Ensuring Quality of Service with Cisco ISA500 Series Integrated Security Appliances

This application note explains how to use the Quality of Service (QoS) features of your Cisco ISA500 Series Integrated Security Appliance (ISA) to manage traffic and improve service on your network.

Contents

Benefits of QoS

How can you ensure that Voice over IP calls are handled without audio issues? How can you provide sufficient bandwidth for the highest priority data transfers? You can use QoS to prioritize the types of traffic that are most important to your business.

Typically, networks operate on a best-effort delivery basis, which means that all traffic has equal priority and an equal chance of being delivered in a timely manner. Likewise, when congestion occurs, all traffic has an equal chance of being dropped. You can use QoS features to select and prioritize users, applications, and services. QoS can make network performance more predictable and bandwidth utilization more effective.

All networks can benefit from QoS for optimum efficiency. QoS is especially important for real-time streaming multimedia applications such as voice over IP, online games, and IPTV, since these applications are delay sensitive and often require a fixed bit rate.

In Cisco ISA500 Series Integrated Security Appliances, you can configure QoS for the WAN, the LAN, and the wireless network. QoS is fully supported over VPN tunnels as well. You can adjust the QoS settings to achieve these goals:

- Support dedicated bandwidth.
- Prevent and manage network congestion.
- Set priorities for users, applications, and services.

Enabling QoS Features

Use the Networking > QoS > General Settings page to enable QoS features on each interface. Until you enable QoS, other configuration pages are unavailable and traffic is handled on a best-effort basis.

Configuring QoS for Your Internet Traffic

Most network congestion involves traffic to and from the Internet, through a WAN interface. To control traffic and prevent issues such as delay and jitter, you can classify traffic and establish policies to ensure that important users, applications, and services receive priority treatment. For example, you can prioritize inbound traffic for a web server that you host, or reserve bandwidth for Voice over IP calls. Another approach is to specify the types of traffic that have low priority.

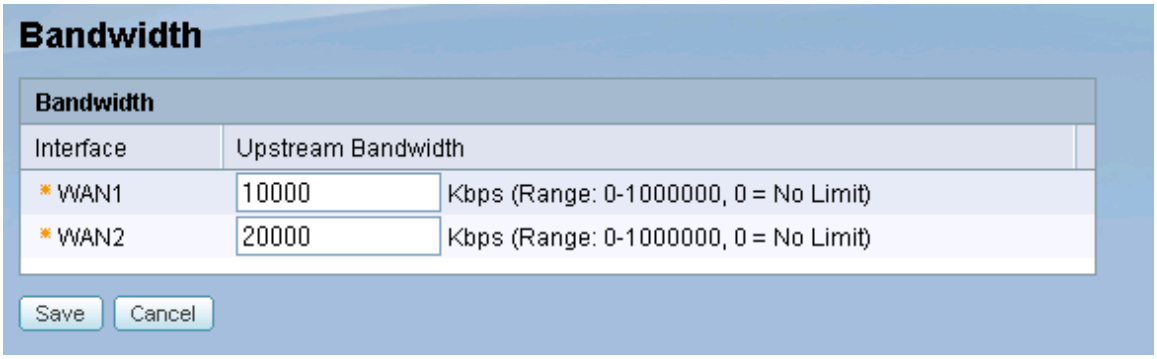
This process involves the following tasks:

1. Enable WAN QoS.
2. Specify the available bandwidth.
3. Create “traffic selectors” to classify the WAN traffic.
4. Create “policy profiles” to handle the selected traffic.
5. Apply one inbound and one outbound QoS policy profile to each WAN interface.
6. Decide how the priority queues operate (if you are using these queues in your policy profiles).

Specifying the Bandwidth from your ISP

It’s important to specify the upstream bandwidth that is provided by your ISP. Enter this information on the Networking > QoS > WAN QoS > Bandwidth page. It will limit the upstream rate to the specified bandwidth. If the upstream traffic exceeds this bandwidth, the traffic will be handled according to the applicable QoS policy profiles and queue settings.

Tip: Effective bandwidth is typically less than the ISP’s advertised limit. From a practical standpoint, some administrators choose to specify a rate that is one level below the advertised limit.



Classifying the WAN Traffic

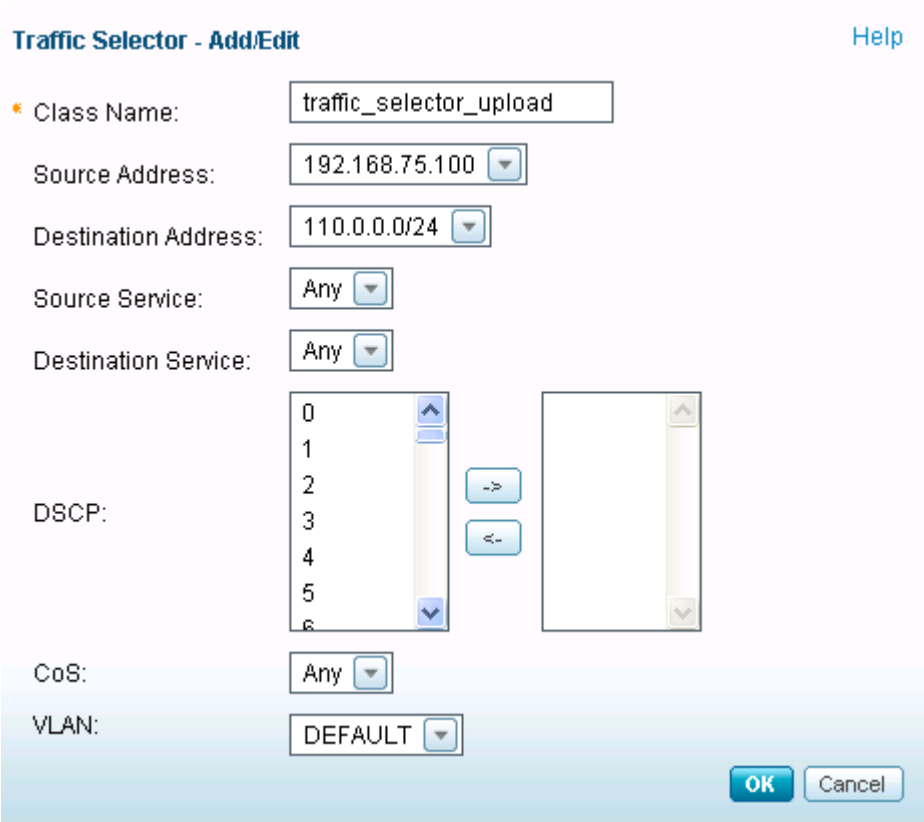
After enabling WAN QoS, use the Networking > QoS > WAN QoS > Traffic Selector (Classification) page to classify the traffic that is important to you. Traffic selectors tell the ISA, "Watch for traffic that matches these criteria." The ISA

can select traffic based on elements such as the IP address of the user and the destination, as well as the service or the VLAN in use. The ISA can store up to 256 traffic selectors. You can use up to 64 in each QoS Policy Profile that you create.

To add a new traffic selector, click **Add**, and then enter the criteria. For more information, refer to the online Help and the following examples.

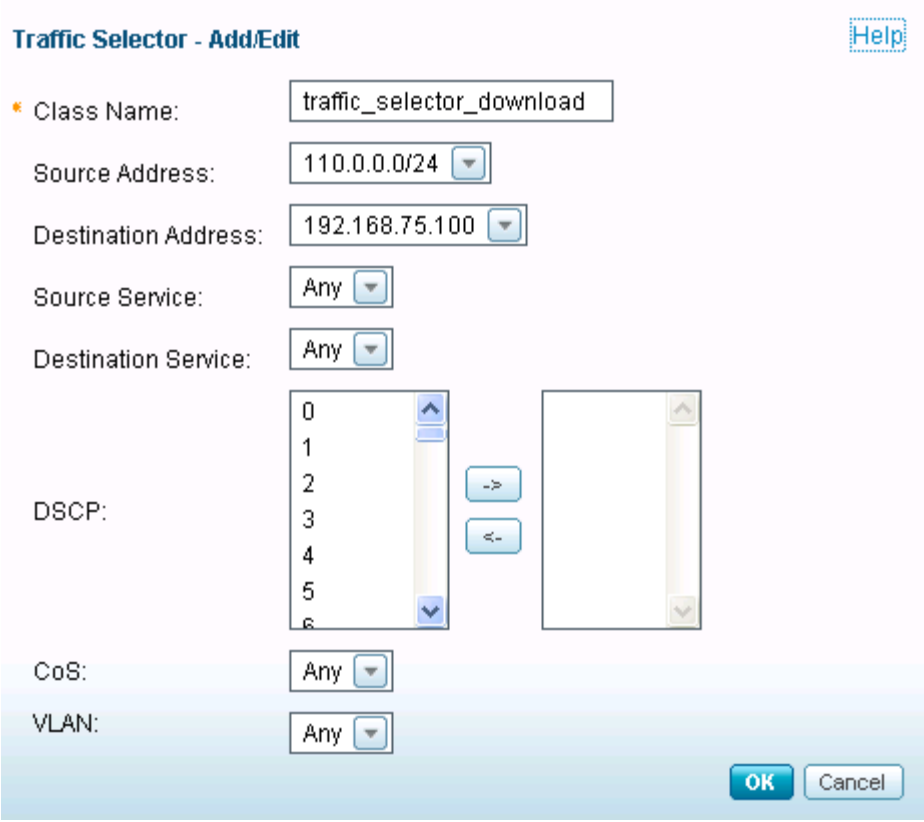
Example: Selecting Outbound Traffic by Using the Source and Destination Addresses

The following example tells the ISA to watch for uploads from a LAN device (192.168.75.100) to an FTP server (110.0.0.0/24). If this type of traffic is not critical to your business, you could use this traffic selector an inbound QoS policy profile that places the traffic into a low priority queue.



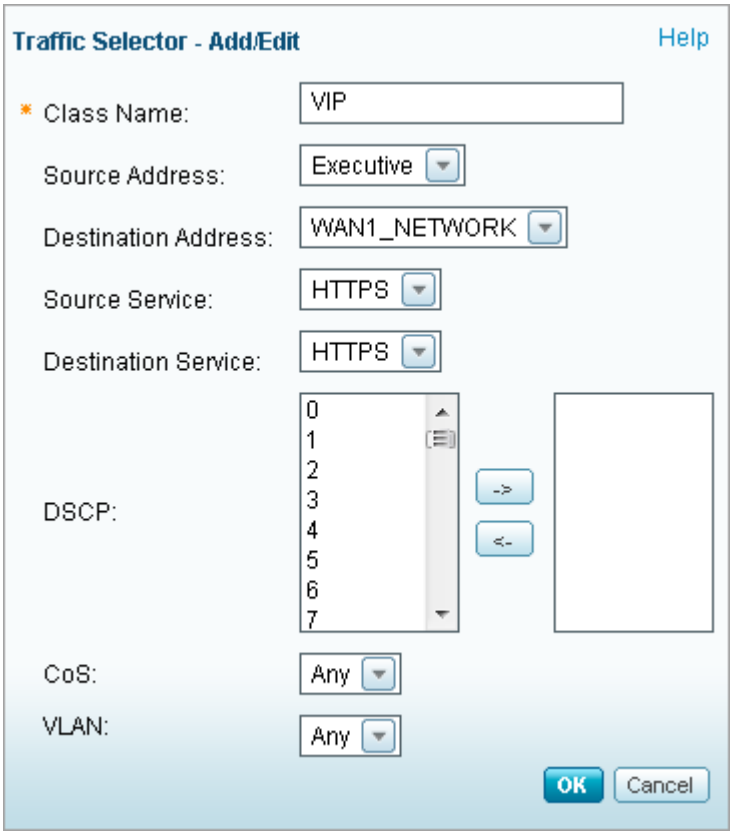
Example: Selecting Inbound Traffic by Using the Source and Destination Addresses

The next example tells the ISA500 to watch for downloads from an Internet address (110.0.0.0/24) to a LAN device (192.168.75.100). If this type of traffic is not critical to your business, you could use this traffic selector in an inbound QoS policy profile that places this traffic into a low priority queue.



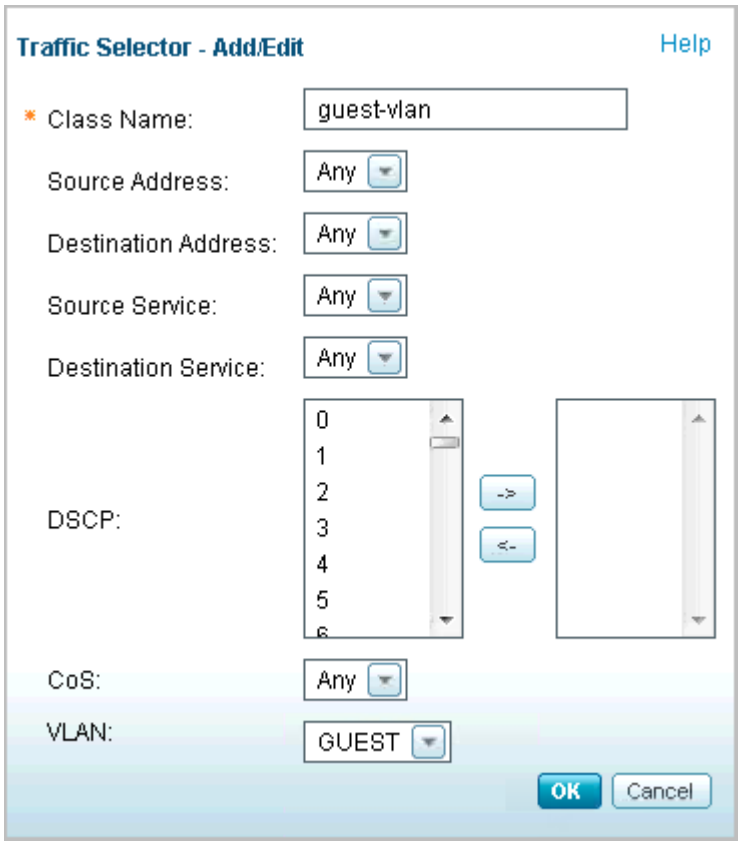
Example: Selecting a VIP user

This example tells the ISA500 to watch for HTTP traffic from a particular user (specified by entering an IP address). If this user's HTTP traffic is critical to your business, you could use this traffic selector in an outbound QoS policy that places this traffic into a high priority queue.



Example: Limiting the bandwidth for guest users

This example tells the ISA500 to watch for any traffic from the GUEST VLAN. Since guest users' activity is not critical to your business, you could use this traffic selector in an outbound QoS policy that limits the bandwidth for this type of traffic.



Choosing How to Handle the Selected WAN Traffic

After enabling WAN QoS and creating traffic selectors, use the Networking > QoS > WAN QoS > QoS Policy Profile page to create QoS policy profiles. A policy profile tells the ISA, "When you see this class of traffic, perform these actions." You can add up to 64 class rules to each QoS policy profile. The ISA can store up to 32 QoS policy profiles, although you can apply only one outbound policy and one inbound policy to each WAN interface.

To add a policy profile, click **Add**. Enter a **Policy Name**, and then choose **Inbound** or **Outbound**.

To add a class rule, click **Add**. Then choose a traffic selector and the actions to apply to the selected traffic. You can add up to 64 class rules to each policy profile.

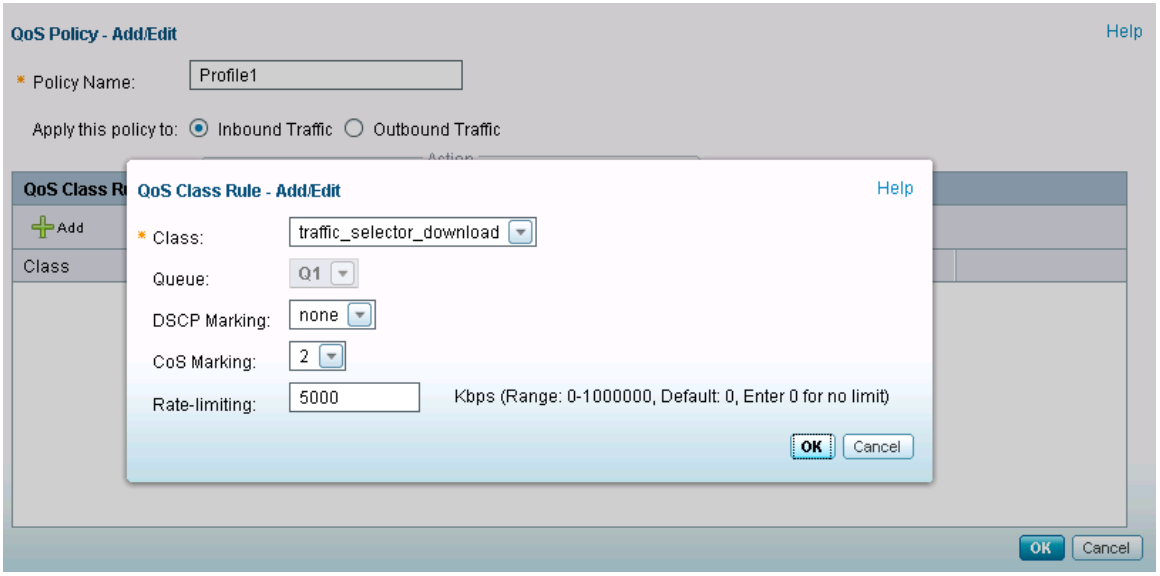
The precedence of these rules is determined by the order in which they appear. The class rules that are lower in the list have precedence over the rules that are higher in the list. For example, suppose that we have an *FTP* class rule that puts FTP traffic into Q2 and a *Manager* class rule that puts a particular manager's traffic into Q1. Suppose that this manager uses FTP to put a file on an external server. In this situation, does the traffic stream go to Q2, as specified in the *FTP* class rule, or to Q1, as specified in the *Manager* rule? To ensure that the *Manager* rule has precedence over the *FTP* rule, we would add the *FTP* rule first and then add the *Manager* rule.

For more information about policy profiles, refer to the online Help and the following examples.

Example: Policy profile for downloads from a specified server

For inbound traffic, you can limit the download rate and change the DSCP and CoS values that other devices and applications can use to judge the importance of a packet.

In the following example, the policy profile applies to inbound traffic for the *traffic-selector_download* class that you saw in the Traffic Selectors examples. If the ISA sees inbound traffic matching the criteria, then the ISA limits the download rate to 5Mbps and changes the CoS value to 2.

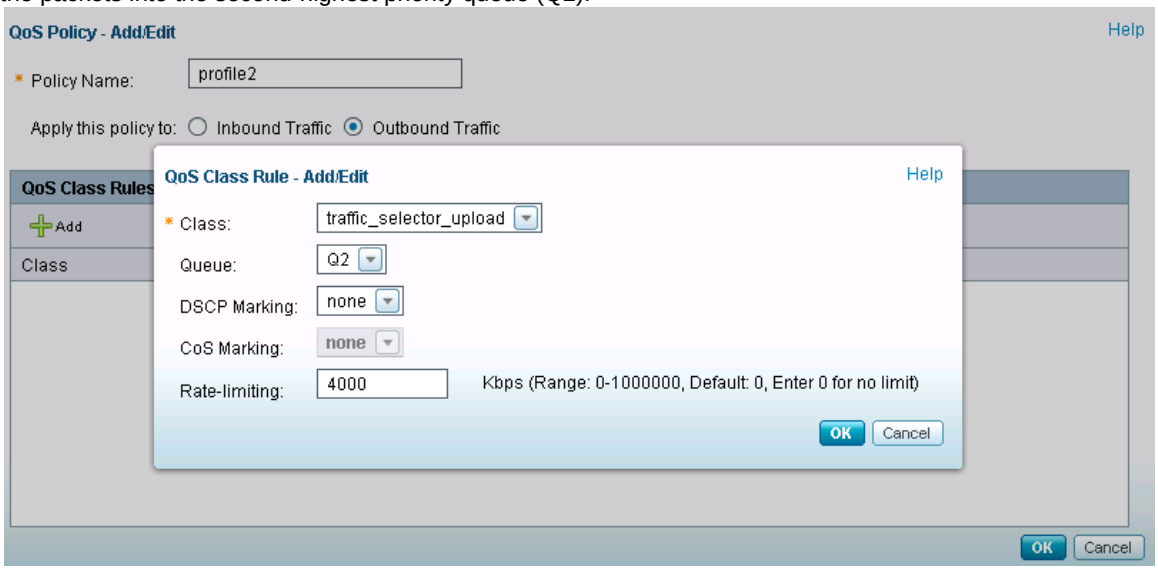


Example: Policy profile for two classes of traffic

For outbound traffic, you can send the traffic to a priority queue, limit the upload rate, and change the DSCP value that other devices and applications can use to judge the importance of a packet.

In the following example, the policy profile applies to outbound traffic for two classes: the *traffic_selector_upload* class and the *VIP* class that you saw in the Traffic Selectors section. If the ISA sees outbound traffic matching either of the specified traffic selectors, it performs the actions in the class rules.

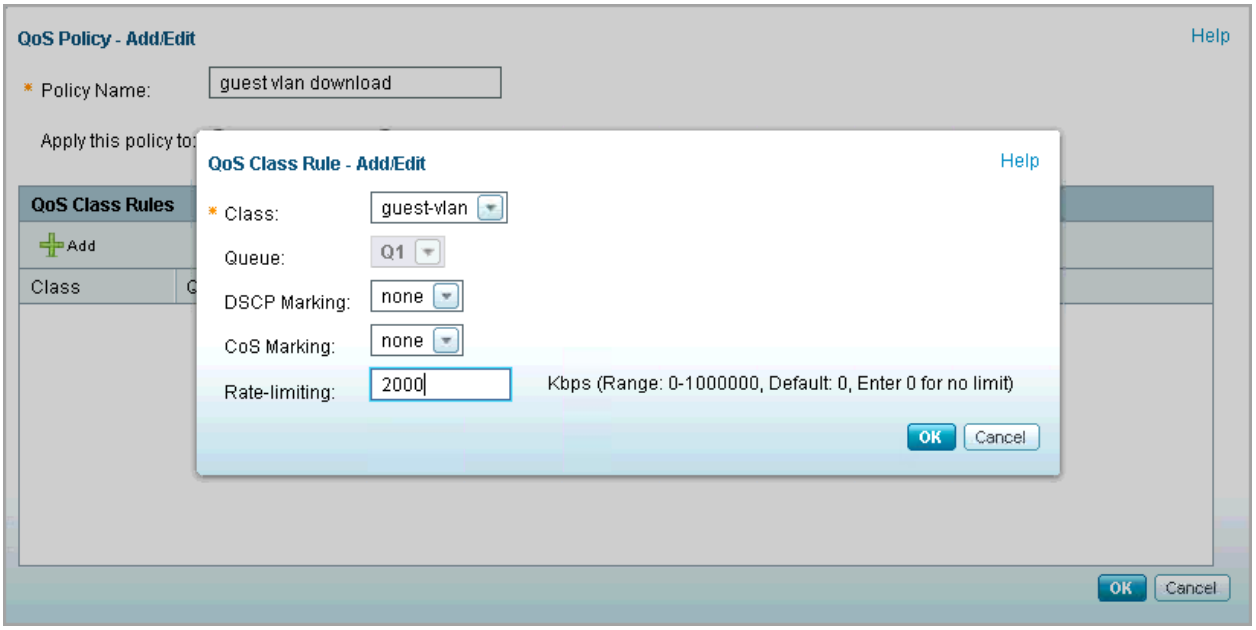
If the traffic matches the criteria in the *traffic_selector_upload* class, the ISA limits the upload rate to 4Mbps and puts the packets into the second-highest priority queue (Q2).



If the traffic matches the criteria for the *VIP* class, the ISA puts the traffic into Q1.

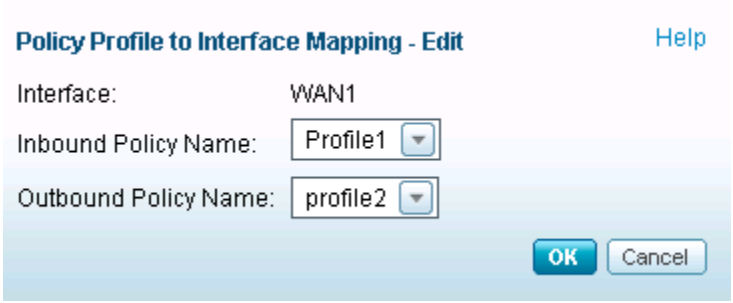
Example: Policy Profile for guest traffic

In this example, outbound traffic from the GUEST VLAN is limited to 2Mbps.



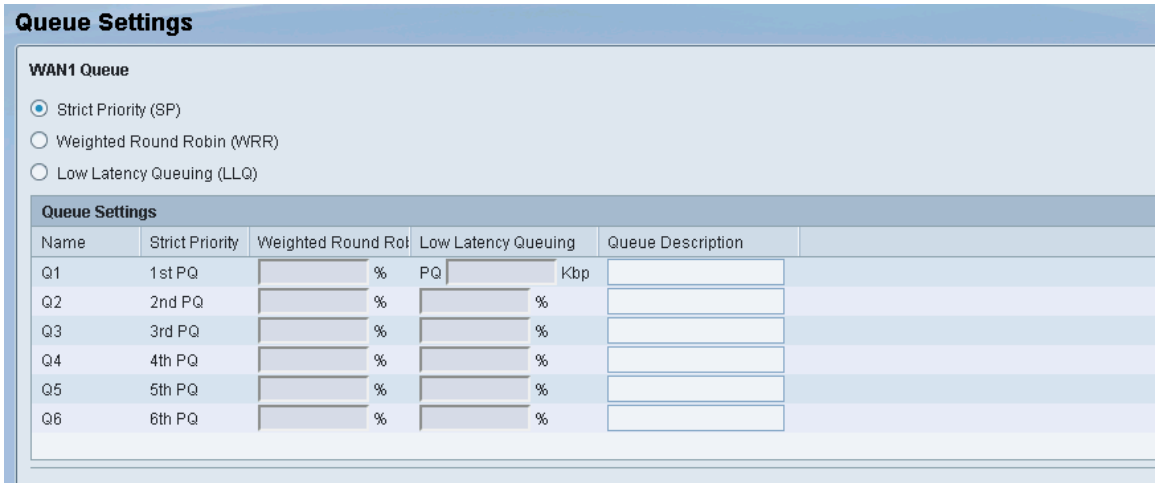
Applying QoS Profiles to a WAN Interface

After adding QoS profiles, use the Networking > QoS > WAN QoS > Policy Profile to Interface Mapping page to apply one outbound policy and one inbound policy to each WAN interface.



Deciding How the WAN Priority Queues Operate

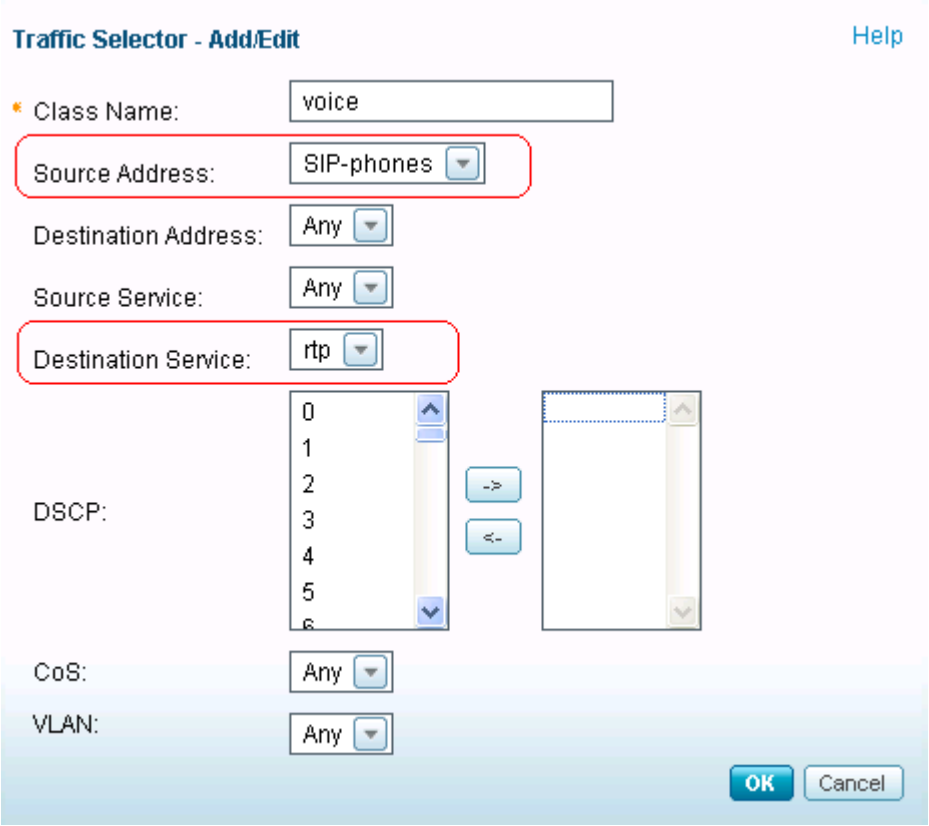
If you use queues in your QoS Policy Profiles, you can adjust the settings on the Networking > QoS > WAN QoS > Queue Settings page. The ISA supports six WAN priority queues, from Q1 (highest) to Q6 (lowest). You can use different approaches: Strict Priority (SP), Weighted Round Robin (WRR), and Low Latency Queuing (LLQ).



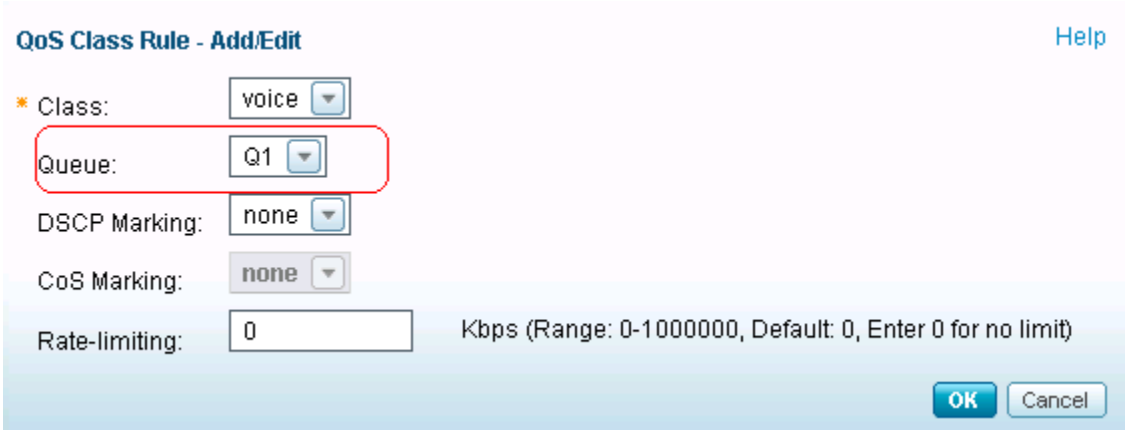
- **Strict Priority (SP):** This option is selected by default. Traffic from Q1 is transmitted first. Traffic from the lower queues is processed only after the Q1 has transmitted, thus ensuring the highest level of bandwidth for Q1. A disadvantage of SP is that high traffic from Q1 may provide no opportunity for the lower queues to transmit.
- **Weighted Round Robin (WRR):** Traffic is sent from the queues in round-robin fashion. The number of packets sent from a queue is proportional to the weight of the queue. The higher the weight, the more frames are sent. As compared to SP, WRR offers more opportunities for lower queues to transmit.
- **Low Latency Queuing (LLQ)**: Traffic from the Q1 is transmitted first, but Class-Based Weighted Fair Queuing (CBWFQ) allows delay-sensitive data (such as voice) to be de-queued and sent first.

Example: Prioritizing voice traffic

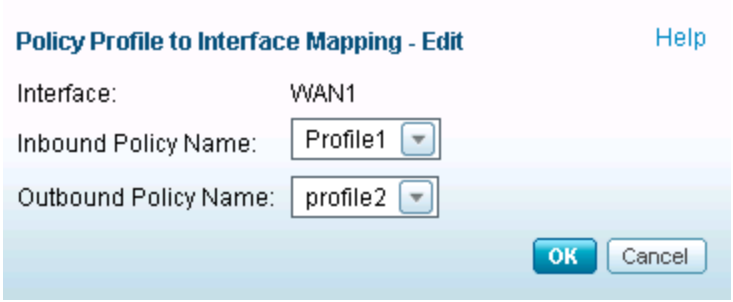
If you know the IP address of the phones, you can use the IP address to filter the voice traffic. Or you can predefine the voice traffic (SIP and RTP) through L4 port, and then use the destination service (RTP) to select the traffic. First, create a Traffic Selector that watches for RTP traffic from the SIP-phones range of IP addresses.



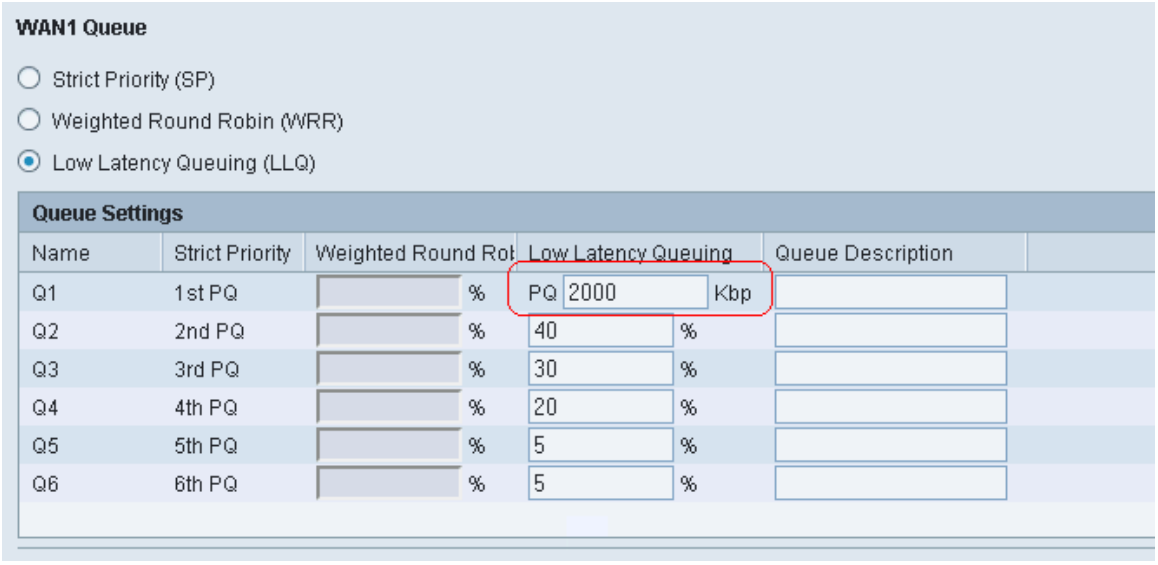
Then create a class rule that places this traffic into Q1.



Next, apply this rule to the WAN interface.



Finally, configure the WAN queue settings to use LLQ. In this example, the PQ value is set to 2000 because the voice traffic at this site (given the number of phones and the bandwidth) does not exceed 2Mbps.



Configuring QoS for Your Local Network

If your local network is very busy or includes time-sensitive applications such as Voice over IP, you can ensure that important traffic is prioritized.

Choosing How to Classify and Prioritize LAN Traffic

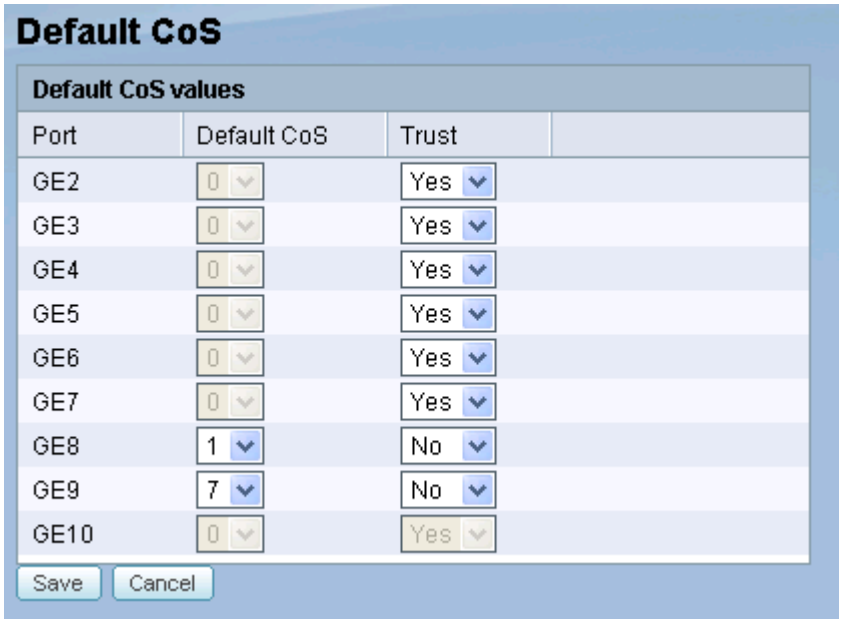
To classify LAN traffic, use the Networking > QoS > LAN QoS > Classification Methods page. CoS is the default classification method. As a general rule, use CoS for trunk ports that connect to devices that use CoS to prioritize traffic. Use DSCP for access ports and for trunk ports that connect to devices using DSCP to prioritize traffic.

Example: Using CoS values to prioritize LAN traffic

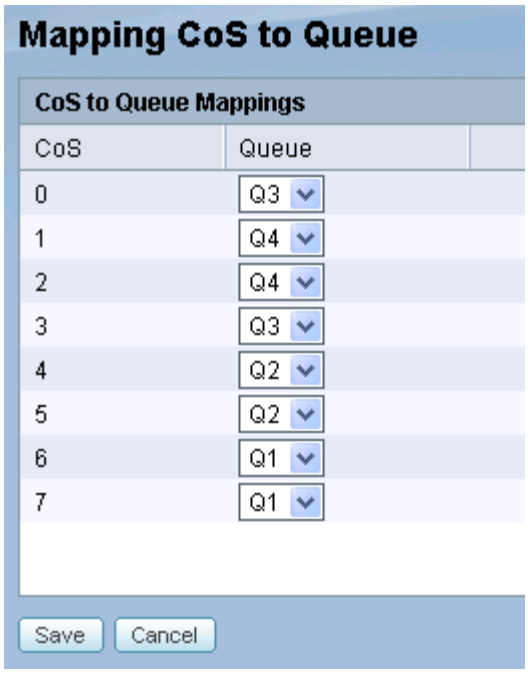
You can specify the CoS value for each port, and assign the CoS values to priority queues to manage the traffic. This process involves the following tasks:

1. Classify traffic by assigning CoS values to ports.
2. Assign the CoS values to priority queues.

To assign CoS values to ports, use the Networking > QoS > LAN QoS > Default CoS page. In this example, port GE8 is connected to a computer, and port GE9 is connected to a voice gateway. The administrator classifies the voice traffic by assigning the lowest CoS value, 1, to GE8 and the highest CoS value, 7, to GE9.



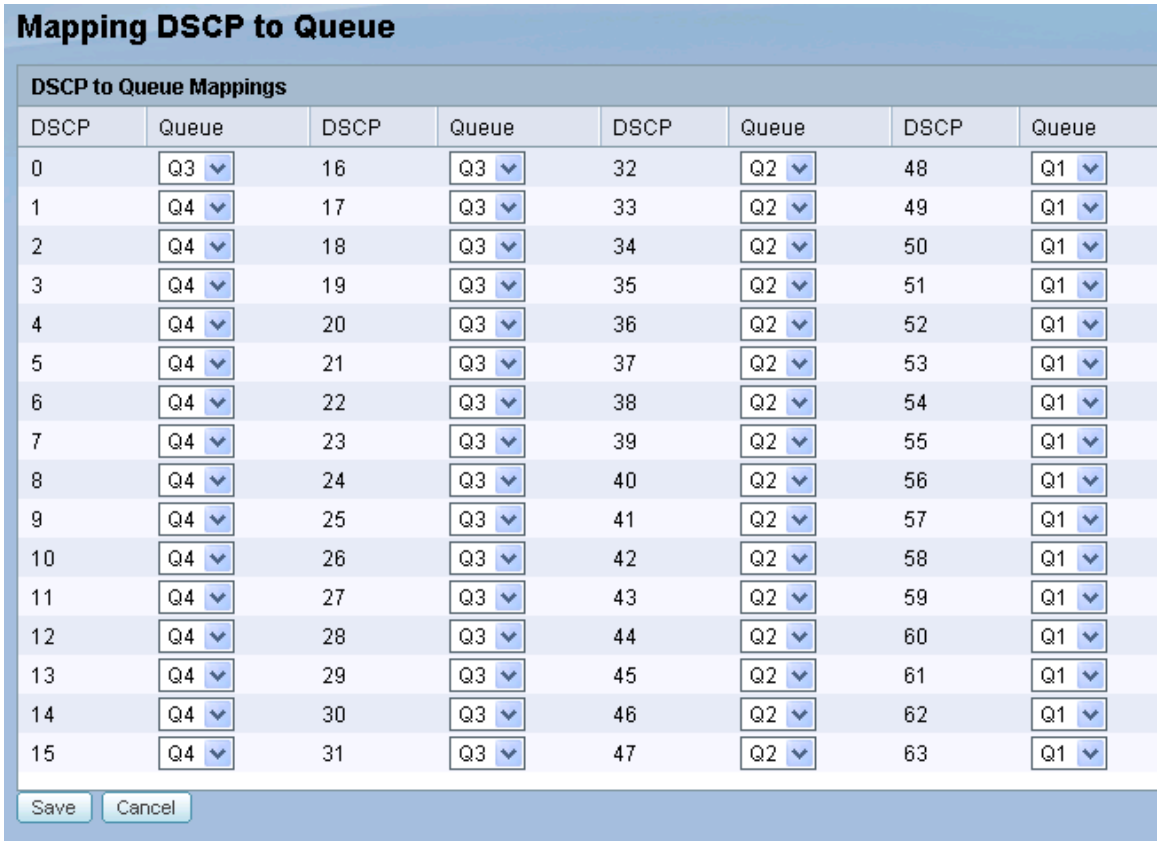
To assign CoS values to Queues, use the Networking > QoS > LAN QoS> Mapping CoS to Queue page.



Example: Using DSCP Values to prioritize LAN traffic

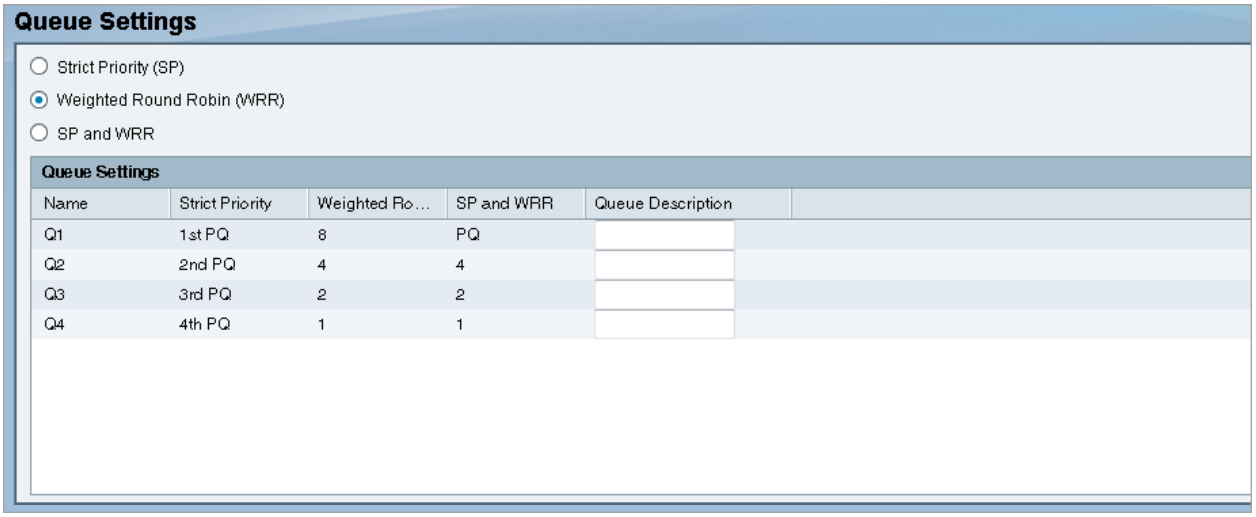
DSCP values are carried in the IP header of incoming traffic. By default, each DSCP value is mapped to a queue. The default mappings are valid for most purposes, but you can change the queues as needed.

You can review and modify these values on the Networking > QoS > LAN QoS > Mapping DSCP to Queue page.



Deciding How the LAN Priority Queues Operate

You can adjust the settings for the LAN priority queues on the Networking > QoS > LAN QoS > Queue Settings page. The ISA supports four LAN priority queues, from Q1 (highest) to Q4 (lowest). You can use different approaches: Strict Priority (SP), Weighted Round Robin (WRR), and Low Latency Queuing (LLQ).



- **Strict Priority (SP):** Traffic from Q1 is transmitted first. Traffic from the lower queues is processed only after the Q1 has transmitted, thus ensuring the highest level of bandwidth for Q1. A disadvantage of SP is that high traffic from Q1 may provide no opportunity for the lower queues to transmit.
- **Weighted Round Robin (WRR):** This option is selected by default. Traffic is sent from the queues in round-robin fashion. The number of packets sent from a queue is proportional to the predefined weight of the queue. The higher the weight, the more frames are sent. As compared to SP, WRR offers more opportunities for lower queues to transmit.
- **SP and WRR.** This option applies SP to Q1 and WRR to the other queues. The PQ weight is assigned to Q1 and the predefined weights 4, 2 and 1 are assigned to Q2, Q3, and Q4 respectively. There is no limit for PQ, indicating that WRR queues may not have an opportunity to transmit if PQ is sending high volumes of traffic.

Configuring QoS on Your Wireless Network

On a busy wireless network, you need to ensure that important and time-sensitive traffic is prioritized.

Enabling Wireless QoS

Use the Networking > QoS > General Settings page to enable QoS features on your wireless network. The Wireless QoS pages are unavailable until this setting is enabled.

If the wireless QoS is disabled, then traffic is managed according to the Wi-Fi Multimedia (WMM) standard. Wi-Fi Multimedia is enabled by default on the Wireless > Basic Setting page.

Choosing How to Classify Wireless Traffic

You can use DSCP or CoS values to classify wireless traffic on each SSID. DSCP is the default classification method. To change this setting, use the Networking > QoS > Wireless QoS > Classification Methods page.

Classifying and Prioritizing Wireless Traffic

Use the Wireless QoS pages to classify and prioritize wireless traffic. The procedures are the same as those for LAN QoS.

Ensuring QoS with VPN Traffic

The ISA supports QoS Pre-classify for IPSec VPN, and this feature is always enabled. The ISA will copy the DSCP value from the original IP header before encryption to the IP header. If the other device is QoS aware, it can classify the IPSec traffic according to the copied DSCP values.

Troubleshooting

If I add two overlapping class rules to a WAN QoS Priority Profile, which one will take priority?

The relative priority of the class rules is determined by the order in which they appear in the policy profile. The class rules that are lower in the list have precedence over the rules that are higher in the list.

Which WAN QoS priority queue will be used for general traffic by default?

Q6, the lowest queues is be used by default.

Can I limit the rate for multicast traffic?

Yes. You can set the destination address to multicast IP address to filter the traffic, then bind it to the WAN interface inbound direction.

Can I use QoS to limit the rate of DMZ server and port forwarding traffic?

Yes. For example, let's say that you set up a DMZ to allow Internet users to access an FTP server on your DMZ. You can configure your outbound QoS profile to limit the rate of FTP traffic so that users' downloads do not consume all of your bandwidth. When you set up the Traffic Selector, set the Source Address to the private IP address of the server. Likewise, you can configure an inbound policy profile to limit the bandwidth consumed by uploads from Internet users to your FTP server. In traffic selector for this class rule, set the Destination Address to the private IP address of the server.

Sometimes, after I modified the QoS setting, it doesn't take effect immediately.

When you apply a new QoS setting, it won't apply to traffic that is already queued or in the process of being transferred. If you want to stop all traffic and immediately enforce the new QoS setting, you can use the Firewall > Session Limits page to disconnect all the sessions.

For More Information

Product Resources	Location
Product Documentation	www.cisco.com/go/isa500resources
Cisco Small Business Support Community	www.cisco.com/go/smallbizsupport
Cisco Small Business Support and Resources	www.cisco.com/go/smallbizhelp
Phone Support Contacts	www.cisco.com/go/sbsc
Firmware Downloads	www.cisco.com/go/isa500software
Cisco Partner Central for Small Business (Partner Login Required)	www.cisco.com/web/partners/sell/smb
Cisco Small Business Home	www.cisco.com/smb

78-21038-01