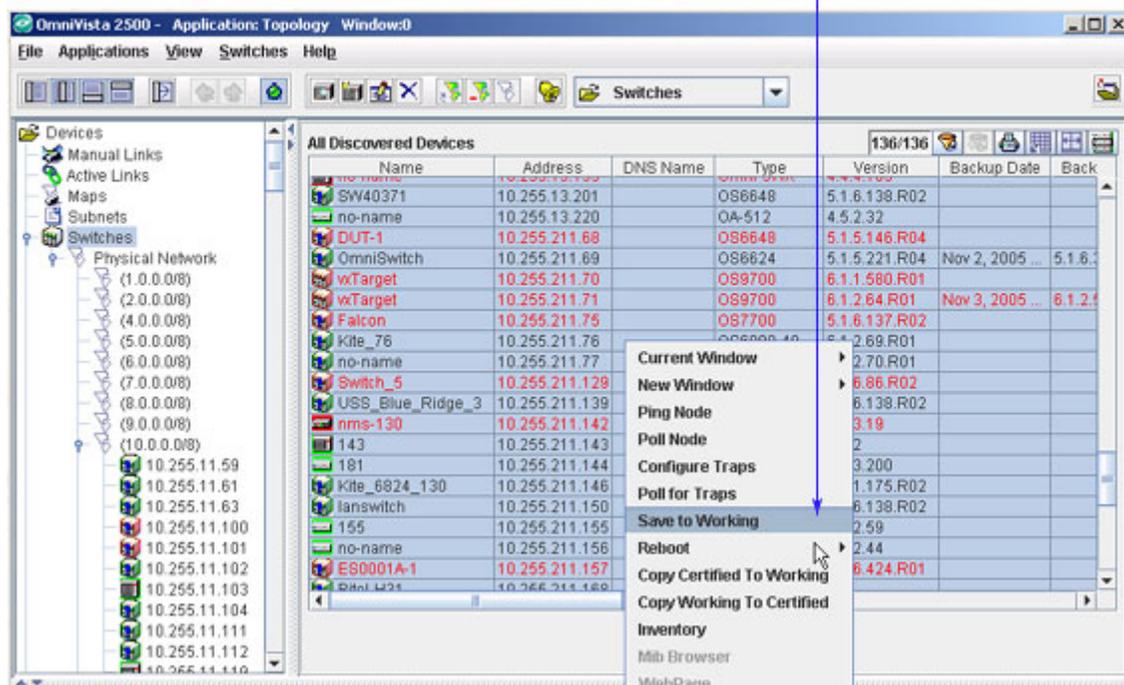
## Saving Changes to the Switch

When PolicyView QoS is executed, it writes the address of the LDAP repository to each QoS-qualified switch in the list of All Discovered Devices. The LDAP address is written to the running configuration of the switch. For this reason, once PolicyView QoS has executed, all switches are left with their running configuration in the "Unsaved" state (indicating that the running configuration has changes that have not been saved to the working directory). When a switch reboots, its running configuration is lost, so it is important to save the running configuration to the working directory and then the certified directory after PolicyView QoS has executed. To do this, follow the steps below.

**Note:** All changes made to the switch configuration will be saved, including any changes made via the CLI, WebView, or other OmniVista applications, in addition to the changes made by the PolicyView QoS application.

1. Go to the Topology application.
2. Select **Switches** in the tree to display the list of All Discovered Devices. Click the **Changes** column to sort the list according to the switch configuration state.
3. Select all switches with "Unsaved" changes, right-click, and select **Save to Working**. The **Changes** field will display "Uncertified" when the changes are saved to the working directory.
4. Select all switches with "Uncertified" changes, right-click, and select **Copy Working to Certified**. The **Changes** column will go blank when the Working Directory is saved to the Certified Directory (this may take a few minutes).

Click on the Changes Column to sort switches. Select all "Unsaved" switches, right-click, and select Save to Working. Then select "Uncertified" switches, right-click, and select Copy Working to Certified.

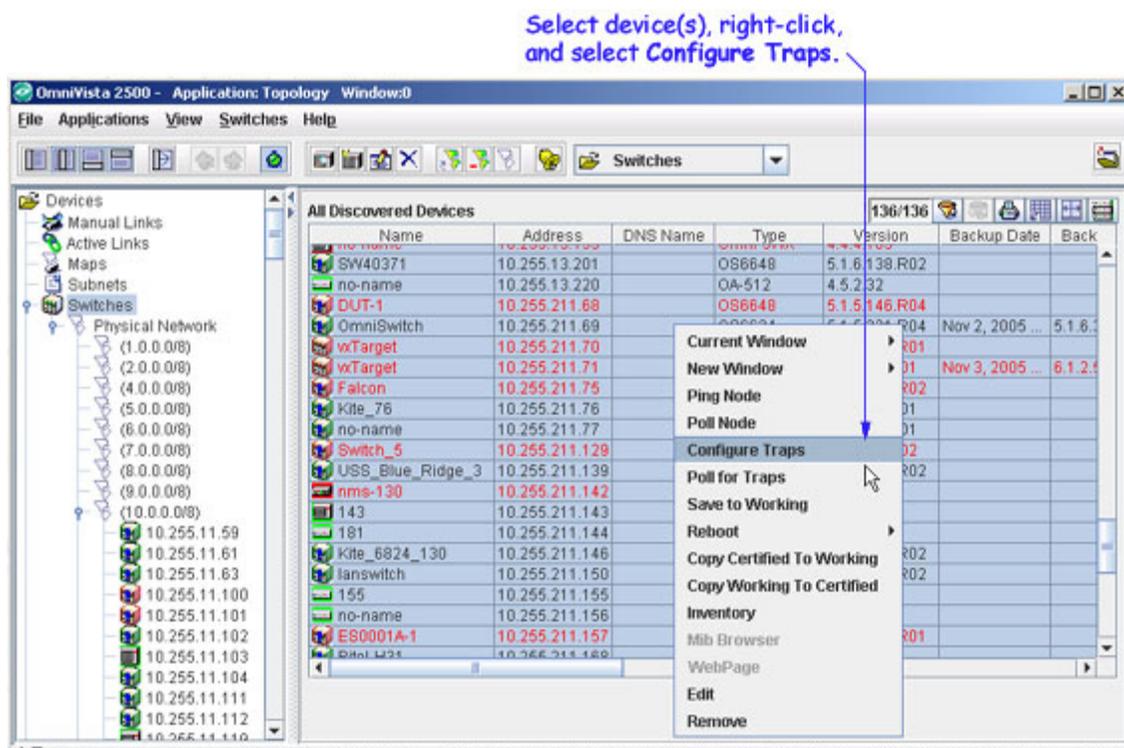


Note: See the Topology application help for more details.

## Required Traps

You must configure the switches in the network to send OmniVista the traps that are needed by the PolicyView QoS application. To configure traps for one or more devices, go to the Topology application, select the device(s) in the list of All Discovered Devices, right-click, and select **Configure Traps** from the pop-up menu. The Configure Traps window is displayed. PolicyView QoS requires the following traps:

- Trap **policyEventNotification** is required from OmniSwitch 7700s/7800s.
- Trap **policyEvent** is required from XOS devices.



**Note:** See the Topology application help for step-by-step instructions for configuring traps.

## Policy Precedence and Conflicts

PolicyView QoS enables you to define the precedence of policies created in PolicyView. A policy rule's precedence determines which policy will take effect in the rare case of a conflict. QoS policies can be created through the CLI, through WebView, and through SNMP MIB browsers as well as through PolicyView QoS. Policies created through the CLI, WebView, or MIB browsers are not written to the LDAP repository and are not manageable through the PolicyView QoS application.

**Note:** It is highly recommended that network administrators who use PolicyView QoS to create policies do NOT use any outside management tools for creating policies, conditions, or actions.

Policies created in PolicyView QoS are assigned a precedence value between 30001-65535. However, precedence values 30001-65535 are not reserved for PolicyView QoS policies. Policies can also be created using the CLI, WebView, or a MIB browser, and these policies can be assigned any precedence value between 0-65535. Therefore, it is possible to assign these policies the same precedence that is assigned to policies created through the PolicyView QoS application. For this reason, if you are creating policies using PolicyView QoS as well as outside management tools (which is NOT recommended), do not assign precedence values between 30001-65535 to any policies created outside of the PolicyView QoS application.

- One Touch Voice policies have precedence values between 45000 and 65535.
- One Touch Data policies have precedence values between 40000 and 44999.

- Expert Mode policies have precedence values between 30000 and 39999.

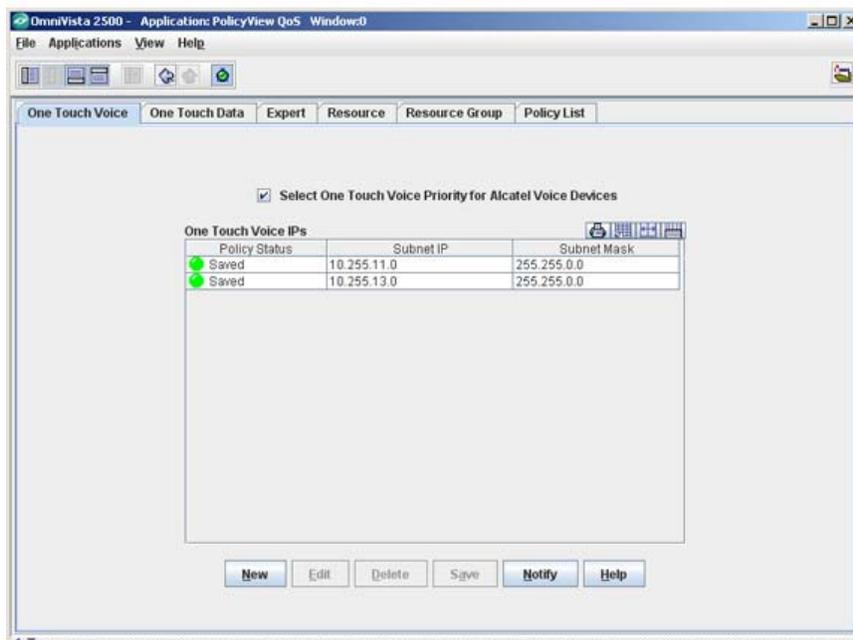
## One Touch Voice Tab

The **One Touch Voice** tab (shown below) enables you to easily assign the highest quality of service to all voice traffic that enters the network and all voice traffic that originates from the network. There are four QoS priority queues supported by Alcatel devices: Platinum, Gold, Silver, and Bronze. Platinum provides the highest QoS and Bronze provides the lowest QoS. The **One Touch Voice** tab enables you to assign Platinum QoS to voice traffic in two ways:

- Select the checkbox at the top of the window and click the **Save** button to automatically create a Layer 2 policy that provides Platinum QoS for all voice traffic flowing to a pre-configured range of Alcatel MAC addresses. The pre-configured MAC addresses belong to Alcatel voice devices and IP phones.
- Click the **New** button, enter one or more IP subnets in the **Create One Touch Voice IP** panel, and click the **Save** button to create Layer 3 policies that provide Platinum QoS for all voice traffic flowing to, and originating from, the IP subnet(s) entered. Note that when you do this, two policies are created for each subnet entered - one for traffic originating from the subnet, and one for traffic flowing to the subnet. If the Layer 2 MAC address policies described above do not exist at that time, they will also be created. (This is explained in more detail below.) All policies created are applied to all QoS-enabled devices in the list of All Discovered Devices.

**Note:** OmniSwitch 6800/7000/8000/9000 series switches support the 802.1 priority. However, 6600 series switches and some current XOS hardware and firmware releases do not. Please refer to the switch Release Notes for information on the specific QoS functions available on various current platforms and combinations of hardware/firmware.

One Touch Voice Tab



## One Touch Voice Layer 2 (MAC) Policies

As mentioned above, you can select the checkbox at the top of the window and click the **Save** button to automatically create a policy that provides Platinum QoS for all voice traffic flowing to a pre-configured range of MAC addresses for Alcatel voice devices and IP phones. The MAC address range is:

- 00:80:9F:\*.\*\*.\*

The policy includes a condition specifying destination MAC addresses that match the range, and an action specifying the highest priority provisioned QoS, which is Platinum QoS.

It is important to note that OS6250 and OS6250-M devices have a limitation where “non-IP” policies (no L3, L4 conditions) only apply to “non-IP” packets. This requires an additional step to apply the policy to L3 traffic across the network. For these devices, you must specify the sub-networks for voice phones to ensure the policy is applied to L3 traffic. If your network contains 6250/6250-M devices, enter the applicable IP subnets to [create Layer 3 policies](#) in addition to the One Touch Platinum QoS Layer 2 policy that you create using the checkbox at the top of the window.

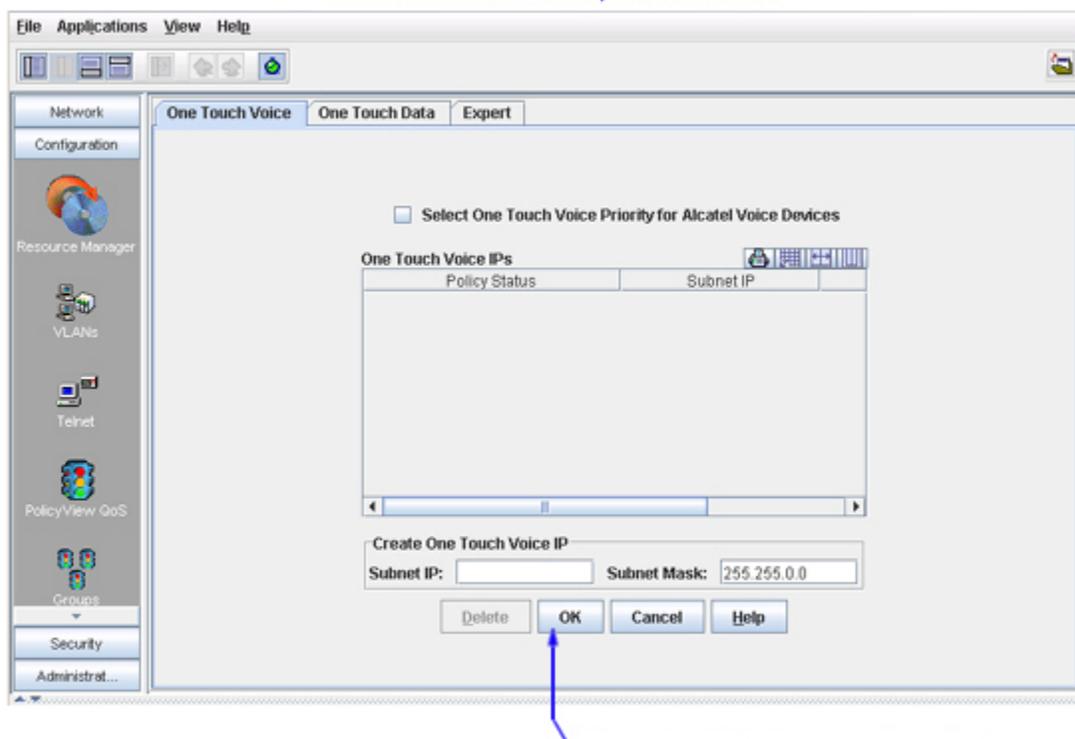
Also, network administrators should be aware that Layer 2 policies (policies that specify MAC addresses) are “lost” when traffic passes through a router. If traffic is expected to travel more than one router hop, it is advisable to [create Layer 3 policies](#) in addition to the One Touch Platinum QoS Layer 2 policy that you create using the checkbox at the top of the window.

**Note:** In Expert Mode, priority levels for each condition can be set from 0 - 7. A value of 7 provides the highest priority and a value of 0 provides the lowest priority. Platinum QoS is equal to a priority level of 7. However, for **802.1** voice traffic, Platinum QoS provides a priority level of 5.

## Creating One Touch Voice Layer 3 (IP) Policies

As stated above, you can create One Touch Voice Layer 2 (MAC) policies by selecting the checkbox at the top of the window and clicking the **Save** button. However, to create Layer 3 One Touch Voice policies, follow the steps below. (Note that devices on the subnets entered should be voice-capable.)

## One Touch Voice Layer 3 Policies



Enter subnet IP address and mask, then click OK. Click Save to save the policy.

1. Click the **New** button. The **Create One Touch Voice IP** panel appears (shown above).
2. Enter the IP subnet address and mask in the Subnet IP and Subnet Mask fields, respectively.
3. Click the **OK** button. The **Create One Touch Voice IP** panel disappears, the subnet appears in the **One Touch Voice IPs** table as "Unsaved", and the **Save** button is enabled. Repeat steps 1 - 3 to add additional subnets.
4. Click the **Save** button to save the policy to the LDAP repository.

Policies are written to the LDAP repository as follows:

- Two policies are written to LDAP for each subnet listed in the **One Touch Voice IPs** table.
- One policy is written to LDAP for each of the six pre-configured ranges of Alcatel voice MAC addresses.

5. Click the **Notify** button to notify the network switch(es) assigned to the created One Touch Voice policy to re-cache their policy information. Clicking the **Notify** button causes all QoS-enabled switches to flush their policy tables and reload policies from the LDAP repository, which is very expensive in terms of switch resources and time. If any One Touch Data or Expert mode policy has already been defined, the switch(es) to which the policy is assigned will re-cache its policy table also. It is recommended that you verify all policies that you have created and apply them at the same time to minimize switch downtime.

**Note:** If you have entered a subnet incorrectly or in error, delete it by selecting the subnet in the **One Touch voice IPs** table and clicking the **Delete** button. If you delete a subnet that was previously applied to the network, the policies for that subnet are deleted from LDAP when the **Save** button is clicked.

## Editing One Touch Policies

Follow the steps below to edit One Touch Voice layer 3 (IP) policies.

1. Select the desired policy from the **One Touch Voice IPs** table.
2. Click the **Edit** button. The **Edit One Touch Voice IP** panel appears.
3. Make the necessary change in the **Subnet Mask** field.

**Note:** The **Subnet IP** field cannot be changed. If you want to change the **Subnet IP**, you have to delete and recreate the policy.

4. After making the changes, click the **OK** button. The edited policy appears in the **One Touch Voice IPs** table as "Unsaved".
5. Click the **Save** button to apply the policy to the LDAP repository. Repeat the same steps to create additional policies.

## Verifying the Notify Operation

When the information entered in the **One Touch Voice** tab is successfully saved to the LDAP repository, a "One Touch Voice Policies Save Complete" message is displayed. The success or failure of the LDAP save operation is also reported in the status panel, as shown below.

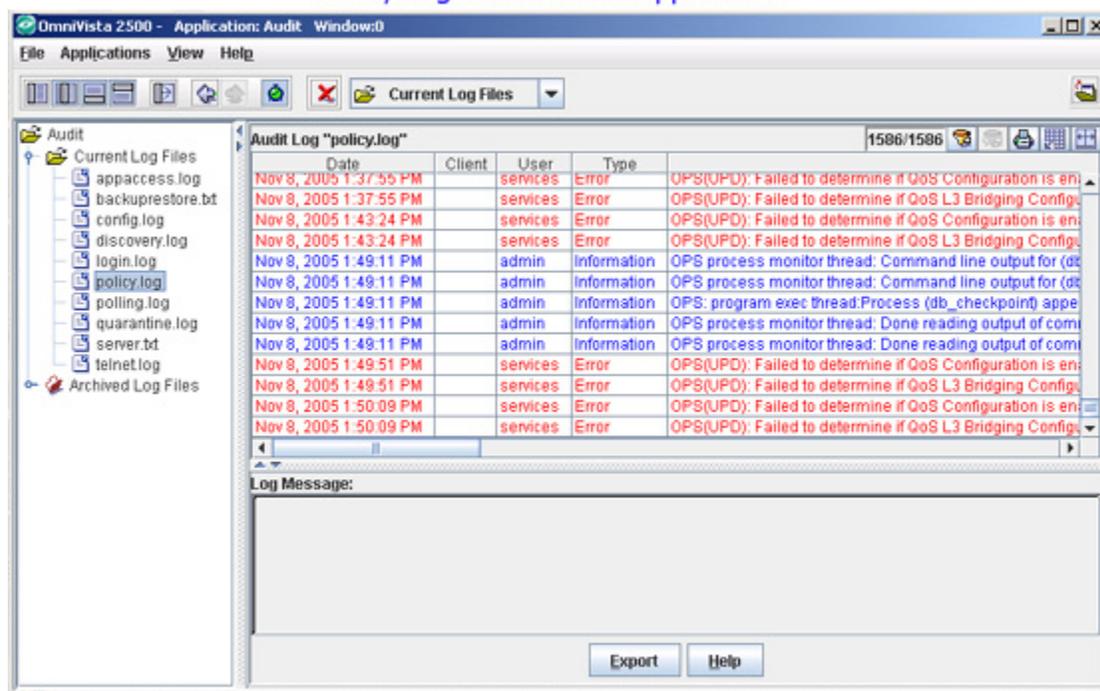
Date	Application	Type	Message
Tue Nov 08 14:23:33 PST 2005	PolicyView QoS	Info	Read com.alcatel.ov1.policies.
Tue Nov 08 14:27:33 PST 2005	PolicyView QoS	Info	Saving policies
Tue Nov 08 14:27:33 PST 2005	PolicyView QoS	Info	Save complete

When the **Notify** button is clicked, an SNMP message is sent to each QoS-qualified device in the list, informing that the information in the LDAP repository has changed and commanding the devices to update their cached policies with current information from the LDAP repository. (Note that a qualified device is a device that can support the PolicyView QoS application and provisioned QoS. AOS devices are qualified devices. XOS devices are qualified devices if their flash file systems contain the policy.img file and the qos.img file.) The success or failure of the "Notify" operation is reported in the Status panel.

In addition to the Status panel, the success or failure of the policy re-cache operation for each switch is reported in the policy.log file, including an indication of any error that may have occurred (shown below). Note that the re-cache operation for each switch occurs in a separate thread and may take some time. Be sure to check the policy.log file for the re-cache status of the "Notify" operation.

Note that any errors that occur will also be reported in the file server.txt, which can be viewed from the Audit application.

## Policy Log in the Audit Application



### Example of an One Touch Voice IP Policy Creation

Let's say we are creating One Touch Voice MAC policy and One Touch Voice IP policy simultaneously and the following two IP subnets are entered into the **One Touch Voice IPs** table:

**155.144.32.43** with subnet mask **255.255.255.0**

**155.144.35.76** with subnet mask **255.255.0.0**

When saved, the following policies are created and written to the LDAP repository:

#### **OneTouchVR\$AlcatelVoIPMacDstA**

Condition specifies traffic flowing to destination MAC address 00:80:9F:3A:\*\*:\*\*

Action specifies platinum QoS for this traffic

#### **OneTouchVR\$AlcatelVoIPMacDstB**

Condition specifies traffic flowing to destination MAC address 00:80:9F:3B:\*\*:\*\*

Action specifies platinum QoS for this traffic

#### **OneTouchVR\$AlcatelVoIPMacDstC**

Condition specifies traffic flowing to destination MAC address 00:80:9F:3C:\*\*:\*\*

Action specifies platinum QoS for this traffic

#### **OneTouchVR\$AlcatelVoIPMacDstD**

Condition specifies traffic flowing to destination MAC address 00:80:9F:3D:\*\*:\*\*

Action specifies platinum QoS for this traffic

#### **OneTouchVR\$AlcatelVoIPMacDstE**

Condition specifies traffic flowing to destination MAC address 00:80:9F:3E:\*\*:\*\*

Action specifies platinum QoS for this traffic

**OneTouchVR\$AlcatelVoIPMacDstF**

Condition specifies traffic flowing to destination MAC address 00:80:9F:3F:\*.\*\*.\*

Action specifies platinum QoS for this traffic

**OneTouchVR\$AlcatelVoIPAirSpD**

Condition specifies traffic flowing to destination MAC address 00:0B:85:00:\*.\*\*.\*

Action specifies platinum QoS for this traffic

**OneTouchVR\$D155.144.32.1**

Condition specifies traffic flowing to destination IP address range 155.144.32.1 - 155.144.32.254

Action specifies platinum QoS for this traffic

**OneTouchVR\$S155.144.32.1**

Condition specifies traffic originating from source IP address range 155.144.32.1 - 155.144.32.254

Action specifies platinum QoS for this traffic

**OneTouchVR\$D155.144.35.76**

Condition specifies traffic flowing to destination IP address range 155.144.00.1 - 155.144.255.254

Action specifies platinum QoS for this traffic

**OneTouchVR\$S155.144.35.76**

Condition specifies traffic originating from source IP address range 155.144.00.1 - 155.144.255.254

Action specifies platinum QoS for this traffic

Please note that names beginning with "OneTouchVR" are the names used for the policies in the LDAP repository. Within the PolicyView QoS application, all One Touch Voice rules are referred to by the generic composite name **OneTouchVoiceRule**, no matter how many individual One Touch Voice rules have been written to the LDAP repository. Individual LDAP rules for One Touch Voice rules can be viewed in the Expert Mode window.

## Deleting One Touch Voice Policies

### Deleting All One Touch Voice Policies for Alcatel Voice Devices

To delete all Layer 2 (MAC) policies for Alcatel voice devices, uncheck the checkbox at the top of the window and click the **Save** button.

- All One Touch Voice Layer 2 policies are removed from the LDAP repository.
- All One Touch Voice Layer 2 policies are removed from switch attributes in the LDAP "role" objects.
- A confirmation message is displayed when the LDAP repository has been updated. The success of the LDAP "Save" operation is also reported in the policy.log file.

When the **Notify** button is clicked, an SNMP message is sent to the each QoS-qualified device in the list, informing that the information in the LDAP repository has changed and commanding the devices to update their cached policies with the current information from the LDAP repository.

The success or failure of the policy re-cache operation for each switch is reported in the policy.log file in the Audit application, including an indication of any error that may have

occurred. Note that the re-cache operation for each switch occurs in a separate thread and may take some time. Be sure to check the policy.log file for the re-cache status of each switch.

### Deleting One Touch Voice Policies for IP Subnets

Follow the steps below to delete One Touch Voice policies for individual IP Phone subnets.

1. Select the desired subnet in the **One Touch Voice IPs** table and click the **Delete** button. The policy status changes to "Unsaved Delete." Repeat this step to delete additional subnets.
2. Click the **Save** button to apply the changes to the LDAP repository.
3. All One Touch Voice policies for the subnets you deleted are removed from the LDAP repository (both Layer 2 and Layer 3 Policies), and all qualified devices in the list of All Discovered Devices are commanded to re-cache their Policies from the LDAP repository by clicking the **Notify** button.

**Note:** Clicking the **Notify** button causes all QoS-enabled switches to flush their policy tables and reload policies from the LDAP repository, which is very expensive in terms of switch resources and time. If any One Touch Data or Expert mode policy has been defined, the switch(es) to which the policy was assigned will also re-cache its policy tables.

### Icons in the One Touch Voice IPs Table

Status icons in the **One Touch Voice IPs** table are color coded. The **Policy Status** column displays yellow, green, or red LEDs depending on the status.

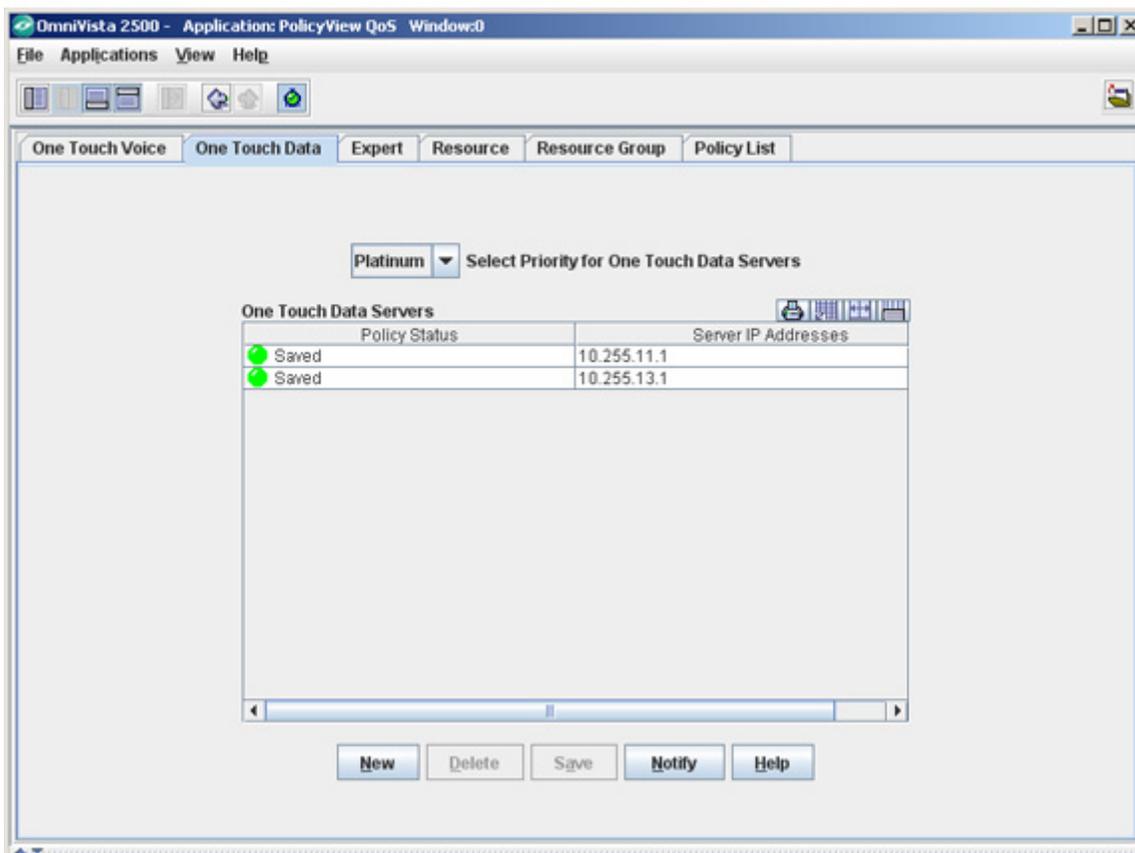
- A yellow LED indicates that the policies for the subnet are in a "Unsaved" state, which means that the changes have not been propagated to the LDAP repository.
- A green LED indicates that the policy has been successfully written to the LDAP repository.
- A red LED indicates that an error condition has made it impossible to write the One Touch Voice policy to the LDAP repository.

### One Touch Data Tab

The **One Touch Data** tab (shown below) enables you to easily assign the desired quality of service (Platinum, Gold, Silver, or Bronze) to all data traffic flowing to, and originating from, specific data servers. Two policies are created for each server: one for data originating from the server, and one for data transmitted to the server. All policies created are applied to all QoS-enabled devices in the list of All Discovered Devices.

**Note:** OmniSwitch 6800/7000/8000/9000 series switches support the 802.1 priority. However, 6600 series switches and some current XOS hardware and firmware releases do not. Please refer to the switch release notes for information on the specific QoS functions available on various current platforms and combinations of hardware/firmware.

## One Touch Data Tab

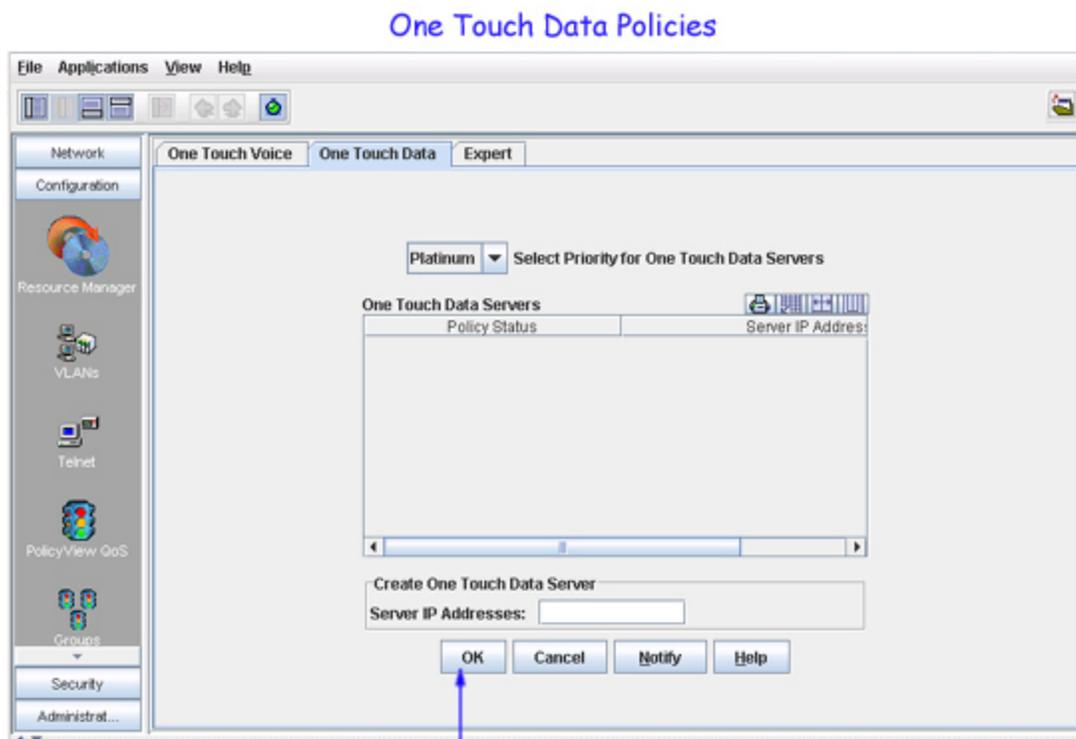


## One Touch Data Policies

When you create a One Touch Data policy, the priority you select (Platinum, Gold, Silver, or Bronze) is assigned to all servers in the **One Touch Data Servers** table. (Use the Expert mode if you need to assign a different priority to any server.)

- **Platinum** - provides the highest quality of service (and maps to a firmware priority of 7)
- **Gold** - provides the next-highest quality of service (and maps to a firmware priority of 5)
- **Silver** - provides the next-highest quality of service (and maps to a firmware priority of 3)
- **Bronze** - provides the same quality of service as best effort (and maps to a firmware priority of 1)

Two policies are created for each server. One policy includes a condition specifying a source IP address of the server and the second policy includes a condition specifying a destination IP address of the server. Both policies include an action specifying the selected priority QoS. Follow the steps below to create One Touch Data policies.



Enter the Server IP address, then click OK. Click Save to save the policy.

1. Click the **New** button. The **Create One Touch Data Server** panel appears (as shown above).
2. Enter the server IP address in the **Server IP Addresses** field. (Note that the \* wildcard character is not allowed in server addresses.)
3. Click the **OK** button. The Create One Data Server panel disappears, the server appears in the **One Touch Data Servers** table as "Unsaved", and the **Save** button is enabled. Repeat steps 1 - 3 to add additional servers.
4. Click the **Save** button to save the policy to the LDAP repository.
5. Click the **Notify** button to notify the selected switches in the list to re-cache their policy information.

Clicking the **Notify** button causes the selected QoS-enabled switches to flush their policy tables and reload policies from the LDAP repository, which is very expensive in terms of switch resources and time. If any One Touch Voice or Expert mode policy has already been defined, the switch(es) to which the policy is assigned will also re-cache its policy tables. It is recommended that you verify all policies that you have created and apply them at the same time to minimize switch downtime.

**Note:** If you have entered a Server IP address incorrectly or in error, delete it by selecting the Server IP address in the **One Touch Data Servers** table and clicking the **Delete** button. If you delete a server that was previously applied to the network, the policies for that server are deleted from LDAP when the **Save** button is clicked.

### Applying the Policy

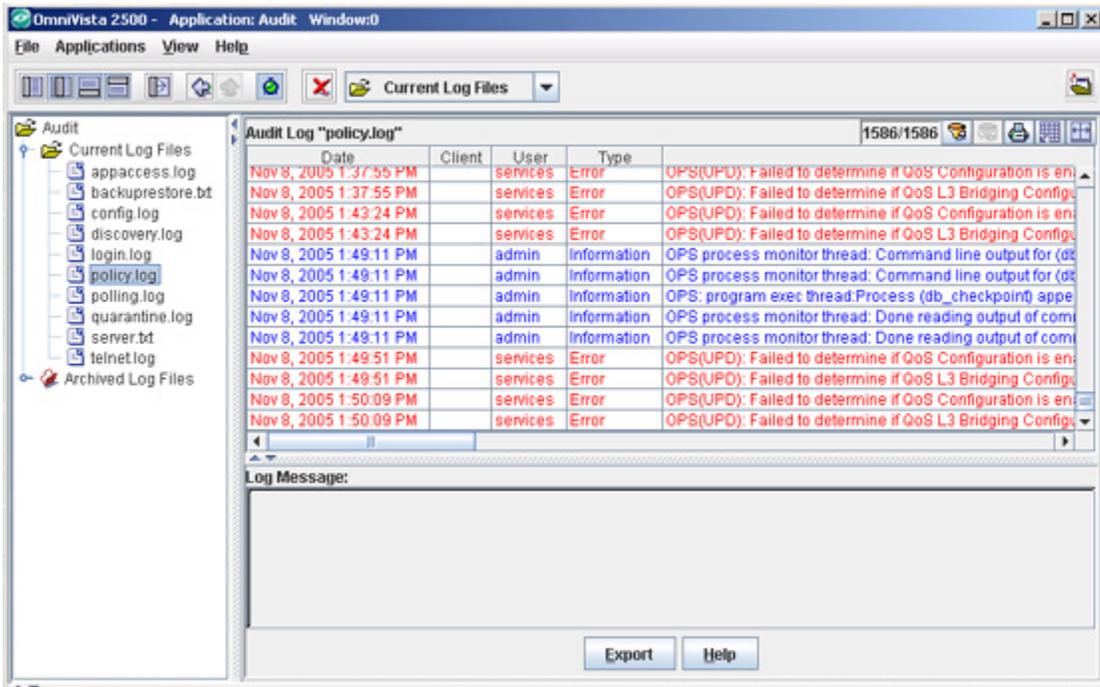
When the information entered in the **One Touch Data** tab is successfully saved to the LDAP repository, a "One Touch Data Policies Save Complete" message is displayed. The success or failure of the LDAP operation is also reported in the Status panel, as shown below.

Date	Application	Type	Message
Tue Nov 08 14:23:33 PST 2005	PolicyView QoS	Info	Read com.alcatel.ov1.policies.
Tue Nov 08 14:27:33 PST 2005	PolicyView QoS	Info	Saving policies
Tue Nov 08 14:27:33 PST 2005	PolicyView QoS	Info	Save complete

When the **Notify** button is clicked, an SNMP message is sent to each QoS-qualified device in the list of All Discovered Devices, informing that the information in the LDAP repository has changed and commanding the devices to update their cached policies with the current information from the LDAP repository. (Note that a qualified device is a device that can support the PolicyView QoS application and provisioned QoS. The OmniSwitch 6800/7000/8000/9000 switches are qualified devices. XOS devices are qualified devices if their flash file systems contain the policy.img file and the qos.img file.)

In addition to the Status panel, the success or failure of the policy re-cache operation for each switch is reported in the policy.log file, including an indication of any error that may have occurred (shown below). Note that the re-cache operation for each switch occurs in a separate thread and may take some time. Be sure to check the policy.log file for the re-cache status of the "Notify" operation.

### Policy Log in the Audit Application



Note that any errors that occur will also be reported in the file server.txt, which can be viewed from the Audit application.

### Example of an Apply Policy (or Update Policy) Operation

Let's say **Platinum** was selected as the priority and the following two server IP addresses were entered in the **One Touch Data Servers** table:

**164.178.32.107**

**164.178.33.51**

When applied, the following policies are created and written to the LDAP repository:

#### **OneTouchDR\$S164.178.32.107**

Condition specifies traffic originating from source IP address 164.178.32.107

Action specifies Platinum QoS for this traffic

#### **OneTouchDR\$D164.178.32.107**

Condition specifies traffic transmitted to destination IP address 164.178.32.107

Action specifies Platinum QoS for this traffic

#### **OneTouchDR\$S164.178.33.51**

Condition specifies traffic originating from source IP address 164.178.33.51

Action specifies Platinum QoS for this traffic

#### **OneTouchDR\$D164.178.33.51**

Condition specifies traffic transmitted to destination IP address 164.178.33.51

Action specifies Platinum QoS for this traffic

Please note that the names beginning with "OneTouchDR" are the names used for the policies in the LDAP repository. Within the PolicyView QoS application, all One Touch Data policies are referred to by the generic composite name **OneTouchDR**, no matter how many individual One Touch Data policies have been written to the LDAP repository. One Touch Data rules that have been created automatically by PolicyView can be viewed in the Expert mode window.

**Note:** This naming convention is different from previous releases. Installation of updated PolicyView software will update and migrate the names from previous installations.

### Deleting One Touch Data Policies

Follow the steps below to delete One Touch Data policies for individual data servers.

1. Select the desired server in the **One Touch Data Servers** table and click the **Delete** button. The policy status changes to "Unsaved Delete". Repeat this step to delete additional servers.
2. Click the **Save** button to apply the changes to the LDAP repository.

When you click the **Save** button:

- All One Touch Data policies for the servers you selected are removed from the LDAP repository.
- All One Touch Data policies for the servers you selected are removed from switch attributes in the LDAP "role" objects.
- The servers are removed from the **One Touch Data Servers** table.
- A confirmation message is displayed when the LDAP repository has been successfully updated. The success of the LDAP "Save" operation is also reported in the policy.log file.

When the **Notify** button is clicked, an SNMP message is sent to each QoS-qualified device in the list of All Discovered Devices, informing that the information in the LDAP repository has changed and commanding the devices to update their cached policies with the current information from the LDAP repository.

The success or failure of the policy re-cache operation for each switch is reported in the Status panel, including an indication of any error that may have occurred. Note that the re-cache operation for each switch occurs in a separate thread and may take some time. Be sure to check the policy.log file for the re-cache status of each switch.

### Icons in the One Touch Data Servers Table

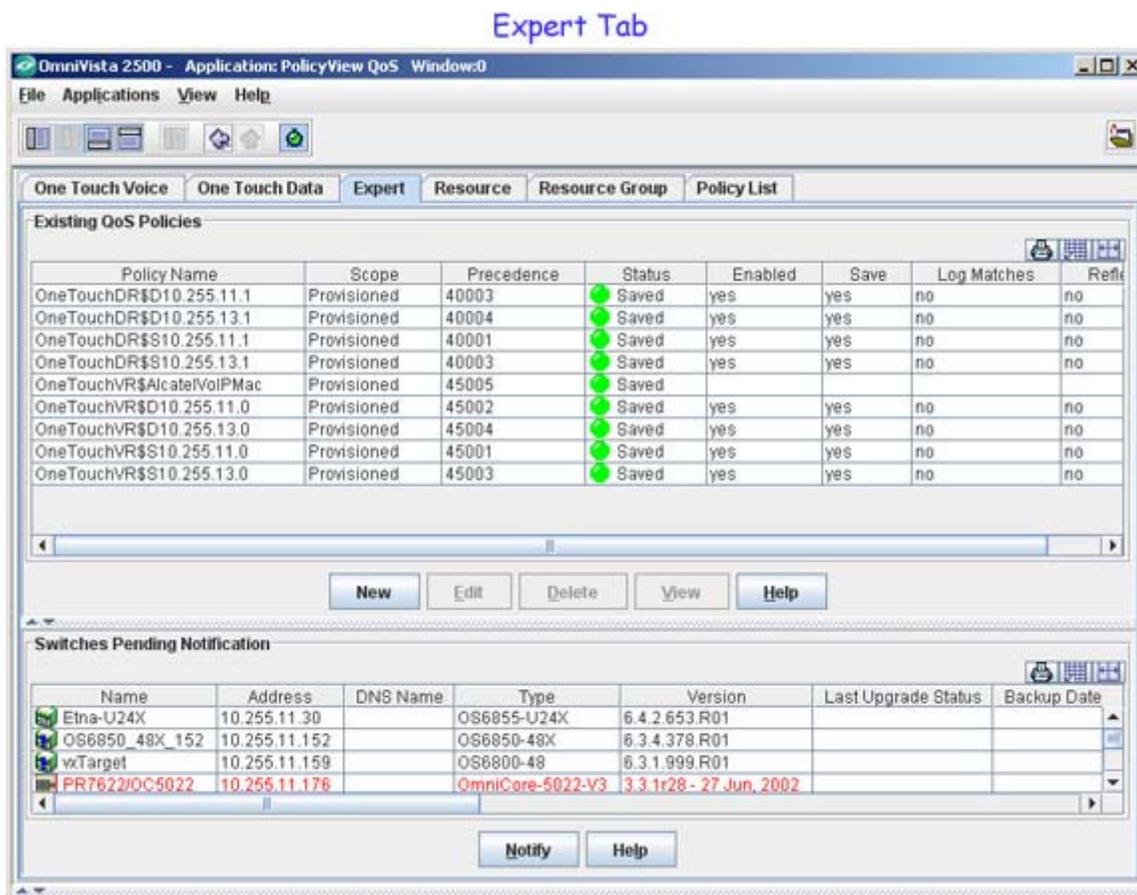
Server icons in the **One Touch Data Servers** table are color coded. The **Policy Status** column displays yellow, green, or red LEDs depending on the status.

- A yellow LED indicates that the policies for the subnet are in a "unsaved" state, which means that the changes have not been propagated to the LDAP repository.
- A green LED indicates that the policy has been successfully written to the LDAP repository.
- A red LED indicates that an error condition has made it impossible to write the One Touch Data Server policy to the LDAP repository.

### Expert Tab

The **Expert** tab (shown below) is used to create, edit, delete, and view custom QoS policies. All current policies are listed in the **Existing QoS Policies** table. To edit, delete, or view a policy, select the policy in the table, and then click the corresponding button at the bottom of the Existing QoS Policies panel. To create a custom policy, click the **New** button to open the PolicyView QoS Expert wizard.

**Note:** One Touch policies cannot be modified or deleted in the Expert mode. To modify or delete One Touch Voice or Data policies, use the One Touch Voice tab or the One Touch Data tab, respectively.



**Note:** The Reflexive attribute cannot be configured for PolicyView QoS policies. However, this attribute can be configured for SecureView ACL policies.

The **Switches Pending Notification** table contains a list of switches whose assigned policies and/or LDAP role configurations have changed as a result of a policy configuration, but have not been notified to re-cache. Click the **Notify** button to notify these devices to re-cache their configurations.

**Note:** The "Notification" operation is expensive in terms of switch resources. Click [here](#) for more details on applying policies to the network.

## Creating Policies in Expert Mode

The PolicyView QoS Expert wizard is used to create a new policy. Creating a new policy consists of the following basic steps:

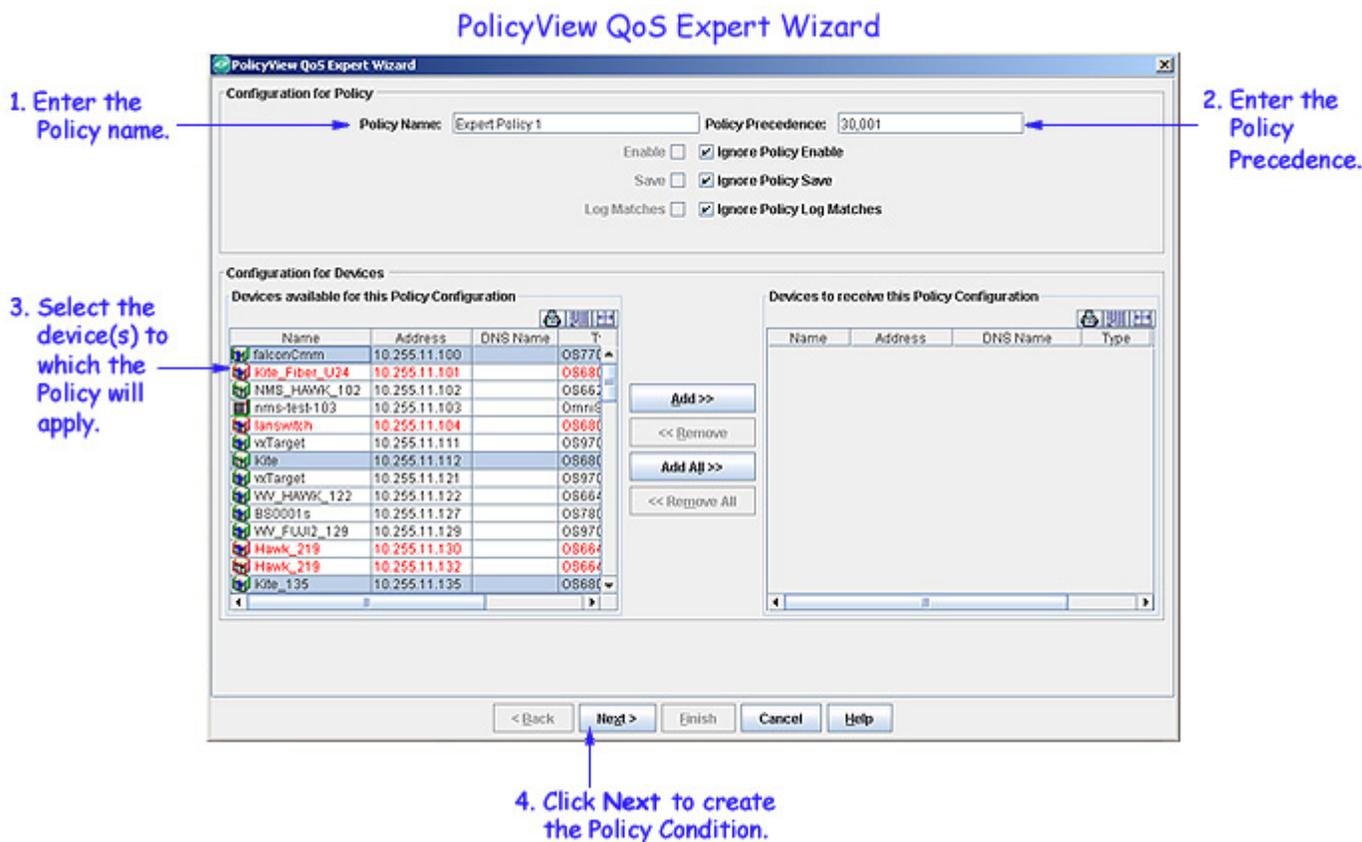
- Creating a Policy:
  - Enter a name for the policy.
  - Set the Policy Precedence value.
  - Specify the devices to which the policy will apply.
- Creating a Policy Condition that specifies the conditions that must be true before traffic will be allowed to flow.

- Creating a Policy Action that specifies parameters for the traffic that will flow.
- Applying the Policy in the network.

**Note:** You cannot create, delete, or edit a One Touch Policy in the Expert mode. You must use the One Touch Voice or One Touch Data tab to create, delete, or edit a One Touch policy.

## Creating a Policy

To start creating a custom QoS policy, go to the **Expert** tab and click the **New** button. The **PolicyView QoS Expert Wizard** window appears. In this screen you can enter the name of the policy, set the policy precedence, and specify the devices to which the policy will apply.



Follow the steps below to create a new policy.

1. Click the **New** button in the **Expert** tab. The **PolicyView Qos Expert Wizard** window appears
2. Enter a policy name in the **Policy Name** field.
3. Enter a **Policy Precedence** (range = 30001 - 500000) in the **Policy Precedence** field.
4. To select the Policy Enable parameter, uncheck the **Ignore Policy Enable** checkbox and then check the **Enable** checkbox. Follow the same steps to select the Save, and the Log Matches parameter.

**Note:** By default the policies are not enabled, saved, or log matched.

5. Select the device(s) to which you want to apply the policy, and then click the **Add** button.
6. Click the **Next** button to create the policy condition.

**Note:** In the Expert mode, the precedence field is pre-filled with the lowest unused precedence value for expert mode policies.

## Creating a Policy Condition

The Policy Condition panel contains tabs and parameters that enable you to create a policy condition. A policy condition enables you to specify one or more conditions that must be true before traffic is allowed to flow. Each tab in the Policy Condition panel enables you to specify a different type of condition for the traffic flow. A brief description of each tab is provided below. Click the hyperlink for each condition for detailed configuration steps.

**Note:** When creating conditions, do not click the **Next** button until you have completed all desired tabs in the Policy Condition panel.

### Expert Wizard Conditions Window

- **L1 Interfaces** - Create a condition that applies the policy to traffic flowing from a specific source interface type or to traffic flowing to a specific destination interface type.
- **L2 MACs** - Create a condition that applies the policy to traffic originating from a MAC address/group or to traffic flowing to a MAC address/group. (Note that any MAC address may contain wildcard characters).
- **L2 VLANs** - Create a condition that applies the policy to traffic flowing from a source VLAN to a destination VLAN, or to traffic flowing from one source VLAN to any

destination VLAN, or to traffic flowing from any source VLAN to one destination VLAN.

- **L2 802.1P** - Create a condition that applies the policy to traffic with a specified 802.1 priority value.
- **L3 IPs** - Create a condition that applies the policy to traffic originating from an IP address/network group or to traffic flowing to an IP address/network group. (Note that any IP address can be masked).
- **L3 DSCP/TOS** - Create a condition that applies the policy to traffic with a specified value in either the DSCP (Differentiated Services Code Point) byte or in the IP TOS (IP Type of Service) byte. Both DSCP and IP TOS are mechanisms used to convey QoS information in the IP header of frames.
- **L4 Services** - Create a condition that applies the policy to traffic flowing between two TCP or UDP ports, or to all traffic originating from a TCP or UDP port, or to all traffic flowing to a TCP or UDP port. You can also create a condition using an existing service/service group.
- **Validity Period** - Specify the dates and times when you wish the policy to be valid (that is, when you wish the policy to be enforced).

**Note:** The OmniSwitch 6800/7000/8000/9000 series switches support 802.1 priority, DSCP, and TOS. However, 6600 series switches and some current XOS hardware and firmware releases do not. Please refer to the switch Release Notes for information on the specific QoS functions available on various current platforms and combinations of hardware/firmware.

## The Interfaces Tab

The **L1 Interfaces** tab, shown below, enables you to create a condition that restricts the policy to traffic flowing from a source interface to a destination interface, or to traffic flowing from a source interface to any destination interface, or to traffic flowing from any source interface to a destination interface. Follow the steps below to create an interface condition.

## Interfaces Tab

The screenshot shows the 'Interfaces Tab' of the 'PolicyView QoS Expert Wizard'. The window title is 'PolicyView QoS Expert Wizard' and the subtitle is 'Set Conditions for Policy Expert Policy 1'. The 'L1 Interfaces' tab is selected, showing options for Source and Destination Interface Type, each with a dropdown menu and a checked checkbox labeled 'Ignore Source/Destination Interface Type in determining Policy Condition'. Navigation buttons at the bottom include '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

### Creating an Interface Type Condition

Create a source and/or destination interface type condition as described below. Do not click the Next button until you have completed all desired tabs in the Policy Condition panel.

#### Source

1. Uncheck the **Ignore Source Interface Type in determining Policy Condition** checkbox. The Source **Interface Type** drop-down list is activated.
2. Select the interface type from the Source **Interface Type** drop-down list.

Selecting a source interface type, restricts the policy to traffic that flow from that interface only. If you leave the field blank or check the **Ignore Source Interface Type in determining Policy Condition** checkbox, you are effectively stating that the source interface type of traffic is not a criterion for the policy.

#### Destination

1. Uncheck the **Ignore Destination Interface Type in determining Policy Condition** checkbox. The Destination **Interface Type** drop-down list is activated.
2. Select the interface type from the Destination **Interface Type** in the drop-down list.

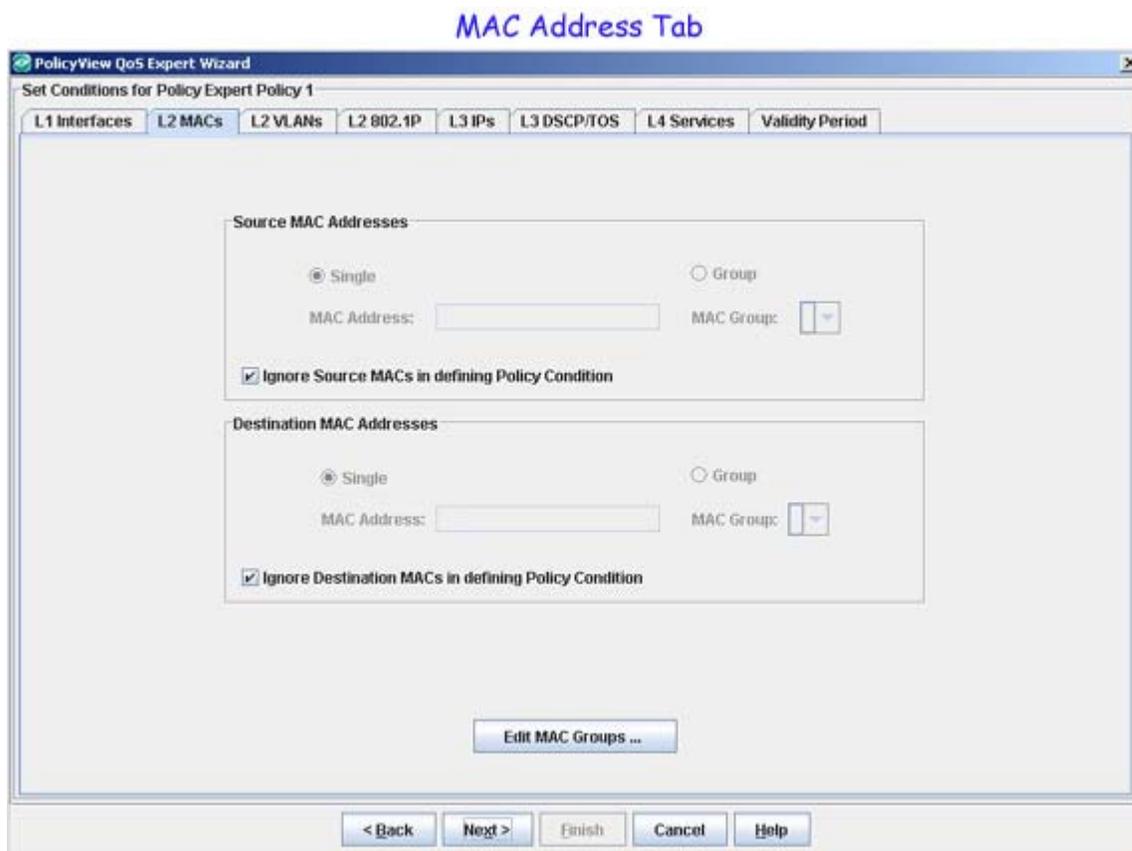
Selecting a destination interface type, restricts the policy to traffic that flows to this interface type only. If you leave the field blank or check the **Ignore Destination Interface Type in**

**determining Policy Condition** checkbox, you are effectively stating that the destination interface type of traffic is not a criterion for the policy.

## The MACs Tab

The **L2 MACs** tab, shown below, enables you to create a condition that applies the policy to traffic originating from, or flowing to, a MAC address/group. Note that Layer 2 conditions (conditions that specify MAC addresses) are "lost" when traffic passes through a router. For this reason, it may be advisable to specify other types of conditions (such as a Layer 3 condition, which specifies IP addresses) when traffic is expected to travel more than one router hop. Using the MAC tab, you can create the following MAC conditions:

- Source MAC address
- Source MAC group
- Destination MAC address
- Destination MAC group



Conditions that specify both a source and a destination MAC address may be rejected by some switch platforms as invalid. However, if you wish to create policies for both source and destination traffic, you can create one policy for the source traffic and a second policy for the destination traffic.

MAC addresses may contain the wildcard character \*. However, one \* character must be entered for each individual hex digit in the MAC address: for example, **00435C:\*\*\*\*\***, not **00435C:\***.

The following MAC address ranges are assigned to Alcatel voice devices and Alcatel IP phones. You can create conditions specifying these address ranges using the MAC Address tab.

- Voice Devices
  - 00809F3A0000 - 00809F3AFFFF
  - 00809F3B0000 - 00809F3BFFFF
  - 00809F3C0000 - 00809F3CFFFF
- IP phones
  - 00809F3D0000 - 00809F3DFFFF
- Multi-Media Devices
  - 00809F3E0000 - 00809F3EFFFF
  - 00809F3F0000 - 00809F3FFFFF

### Creating a MAC Address Condition

Create a source and/or destination MAC address/group condition as described below. Do not click the **Next** button until you have completed all desired tabs in the Policy Condition panel.

#### Source MAC Address

1. Uncheck the **Ignore Source MACs in defining Policy Condition** checkbox.
2. The **Single** radio button is selected and the source **MAC Address** field is activated.
3. Enter the source MAC address in the **MAC Address** field.

Entering a source MAC address, restricts the policy to traffic that originates from this address only. If you check the **Ignore Source MACs in defining Policy Condition** checkbox, you are effectively stating that the source MAC address/group of traffic is not a criterion for the policy.

#### Source MAC Group

1. Uncheck the **Ignore Source MACs in defining Policy Condition** checkbox.
2. Click the **Group** radio button. The destination **MAC Group** drop-down list is activated.
3. Select the group from the **MAC Group** drop-down list. If you want to create, edit, or delete a MAC group click the **Edit MAC Groups...** button.

Selecting a source MAC group, restricts the policy to traffic that originates from this MAC group only. If you check the **Ignore Source MACs in defining Policy Condition** checkbox, you are effectively stating that the source MAC address/group of traffic is not a criterion for the policy.

#### Destination MAC Address

1. Uncheck the **Ignore Destination MACs in defining Policy Condition** checkbox.
2. Click the **Single** radio button. The destination **MAC Address** field is activated. By default, the **Single** radio button is selected.
3. Enter the destination MAC address in the **MAC Address** field.

Entering a destination MAC address, restricts the policy to traffic that flows to this address only. If you check the **Ignore Destination MACs in defining Policy Condition** checkbox, you are

effectively stating that the destination MAC address/group of traffic is not a criterion for the policy.

### Destination MAC Group

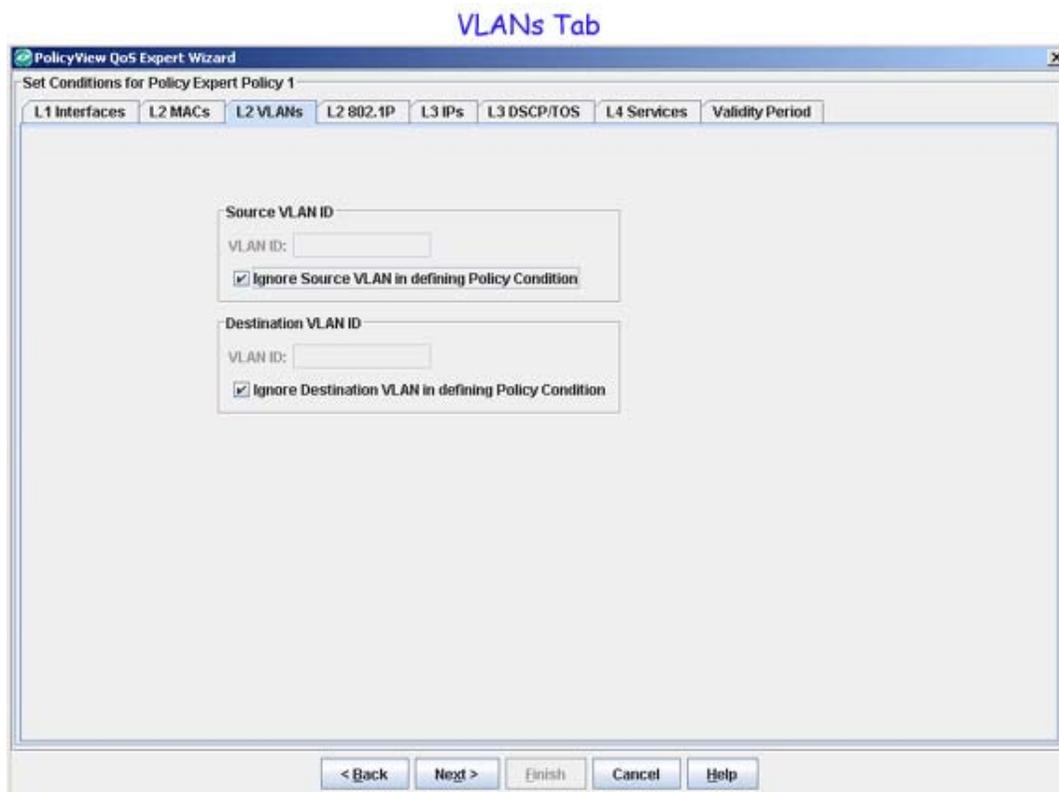
1. Uncheck the **Ignore Destination MACs in defining Policy Condition** checkbox.
2. Click the **Group** radio button. The destination **MAC Group** drop-down list is activated.
3. Select the group from the **MAC Group** drop-down list. If you want to create, edit, or delete a MAC group click the **Edit MAC Groups...** button.

Selecting a destination MAC group, restricts the policy to traffic that flows to this address only. If you check the **Ignore Destination MACs in defining Policy Condition** checkbox, you are effectively stating that the destination MAC address/group of traffic is not a criterion for the policy.

**Note:** When creating a MAC condition for a **NAT** action you must specify a MAC group in the condition. NAT will only work when both the condition and the action specify groups. To create a "one-to-many" condition and action, create a MAC group with a single entry for the condition.

### The VLANs Tab

The **L2 VLANs** tab, shown below, enables you to create a condition that restricts the new policy to traffic flowing from a source VLAN to a destination VLAN, or to traffic flowing from a source VLAN to any destination VLAN, or to traffic flowing from any source VLAN to a destination VLAN. Follow the steps below to [create a VLAN condition](#).



### Creating a VLAN Condition

Create a VLAN condition as described below. Do not click the **Next** button until you have completed all the desired tabs on the Policy Condition panel.

#### Source

1. Uncheck the **Ignore Source VLAN in defining Policy Condition** checkbox. The source **VLAN ID** field is enabled.

2. Enter the desired VLAN ID.

Entering a VLAN ID restricts the policy rule to traffic originating from that VLAN only. If you leave the field blank or check the **Ignore Source VLAN in defining Policy Condition** checkbox, you are effectively stating that the source VLAN ID of traffic is not a criterion for the policy.

#### Destination

1. Uncheck the **Ignore Destination VLAN in defining Policy Condition** checkbox. The destination **VLAN ID** field is enabled.

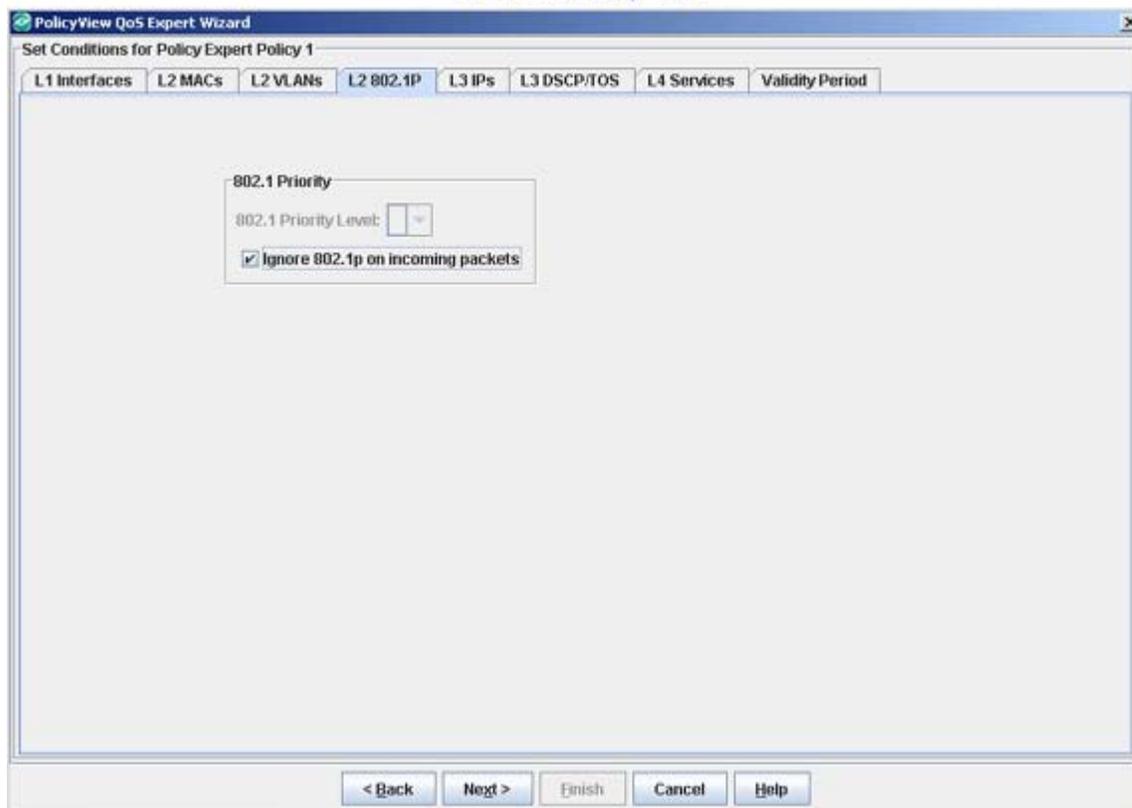
2. Enter the desired VLAN ID.

Entering a VLAN ID restricts the policy rule to traffic flowing to that VLAN only. If you leave the field blank or check the **Ignore Destination VLAN in defining Policy Condition** checkbox, you are effectively stating that the destination VLAN ID of traffic is not a criterion for the policy.

### The 802.1P Tab

The **L2 802.1P** tab, shown below, enables you to create a condition that applies the policy to incoming traffic that has a specified 802.1 priority value in the header of the frame. 802.1p is the IEEE extension of 802.1d and is a standard for the use of MAC-layer bridges in filtering and expediting multicast traffic. 802.1p prioritizes traffic through the insertion of a three-bit priority value into the header of the frame. An 802.1 priority value of 7 provides the highest priority, and an 802.1 priority value of 0 provides the lowest priority. Follow the steps below to create an 802.1 priority condition.

## 802.1 Priority Tab



**Note:** OmniSwitch 6800/7000/8000/9000 series switches support the 802.1 priority. However, 6600 series switches and some current XOS hardware and firmware releases do not. Please refer to the Switch Release Notes for information on the specific QoS functions available on various current platforms and combinations of hardware/firmware.

### Creating an 802.1 Priority Condition

Create an 802.1 Priority condition as described below. Do not click the **Next** button until you have completed all the desired tabs in the Policy Condition panel.

1. Uncheck the **Ignore 802.1p on incoming packets** checkbox. The **802.1 Priority Level** field is enabled. Checking the **Ignore 802.1p on incoming packets** checkbox means that you do not want the 802.1 Priority value of incoming traffic to be a criterion for the policy.
2. Set the **802.1 Priority Level** field to the desired priority value (0-7). This will restrict the policy to incoming traffic that has that 802.1 Priority value in the frame header. A value of 7 provides the highest priority and a value of 0 provides the lowest priority.

**Note:** If an 802.1p value is specified, a DSCP value or a ToS value may not be specified. This restriction does not apply to the OmniSwitch 6800 series switches.

## The IPs Tab

The **L3 IPs** tab, shown below, enables you to create a condition that applies the policy to all traffic originating from, or flowing to, an IP address/network group. Any IP address can be masked. Note that the conditions that specify both a source and a destination IP address/network group will be rejected by the switch as invalid. However, if you wish to create policies for both source and destination traffic, you can create one policy for the source traffic and the second policy for the destination traffic. Using the IPs tab, you can create the following IP conditions:

- Source IP address
- Source network group
- Destination IP address
- Destination network group

### IP Address Tab

The screenshot shows the 'PolicyView QoS Expert Wizard' window, specifically the 'L3 IPs' tab. The window title is 'Set Conditions for Policy Expert Mode Policy 3'. The 'L3 IPs' tab is selected among other tabs: L1 Interfaces, L2 MACs, L2 VLANs, L2 802.1P, L3 DSCP/TOS, L4 Services, and Validity Period. The 'Source IP Addresses' section has four radio buttons: 'Single' (selected), 'Shorthand Mask', 'Subnet Mask', and 'Group'. Below these are fields for 'IP Address', 'IP Subnet Mask', and 'Network Group'. A checkbox labeled 'Ignore Source IPs in defining Policy Condition' is checked. The 'Destination IP Addresses' section has the same layout with 'Single' selected and its 'Ignore Destination IPs in defining Policy Condition' checkbox checked. At the bottom, there is an 'Edit Network Groups ...' button and a navigation bar with '< Back', 'Next >', 'Finish', 'Cancel', and 'Help' buttons.

### Creating an IP Address Condition

Create a source and/or destination IP address/network group condition as described below. Do not click the **Next** button until you have completed all desired tabs in the Policy Condition panel.

#### Source IP Address

1. Uncheck the **Ignore Source IPs in defining Policy Condition** checkbox.
2. The **Single** radio button is selected and the source **IP Address** field is activated.

3. Enter the source IP address in the **IP Address** field.
4. Click either the **Shorthand Mask** or **Subnet Mask** radio button. If you are using a shorthand mask, set the shorthand mask drop-down list to the desired value. If you are using a full subnet mask, enter the mask in the **IP Subnet Mask** field.

**Note:** The \* wildcard character is not allowed in IP addresses.

Entering an IP address restricts the policy rule to traffic originating from that IP address (or masked IP address). If you leave the field blank or check the **Ignore Source IPs in defining Policy Condition** checkbox, you are effectively stating that the source IP address/network group of traffic is not a criterion for the policy.

### Source Network Group

1. Uncheck the **Ignore Source IPs in defining Policy Condition** checkbox.
2. Click the **Group** radio button, and then select the group from the **Network Group** drop-down list. If you want to create, edit, or delete a group, click the **Edit Network Groups...** button.

Selecting a network group restricts the policy rule to traffic originating from that network group. If you leave the field blank or check the **Ignore Source IPs in defining Policy Condition** checkbox, you are effectively stating that the source IP address/network group of traffic is not a criterion for the policy.

### Destination IP Address

1. Uncheck the **Ignore Destination IPs in defining Policy Condition** checkbox.
2. The **Single** radio button is selected and the source **IP Address** field is activated.
3. Enter the source IP address in the **IP Address** field.
4. Click either the **Shorthand Mask** or **Subnet Mask** radio button. If you are using a shorthand mask, set the shorthand mask drop-down field to the desired value. If you are using a full subnet mask, enter the mask in the **IP Subnet Mask** field.

**Note:** The \* wildcard character is not allowed in IP addresses.

Entering an IP address restricts the policy rule to traffic flowing to that IP address (or masked IP address). If you leave the field blank or check the **Ignore Destination IPs in defining Policy Condition** checkbox, you are effectively stating that the destination IP address/network group of traffic is not a criterion for the policy.

### Destination Network Group

1. Uncheck the **Ignore Destination IPs in defining Policy Condition** checkbox.
2. Click the **Group** button, and then select the group from the **Network Group** drop-down list. If you want to create, edit, or delete a group, click the **Edit Network Groups...** button.

Selecting a network group restricts the policy rule to traffic that flows to this network group. If you leave the field blank or check the **Ignore Destination IPs in defining Policy Condition** checkbox, you are effectively stating that the destination IP address/network group of traffic is not a criterion for the policy.

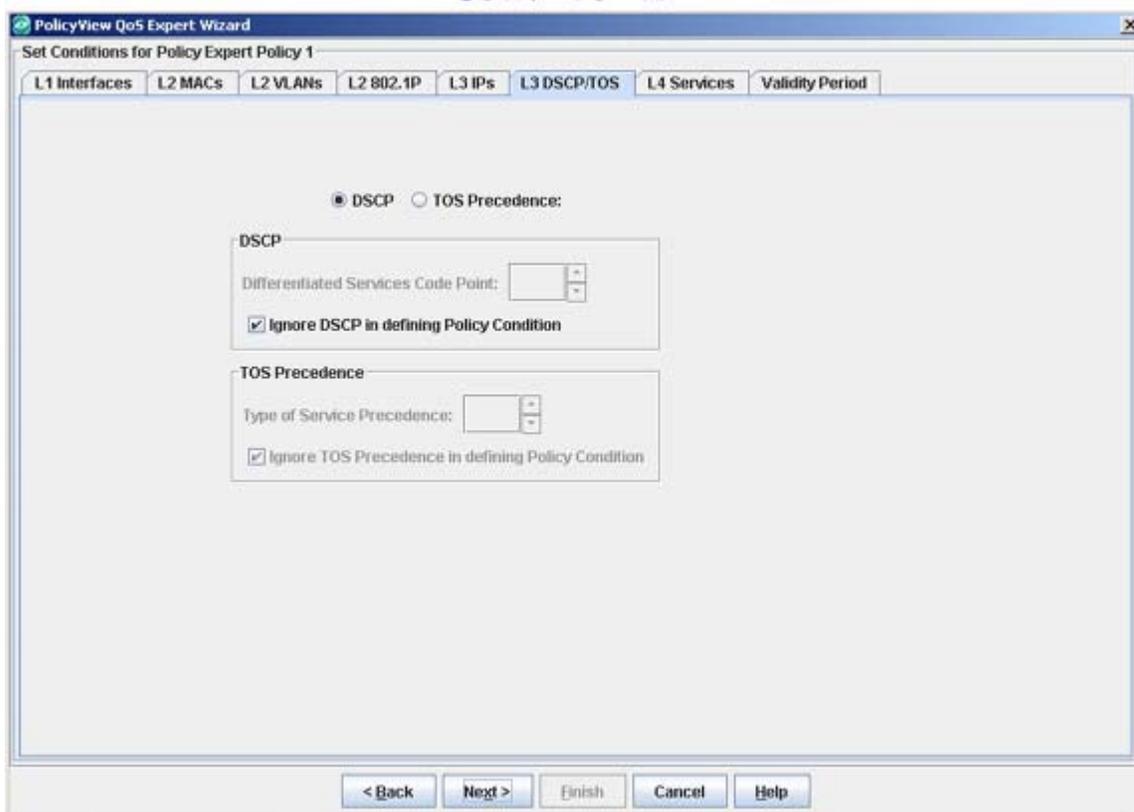
**Note:** When creating an IP condition for a NAT action you must specify a network group in the condition. NAT will only work when both the condition and the action specify network groups. To create a "one-to-many" condition and action, create a network group with a single entry for the condition.

## The DSCP/TOS Tab

The **L3 DSCP/TOS** tab, shown below, enables you to create a condition that applies the policy to incoming traffic that has a specified value in either the DSCP (Differentiated Services Code Point) byte or in the TOS (Type of Service) byte. Both DSCP and TOS are mechanisms used to convey QoS information in the IP header of frames. DSCP and TOS are mutually exclusive - you can use either DSCP or TOS but not both. Follow the steps below to create a DSCP/TOS condition.

**Note:** OmniSwitch 6800/7000/8000/9000 series switches support DSCP and TOS. However, 6600 series switches and some current XOS hardware and firmware releases do not. Please refer to the Switch release notes for information on the specific QoS functions available on various current platforms and combinations of hardware/firmware.

### DSCP/TOS Tab



## About DSCP

Entering a DSCP value creates a condition that applies the policy to traffic that has the specified DSCP value in the IP header of frames. DSCP is specified in RFC 2474 and defines the QoS treatment a frame is to receive from each network device. This is referred to as per-hop behavior.

If you are using DSCP, you can define any value in the range 0-63 as the DSCP value in the IP header of the frame. Traffic that contains this value will match this condition.

### About TOS

Entering a TOS value creates a condition that applies the policy to traffic that has the specified TOS value in the IP header of frames. The TOS byte is defined in RFC 791 and contains two fields. The precedence field is the three high-order bits (0-2) and is used to indicate the priority for the frame. The type of service field (bits 3-6) defines the throughput, delay, reliability, or cost for the frame; however, in practice these bits are not used. If you are using TOS, you can define any value from 0-7 as the value of the precedence field in the TOS byte. (A value of 7 has the highest precedence and a value of 0 has the lowest precedence.) Traffic that contains this value will match this condition.

### Creating a DSCP/TOS Condition

Create a DSCP/TOS condition as described below. Do not click the **Next** button until you have completed all desired tabs in the Policy Condition panel.

1. Select the **DSCP** or the **TOS Precedence** radio button to specify the type of value you will enter.
2. To specify a DSCP value, uncheck the **Ignore DSCP in defining Policy Condition** checkbox to activate the DSCP field. To specify a TOS value, uncheck the **Ignore TOS Precedence in defining Policy Condition** checkbox to activate the **TOS Precedence** field.
3. Enter a DSCP or TOS Precedence value.
  - For DSCP, enter any value in the range 0-63 to specify the DSCP value in the IP header of the frame that will match this condition.
  - For TOS, enter any value from 0-7 to specify the value of the precedence field in the TOS byte that will match this condition. A value of 7 has the highest precedence and a value of 0 has the lowest precedence.

### The Services Tab

The **L4 Services** tab, shown below, enables you to create a condition that applies the policy to traffic flowing between two TCP or UDP ports, or to all traffic originating from a TCP or UDP port, or to all traffic flowing to a TCP or UDP port. The Services tab also enables you to create a condition using a service or a service group. Using the Services tab, you can create the following conditions:

- Service Protocol condition
- Service condition
- Service Group condition

## Services Tab

### Creating a Service Protocol Condition

Create a service protocol condition as described below. Do not click the **Next** button until you have completed all desired tabs in the Policy Condition panel.

1. Select the **Protocol Only** radio button. The **Service Protocol** drop-down list is enabled.
2. Uncheck the **Ignore service protocol in defining Policy Condition** checkbox.
3. Select a protocol from the **Service Protocol** drop-down list (TCP or UDP) to define the type of ports you will specify.
4. Select the **Port(s)** radio button.
5. Specify the source or destination port, or both.
  - If you want to specify a source port, uncheck the **Ignore Source Port in defining Policy Condition** checkbox. The **Source Port** field is activated.
  - If you want to specify a destination port, uncheck the **Ignore Destination Port in defining Policy Condition** checkbox. The **Destination Port** field is activated.
6. If you are specifying a source port, select the port from the **Source Port** drop-down list. If you are specifying a destination port, select the port from the **Destination Port** drop-down list. Both combo boxes display a list of well-known TCP or UDP ports. If you want to create, edit, or delete a service port, click the **Edit Services Ports...** button.

### Creating a Service Condition

Create a service condition as described below. Do not click the **Next** button until you have completed all desired tabs in the Policy Condition panel.

1. Select the **Service** radio button.
2. Uncheck the **Ignore services in determining Policy Condition** checkbox.
3. Select a service from the **Service** drop-down list. If you want to create, edit, or delete a service, click the **Edit Services...** button.

### Creating a Service Group Condition

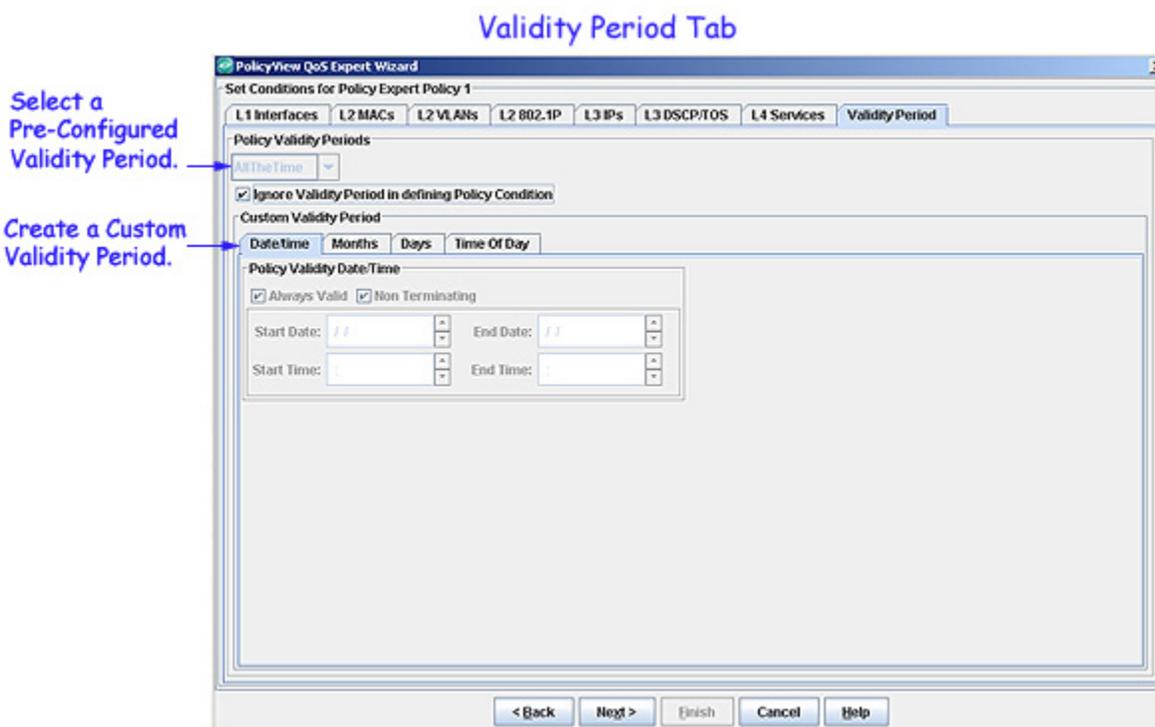
Create a Service Protocol condition as described below. Do not click the **Next** button until you have completed all desired tabs in the Policy Condition panel.

1. Select the **Group** radio button.
2. Uncheck the **Ignore service groups in determining Policy Condition** checkbox.
3. Select a service from the **ServiceGroup** drop-down list. If you want to create, edit, or delete a service, click the **Edit Services Groups...** button.

### The Validity Period Tab

The **Validity Period** tab (shown below) enables you to add a validity period to a condition by specifying the time periods when the policy is active and enforced. Four pre-configured policy validity periods are provided in the drop-down list in the **Policy Validity Periods** pane. They are **AllTheTime**, **Weekdays**, **Weekends**, and **WorkingDay** . You can also create custom validity periods.

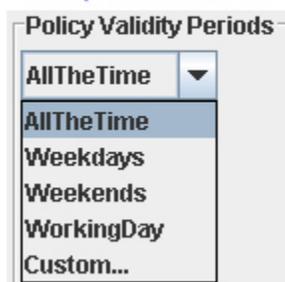
**Note:** The pre-configured validity period **AllTheTime** is the default and is automatically assigned to the condition when the **Ignore Validity Period in defining Policy Condition** checkbox is checked.



### Pre-Configured Validity Periods

To use one of the pre-configured policy validation periods, uncheck the **Ignore Validity Period in defining Policy Condition** checkbox and select the desired validity period from the **Policy Validity Periods** drop-down menu (shown and described below).

### Policy Validity Periods Drop-Down Menu



- **AlltheTime** - Specifies all months of the year, all days of the week, and all hours of the day.
- **Weekdays** - Specifies weekdays (Monday - Friday), all months of the year. Each weekday is 24 hours (midnight to midnight).
- **Weekends** - Specifies Saturday and Sunday, all months of the year. Each Saturday and Sunday is 24 hours (midnight to midnight).
- **WorkingDay** - Specifies weekdays (Monday - Friday), from 9:00 a.m. to 5:00 p.m. all months of the year.
- **Custom** - Select to [create a custom validity period](#).

**Note:** If you do not want a validity period to be part of the policy, make sure that the **Ignore Validity Period in defining Policy Condition** checkbox is checked.

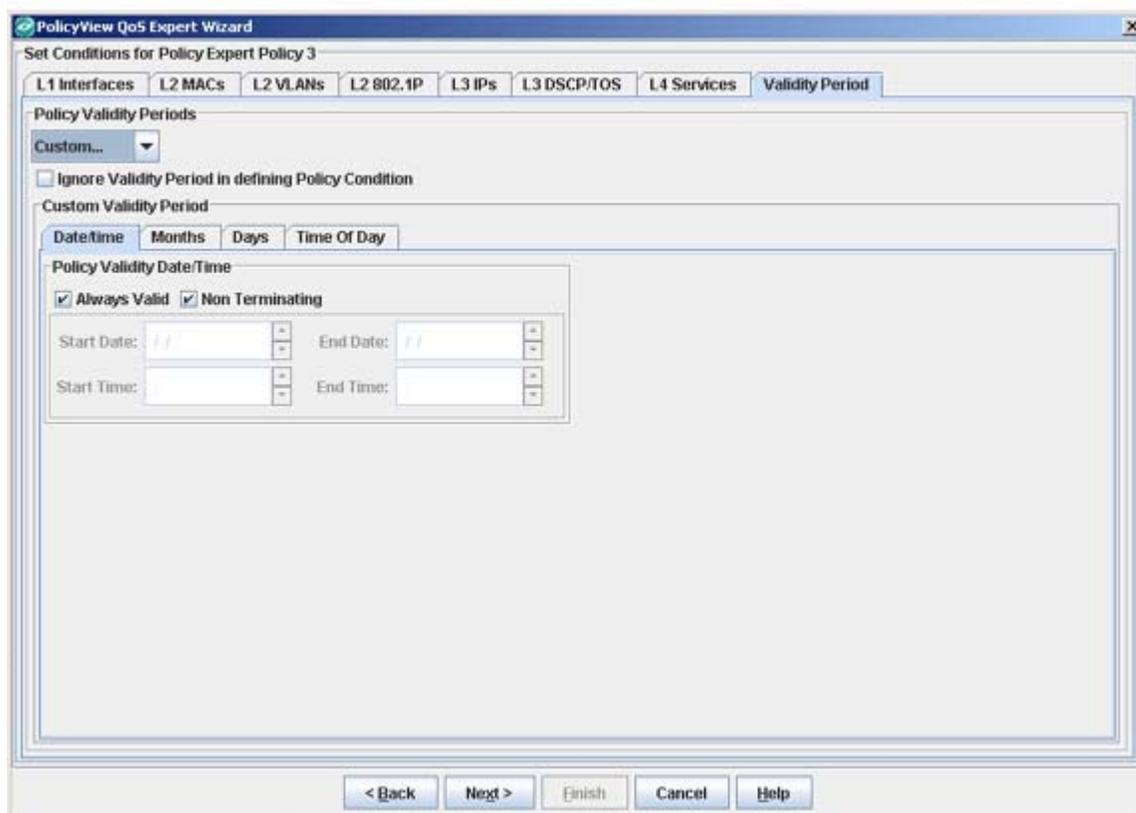
### Creating a Custom Validity Period

To create a custom validity period, uncheck the **Ignore Validity Period in defining Policy Condition** checkbox and select **Custom** from the **Policy Validity Periods** drop-down menu . A custom validity period can specify any desired month, and/or day of the week, and/or time of day. The four subtabs in the Custom Validity Period area - **Date/time**, **Months**, **Days**, and **Time Of Day** - enable you to create custom validity periods.

### Date/time Subtab

The **Date/time** subtab enables you to specify a starting date/time and an ending date/time for a custom validity period.

Date/Time Subtab



Uncheck the **Always Valid** checkbox to specify that the policy validity period will have a start date and a start time, but no end date and end time. Uncheck the **Non Terminating** checkbox to specify that the policy validity period will have a start date and time (you enter in the **Start Date** and **Start Time** fields), and also an end date and time (you enter in the **End Date** and **End Time** fields). Enter a value in the desired fields, or use the up and down arrows.

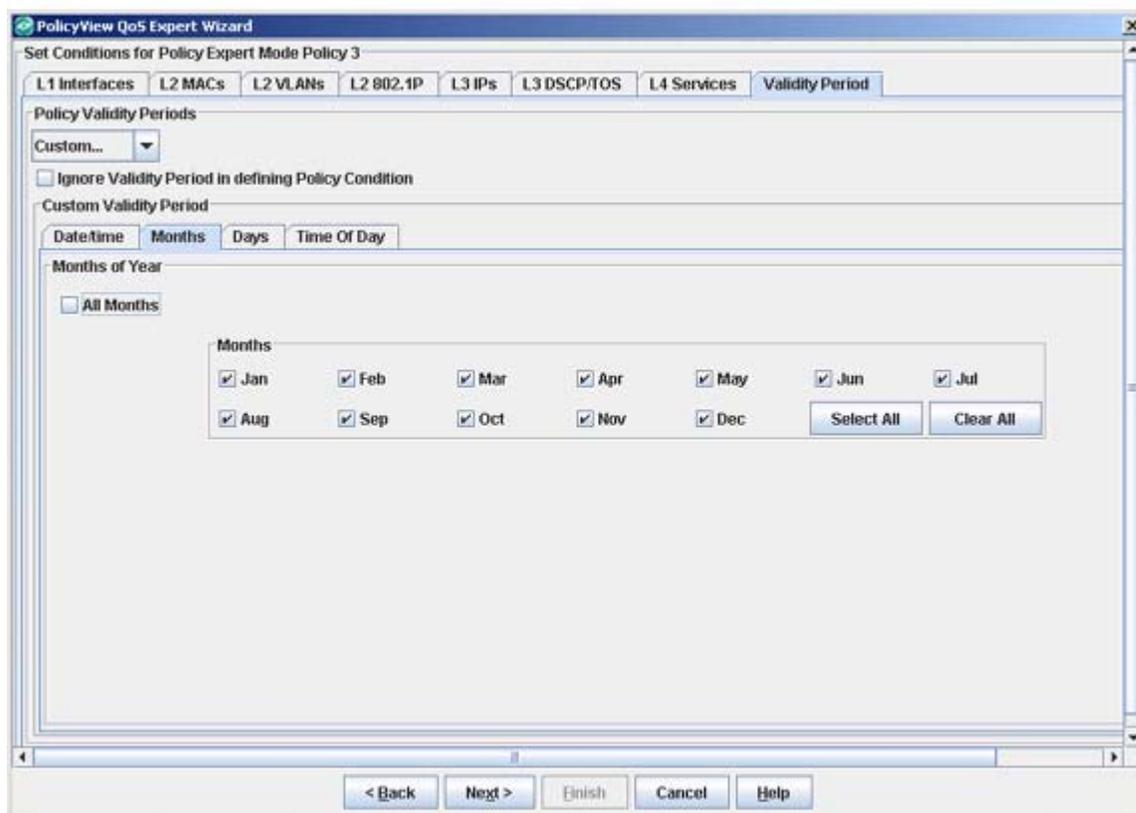
If you check both the **Always Valid** and the **Non Terminating** checkboxes, you cannot enter any desired dates and times in the **Start Date**, **Start Time**, **End Date**, and **End Time** fields.

**Note:** The **Date/time** subtab enables you to define overall starting and ending dates/times for the entire validity period. However, the validity period can include specified months, days, or times of day when it is not active. These inactive periods can be defined using the Months subtab, the Days subtab, and the Time of Day subtab.

### Months Subtab

The **Months** subtab enables you to specify the months of the year that the validity period will be active. A check by a month means the policy will be active and enforced during that month. Check the **All Months** checkbox to automatically check all the months of the year, or uncheck the **All Months** checkbox and select specific months. Click the **Clear All** button to uncheck all the months of the year. You can then check individual months as desired.

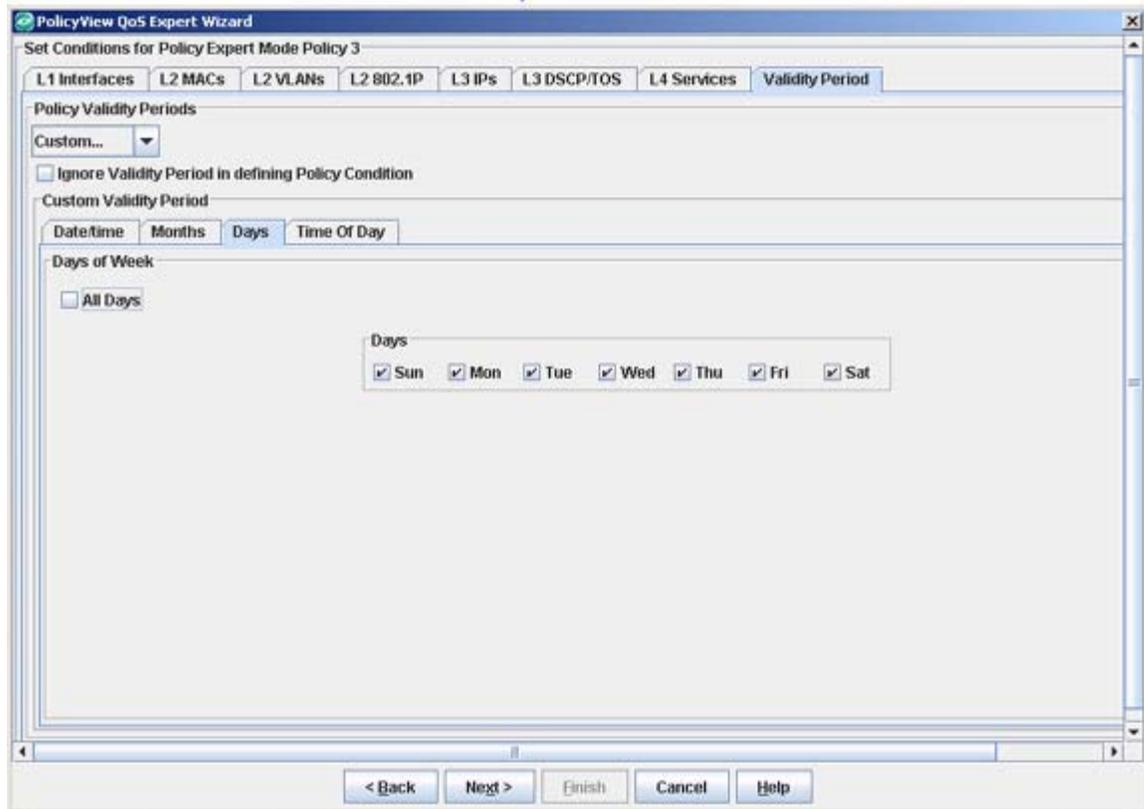
#### Months Subtab



### Days Subtab

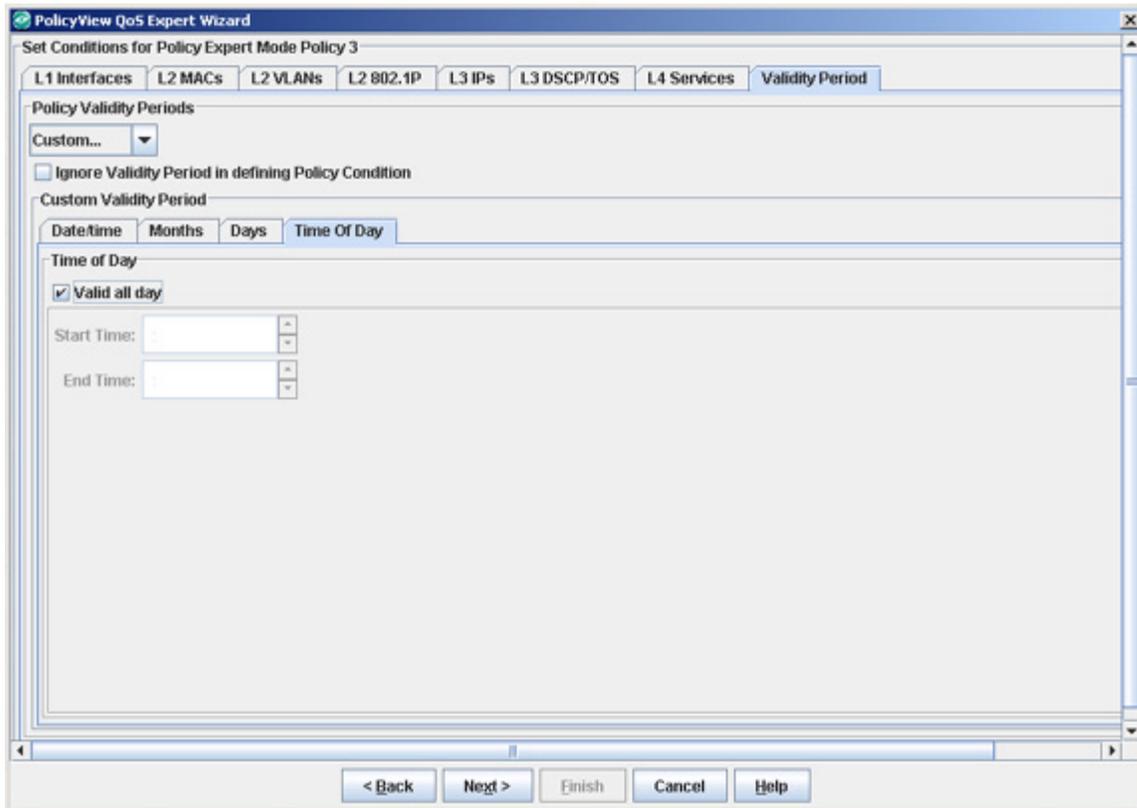
The **Days** subtab enables you to individually specify the days of the week that the validity period will be active. Click the **All Days** checkbox to automatically check all the days of the week, or uncheck the **All Days** checkbox and select specific days. A check by a day means the policy will be active and enforced during that day.

## Days Subtab

**Time Of Day Subtab**

The **Time of Day** subtab enables you to specify a daily starting time and ending time that will apply to each day that the validity period is active. Enable the **Valid all day** checkbox to make the validity period active 24 hours a day during the days that it is active. To specify specific starting and ending times, uncheck the **Valid all day** checkbox and enter the desired times in the **Start Time** and **End Time** fields. Enter a value in the desired fields, or use the up and down arrows.

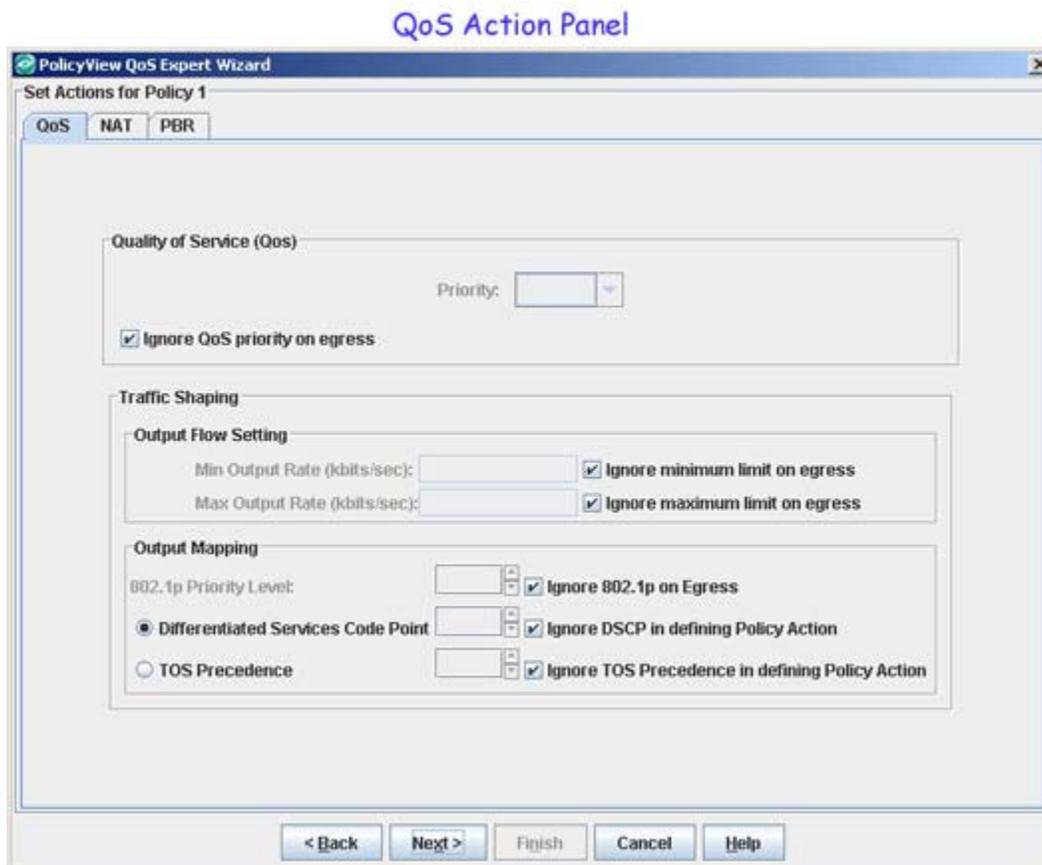
## Time of Day Subtab



**Note:** Click the **Next** button when you have completed all the desired tabs in the Policy Conditions panel.

## QoS Policy Action

The QoS Policy Action tab enables you to specify QoS actions to impose on traffic that meets the configured policy condition(s). When the conditions specified by the policy are true, traffic will flow as specified by the policy action.



## Quality of Service (QoS) Parameters

**QoS Parameters** fields are used to specify the QoS priority the traffic will receive if it meets the configured condition(s). If you want to specify a QoS priority for this traffic, uncheck the **Ignore QoS priority on egress** checkbox, and select the priority from the drop-down menu.

- **Platinum** priority provides the highest quality of service (and maps to a firmware priority of 7).
- **Gold** provides the next-highest quality of service (and maps to a firmware priority of 5).
- **Silver** provides the next-highest quality of service (and maps to a firmware priority of 3).
- **Bronze** provides the same quality of service as best effort (and maps to a firmware priority of 1). A separate egress queue is maintained in the hardware for traffic of each different priority.

## Traffic Shaping Parameters

The **Traffic Shaping** fields are used to specify the egress traffic flow rates and packet tagging characteristics for traffic matching the policy condition(s).

### Output Flow Settings

**Min Output Rate (kbits/sec)** - If you want to specify a minimum output rate, uncheck the **Ignore minimum limit on egress** checkbox, and specify the minimum amount of traffic, in kilobits-per-second, which is guaranteed to be transmitted from the port.

**Max Output Rate (kbits/sec)** - If you want to specify a maximum output rate, uncheck the **Ignore maximum limit on egress** checkbox, and specify the maximum amount of traffic, in kilobits-per-second, which is guaranteed to be transmitted from the port. Even if no other traffic exists, the output will be limited to the rate specified here.

### Output Mapping

The following parameters enable you to specify how packets that match the policy condition(s) will be tagged upon egress from the switch.

**802.1p Priority Level** - If you want outgoing packets tagged with an 802.1p priority level, uncheck the **Ignore 802.1p on Egress** checkbox. Set the **802.1p Priority Level** field to any value between 0 to 7 to specify the desired outgoing 802.1p priority for the traffic. A value of 7 indicates the highest priority and a value of 0 indicates the lowest priority.

For ports that are configured for 802.1q, this value is used in the 802.1q header and indicates the outgoing priority of the frame. When a frame is de-queued for transmission, it is assigned the priority of the queue and mapped to the outgoing 802.1p priority. This priority is combined with the VLAN group ID to create the 802.1p/q header for transmission. Note that if traffic matches the criteria specified by the policy condition, but the outgoing port does not support 802.1p tagging, the policy action will fail.

**Differentiated Services Code Point (DSCP)** - DSCP is defined in RFC 2474. Differentiated Services defines the QoS treatment a frame is to receive from each network device. This is referred to as per-hop behavior. If you enable the **Differentiated Services Code Point** radio button, you can set the associated field to any value from **0-63** to specify the Differentiated Services byte value with which to tag frames upon egress from the switch.

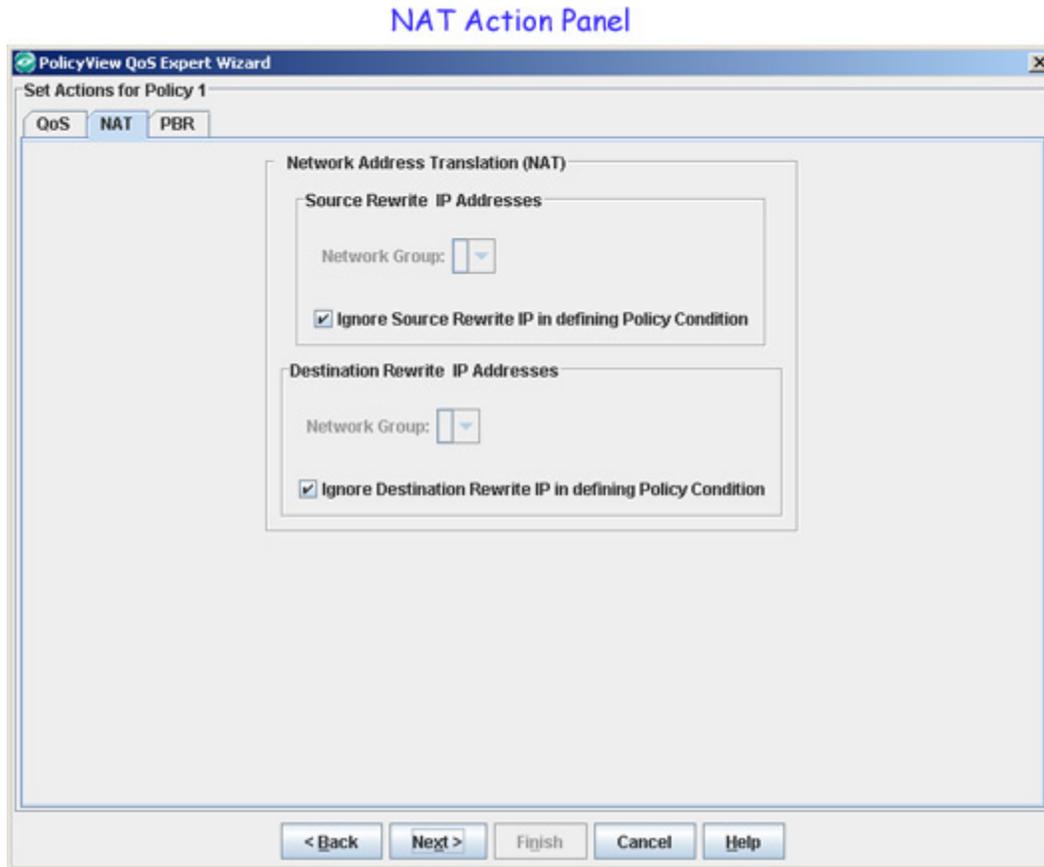
**TOS Precedence** - The TOS byte is defined in RFC 791. This byte contains two fields. The precedence field is the three high-order bits (0-2) and is used to indicate the priority for the frame. The type of service field (bits 3-6) defines the throughput, delay, reliability, or cost for the frame; however, in practice these bits are not used. If you enable the **TOS Precedence** radio button, set the associated field to any value from 0-7 to specify the value that will be inserted into the precedence field of the TOS byte upon egress from the switch. A value of 7 has the highest precedence and a value of 0 has the lowest precedence.

**Note:** You can enable **either** the DSCP or the TOS Precedence radio button to specify the mechanism you want to use (if any) to convey QoS information in the IP header of frames. DSCP and TOS are mutually exclusive. You can use either DSCP or TOS, but not both

### NAT Policy Action

The NAT Policy Action tab enables you to specify Network Address Translation actions to impose on traffic that meets the configured policy condition(s). When the conditions specified by the policy are true, traffic will flow as specified by the policy action.

**Note:** Remember, when creating a condition (e.g., MAC, IP) for a NAT action you must specify a group in the condition. NAT will only work when both the condition and the action specify groups. To create a "one-to-many" condition and action, create a group with a single entry for the condition.



### Source Rewrite IP Address

To include Source Rewrite IP in the NAT Policy condition, uncheck the **Ignore Source Rewrite IPs in defining Policy Condition** option and select Network Group to be used for policy condition from the **Network Group** drop-down menu.

### Destination Rewrite IP Address

To include Destination IP in the Policy Conditions, uncheck the **Ignore Destination Rewrite IPs in defining Policy Condition** option and select Network Group to be used for policy condition from the **Network Group** drop-down menu.

### PBR Policy Action

The PBR Policy Action tab enables you to specify to specify the default IP address to be used for Policy Based Routing on traffic that meets the configured policy condition(s). When the conditions specified by the policy are true, traffic will flow as specified by the policy action.

## PBR Action Panel

PolicyView QoS Expert Wizard

Set Actions for Policy 1

QoS NAT PBR

Policy Based Routing (PBR)

Permanent Gateway IP

PBR Permanent Gateway IP Address:

Ignore PBR Permanent Gateway

Alternate Gateway IP

PBR Alternate Gateway IP Address:

Ignore PBR Alternate Gateway

< Back Next > Finish Cancel Help

### Permanent Gateway IP

To set a Permanent Gateway IP address for traffic that meets the condition(s), uncheck the **Ignore PBR Permanent Gateway** checkbox and enter the default IP address in the **PBR Permanent Gateway IP Address** field.

### Alternate Gateway IP

To specify an alternate IP address for traffic that meets the policy condition(s), uncheck the **Ignore PBR Alternate Gateway** checkbox and enter the alternate IP address in the **PBR Alternate Gateway IP Address** field.

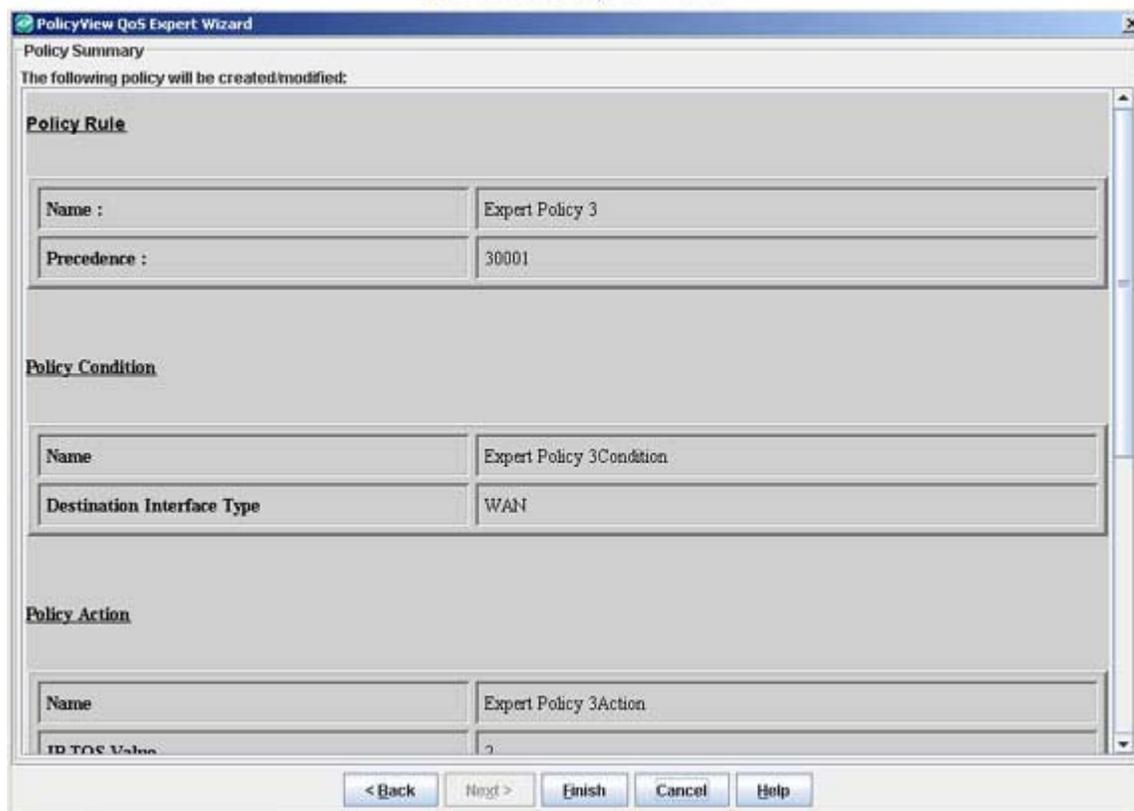
**Note:** The OmniSwitch 6800/7000/8000/9000 series switches support the 802.1 priority, DSCP, and TOS. However, 6600 series switches and some current XOS hardware and firmware releases do not. Please refer to the switch Release Notes for information on the specific QoS functions available on various current platforms and combinations of hardware/firmware.

## Applying Policies to the Network

The final screen of **Policy View QoS Expert Wizard** is the Policy Summary panel. This panel provides a summary of all the policy parameters (conditions, actions, etc.) for you to review. Applying a policy to the network consists of the following steps:

- Saving the policy to the LDAP repository
- Notifying the switches

### QoS Summary Window



The screenshot shows the 'PolicyView QoS Expert Wizard' window with the 'Policy Summary' tab selected. The window title is 'PolicyView QoS Expert Wizard'. The main content area is titled 'Policy Summary' and contains the text 'The following policy will be created/modified:'. Below this, there are three sections: 'Policy Rule', 'Policy Condition', and 'Policy Action'. Each section has a table of parameters.

Policy Rule	
Name :	Expert Policy 3
Precedence :	30001

Policy Condition	
Name	Expert Policy 3Condition
Destination Interface Type	WAN

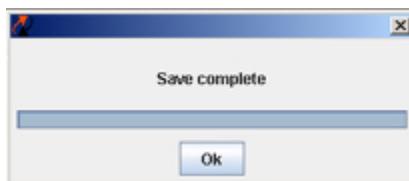
  

Policy Action	
Name	Expert Policy 3Action
IP TOS Value	2

At the bottom of the window, there are five buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

### Saving the Policy to the LDAP Repository

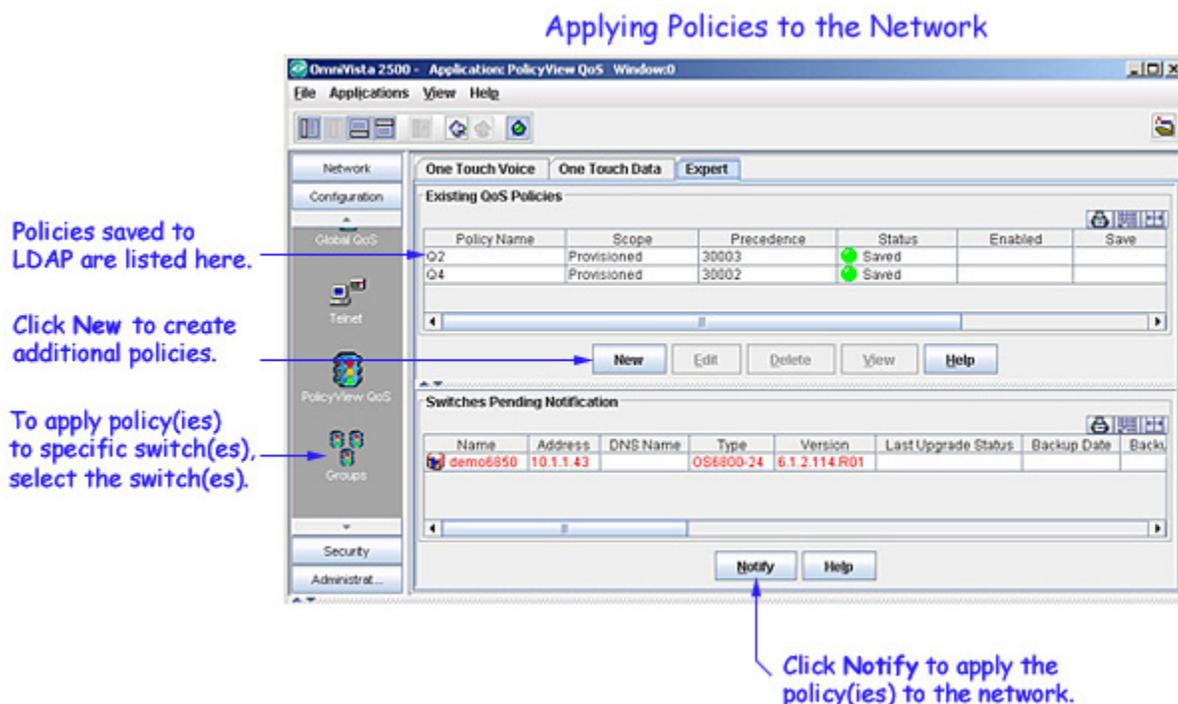
After reviewing the policy, click the **Finish** button to save the policy to the LDAP repository. When the policy is saved, the following confirmation window will appear. Click the **OK** button to return to the **Expert** tab.



You can create additional policies or apply any policy you have created, to the network.

## Notifying the Switches

After saving a policy to the LDAP repository, you will be returned to the **Expert** tab window. This tab lists all the policies that have been created and saved to the LDAP repository. You can apply a policy to all the switches configured for the policy, or you can apply the policy to individual switches within that group.



When you click the **Notify** button, all of the policies listed in the Existing QoS Policies table are applied to all of the switches configured for each policy. To apply the policy(ies) only to certain switches within the configured group of switches, select those switches from the Switches Pending Notification table.

**Note:** Press **Ctrl** or **Shift** while clicking the mouse to select multiple switches.

**Note:** Re-caching policies from the LDAP repository is very expensive in terms of switch resources and time. It is recommended that you verify all policies that you have created and notify the switches at the same time to minimize switch downtime.

## Error and Status Reporting

Messages in the policy.log file report the success or failure of the re-cache operation on an individual switch.

## The Status Panel

When you save policies to the LDAP repository and apply policies to the network, any error that may occur is reported in the Status panel (shown below).

Possible errors include:

- Failure to update the LDAP repository

- Failure to notify selected devices that they must re-cache their policies from the LDAP repository (which will occur if there is an SNMP timeout for any reason)
- Failure of the device to notify SecureView of its policy update status

Date	Application	Type	Message
Thu Nov 10 16:14:17 PST 2005	PolicyView QoS	Info	Saving policies
Thu Nov 10 16:14:22 PST 2005	PolicyView QoS	Info	Save complete
Thu Nov 10 16:15:03 PST 2005	PolicyView QoS	Info	Notifying Devices
Thu Nov 10 16:18:15 PST 2005	PolicyView QoS	Error	A remote processing error was encountered
Thu Nov 10 16:18:15 PST 2005	PolicyView QoS	Error	Notify complete with errors. See Audit server

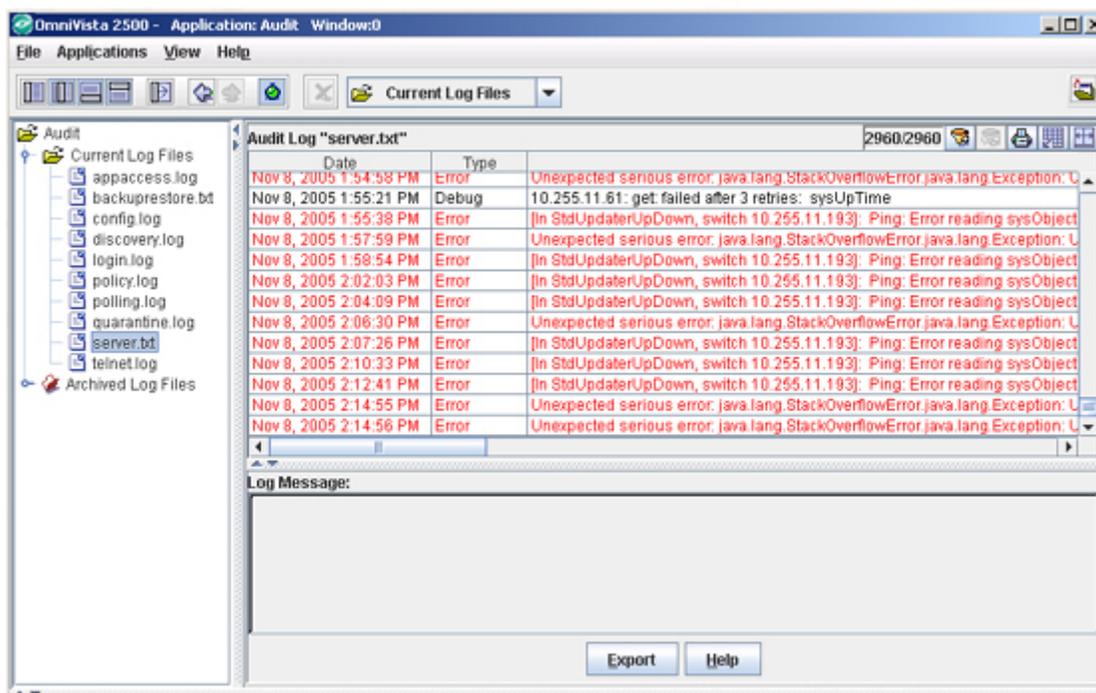
### Traps

When QoS-enabled Alcatel devices are notified that the LDAP repository has been changed, they re-cache their policies from LDAP, and then generate a trap notification to OmniVista informing that they have read the LDAP changes and have updated their internal policy information. Traps can be viewed in the Notifications application.

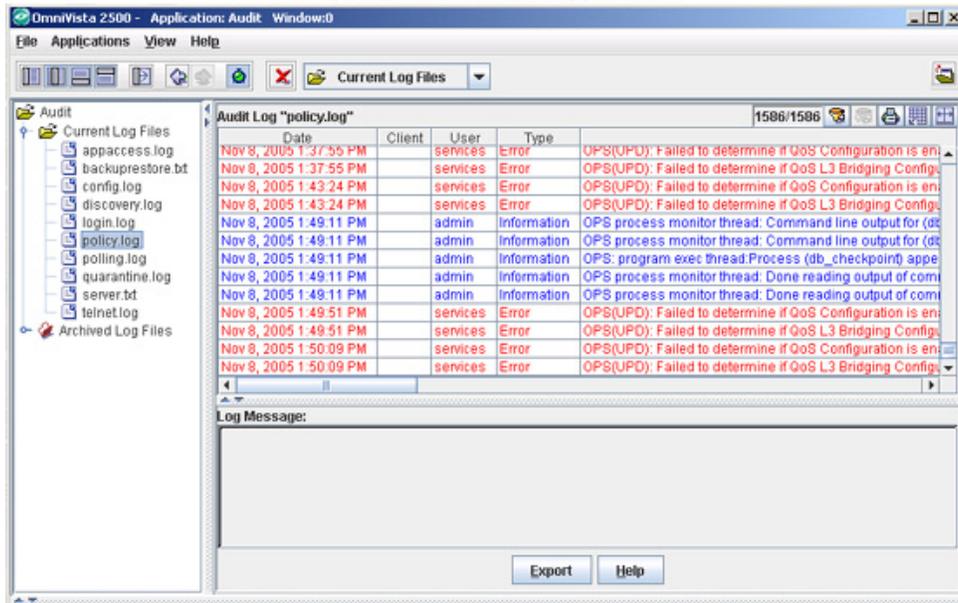
### The policy.log File and server.txt File in the Audit Application

When the PolicyView QoS application detects that a re-cache of policy information has failed on any device, the application writes a report to the OmniVista server.txt file and the policy.log file, which can be viewed from the Audit application.

#### The server.txt File in the Audit Application



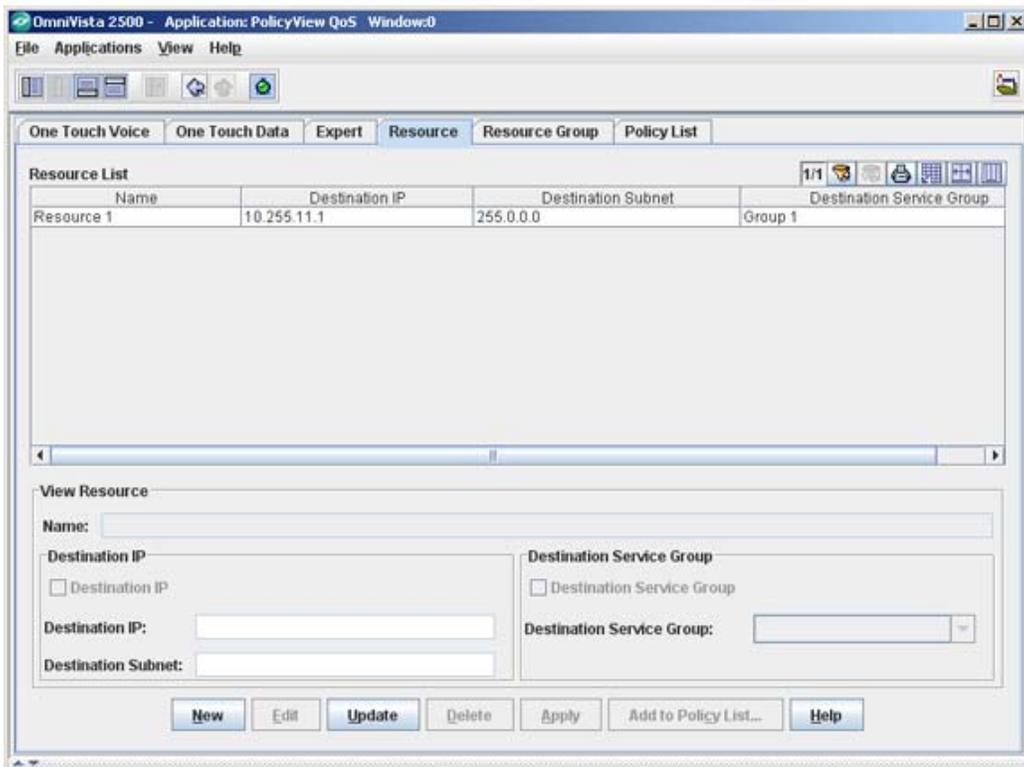
Policy Log in the Audit Application



Resource Tab

The **Resource** tab (shown below) is used to create/edit/delete system resources for QoS Policies. Although you can use Policy View QoS Expert Mode to create Policies for User Network Profiles (UNP), this can be time consuming. the Resource and Resource Group tabs can be used to quickly create Resources that can be turned into Policies and added to Policy Lists.

Resource Tab



## Creating a Resource

A resource is created by specifying a name, destination IP/subnet, and/or a set of services/service groups for the resource. Follow the steps below to create a new resource.

1. Click on the **New** button to activate the "Create Resource" pane.
2. Enter a Name for the Resource (e.g., NMS Performce Server).
3. Configure a Destination IP and/or a Destination Service Group for the Resource.
  - Select the "Destination IP" checkbox and enter a Destination IP and Subnet
  - Select the "Destination Service Group" checkbox and select an existing service group from the drop-down menu or select **New** to bring up the Service Groups window to create a new service group. A service is defined as protocol plus destination port. Policy View QoS defined services and service groups are used in the definition of resources.
4. Click the **OK** button, then click **Apply** to write the configuration to the LDAP Server.

Once the Resource is defined and saved, the corresponding LDAP policy rules, with a default initial precedence value of "50000" (which can modified), an action of "Accept" and validity period of "AllTheTime", is created and saved to the LDAP server.

## Editing a Resource

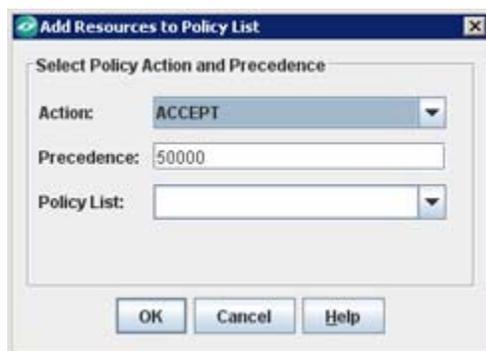
To edit parameters for an existing Resource, select the Resource in the Resource List and click the **Edit** button. Edit the Destination IP and/or Destination Service parameter(s), click **OK**, then click **Apply**. You cannot edit the Resource Name, you can only delete the Resource and create a new one.

## Deleting a Resource

To delete an existing Resource, select the Resource in the Resource List, click the **Delete** button, then click **OK**, then click **Apply**.

## Adding a Resource to a Policy List

After creating a Resource, you can add that Resource to an existing Policy List. Select the Resource(s) you want to add to the list from the Resource List and click on the **Add to Policy List** button. The Add Resources to Policy List window appears.

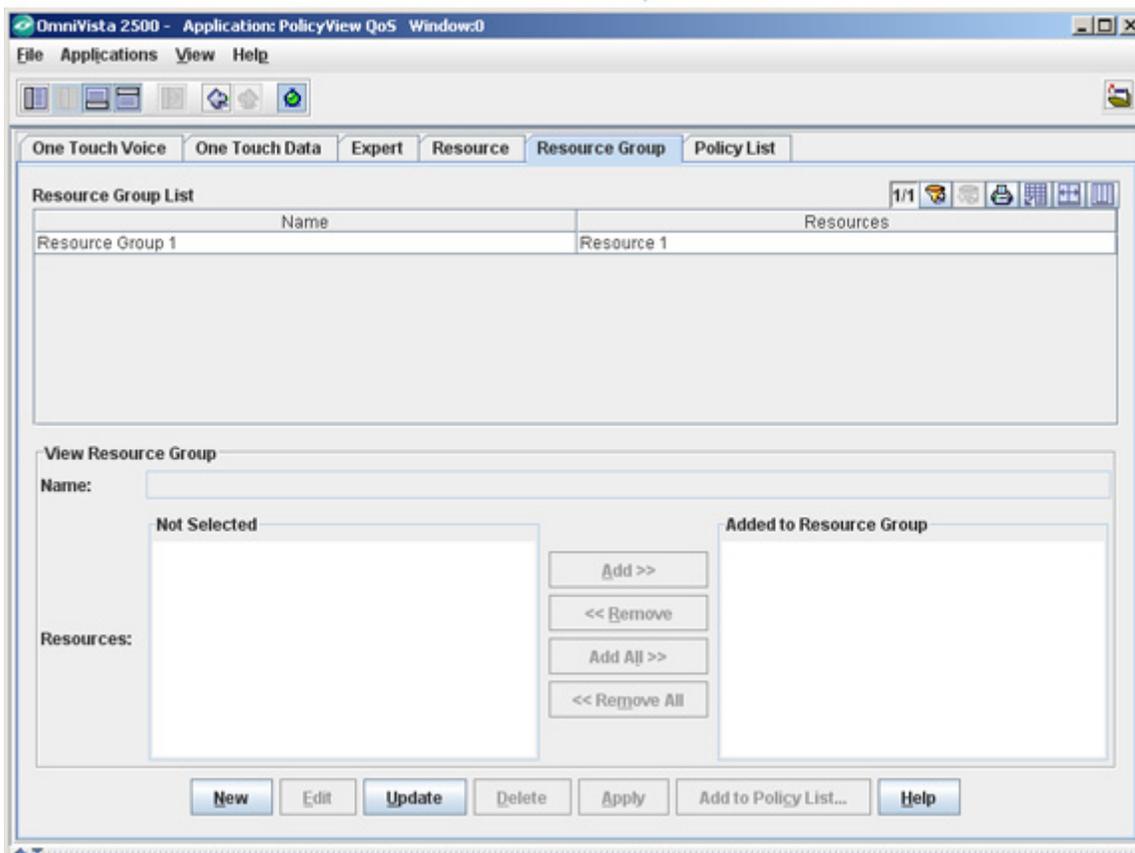


Modify the default settings for **Action** and **Precedence**, if necessary and select an existing **Policy List** from the drop-down menu. Click the **OK** button.

## Resource Group Tab

The **Resource Group** tab (shown below) is used create/edit/delete Resource Groups from existing Resource to quickly create Resource Groups that can be turned into Policies and added to Policy Lists.

Resource Group Tab



### Creating a Resource Group

After creating Resources, you can combine them into a Resource Group, which can then be applied to a Policy List. Follow the steps below to create a Resource Group.

1. Click on the **New** button to activate the "Create Resource Group" pane.
2. Enter a Name for the Resource Group (e.g., NMS Servers).
3. Select the Resources(s) you want to include in the group and use the **Add/Remove** buttons to add them to the Resource Group.
4. Click the **OK** button, then click **Apply** to write the configuration to the LDAP Server.

Once the Resource Group is defined and saved, the corresponding LDAP policy rules, with a default initial precedence value of "50000" (which can be modified), an action of "Accept" and a validity period of "AllTheTime", is created and saved to the LDAP Server.

## Editing a Resource Group

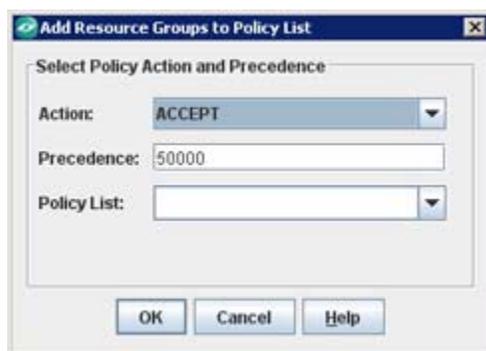
To edit parameters for an existing Resource Group, select the Resource Group in the Resource Group List and click the **Edit** button. Select the Resources(s) you want to add or remove from the group and use the **Add/Remove** buttons to add/remove them to/from the Resource Group., click **OK**, then click **Apply**. You cannot edit the Resource Group Name, you can only delete the Resource Group and create a new one.

## Deleting a Resource Group

To delete an existing Resource Group, select the group in the Resource Group List, click the **Delete** button, then click **OK**, then click **Apply**.

## Adding a Resource Group to a Policy List

After creating a Resource Group, you can add the Resource Group to an existing Policy List. Select the Resource Group(s) you want to add to the list from the Resource Group List and click on the **Add to Policy List** button. The Add Resource Groups to Policy List window appears.



Modify the default settings for **Action** and **Precedence**, if necessary and select an existing **Policy List** from the drop-down menu. Click the **OK** button.

## Policy List Tab

The **Policy List** tab (shown below) displays a list of all policies configured for the switch. It is also used to view, create, modify and delete policy lists and assign QoS/ACL policy rules to a policy list. The QoS/ACL policy rules that you associate with a policy list can be defined using the PolicyView or SecureView ACL applications. In addition, when defining policy list, you have the option to either use policy rules or use resources/resource groups (Resource and Resource Group tabs). Depending on the selection, the new policy list can be defined using a picker control to select any existing policy rules or a table control to select new or existing resources/resource groups. You can also set the precedence of policy rules within a policy list.

### Policy List Tab

