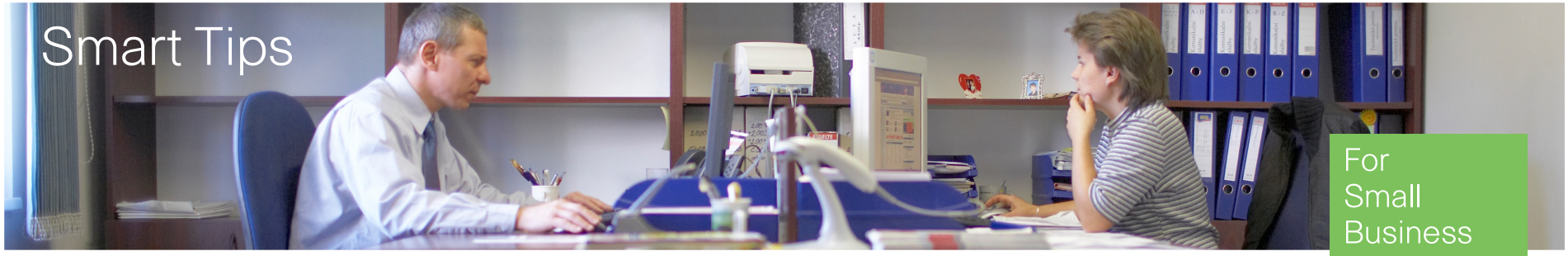


Configuring LAN Quality of Service for Cisco IP Telephony

As the number of devices and LAN traffic increases, traffic segregation, access control, and prioritizing traffic become key requirements. Cisco Small Business Managed Switches have advanced network management and other features that support business growth by providing greater control over network traffic.

Featured Products

This Smart Tip describes the use of a Cisco Small Business 300 Series Managed Switch (model SF 300-48P) with various Power over Ethernet (PoE) and non-PoE switch ports. For details about other Cisco 300 Series Managed Switches, visit: http://www.cisco.com/cisco/go/300switches.

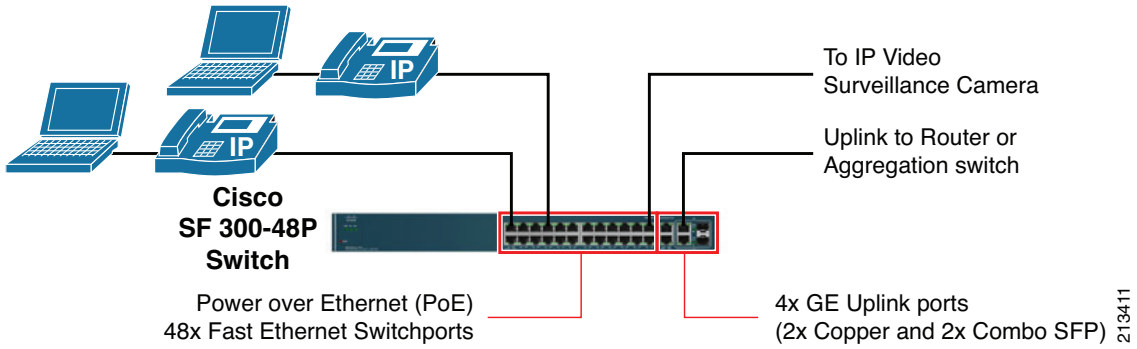
Figure 1 shows an example of the use of the Cisco SF 300-48P Switch in a small business LAN setting.

Why Quality of Service?

Quality of service (QoS) in a network device helps applications such as voice, streaming video, and other time-sensitive applications providing appropriate priority and adequate bandwidth to traffic during network congestion. Voice calls and streaming video may become choppy and jittery if overall traffic exceeds network capacity, so voice and video traffic must receive priority treatment, which is provided by QoS classification. In addition, QoS can provide configured amounts of bandwidth to traffic of other important applications during network congestion, thus ensuring business continuity during such events. Although QoS is of critical importance in a WAN router, a LAN switch can be congested as well, although less frequently; therefore, a switch also requires QoS configuration to avoid any potential degradation of voice or video quality.

This Smart Tip describes the steps to configure a Cisco SF 300-48P switch with QoS to support voice, streaming video (such as video surveillance), and other traffic types commonly found in a small business network. (See Figure 1.)

Figure 1 LAN with QoS



Design Tips

Traffic Classification

In Cisco Smart Design solutions, QoS is used to classify traffic into several traffic classes so that each class can be configured to get the kind of QoS treatment it requires. In Smart Design solutions, the traffic class of a packet is identified by the Differentiated Services Code Point (DSCP) or class of service (CoS) value of the packet. DSCP is a 6-bit field in the IP packet header that can be assigned a specific value to represent the type of QoS treatment the traffic needs. You can configure QoS to treat all packets carrying a specific DSCP value (or multiple specific DSCP values) as a single traffic class, distinct from other traffic classes. Common traffic classes, as defined in Smart Designs, are shown in the first two columns of Table 1.

Although switches forward traffic based on the Ethernet header and not the IP header of a packet, the Cisco Small Business 300 Series Managed Switches read the IP header to classify traffic based on the DSCP carried by the IP packets.

Alternatively, a switch can also classify packets matching a specific value of the 3-bit CoS field found on the Ethernet Header of 802.1q packets.

Note For certain types of QoS actions, the Cisco 300 Series switches also allow traffic classes based on a matching access control list (ACL).

The DSCP code *EF* denotes Expedited Forwarding, which requires that packets of this class should be forwarded with minimum delay, jitter, or packet loss. This DSCP, therefore, is applicable to the voice or real-time video traffic class.

In general, the DSCP codes starting with *AF* (Assured Forwarding) can range from AF11–AF13, AF21–AF23, AF31-AF33, or AF41–AF43. Assured Forwarding requires that traffic of this class must be assured to be forwarded as long as it does not exceed a certain configurable bandwidth limit. The two digits following the prefix *AF* represent AF-class and drop precedence (high, low, or medium). For example, in AF31, the AF-class is 3 and the drop precedence is 1 (drop precedence 1= low drop, 2= medium drop, 3 = high drop).

If congestion occurs among traffic classes with different AF-classes (AF1x, AF2x, AF3x, and AF4x), higher AF class traffic is preferred to be forwarded. However, if congestion occurs among traffic classes with the same AF class (for example, among AF11, AF12, AF13), traffic with high drop precedence is discarded first.

DSCP codes starting with *CS* (Class Selector) range from CS0 through CS7, and were created to be backward compatible with QoS systems that use IP precedence (rather than DSCP) for traffic classification. In practice, however, a combination of CS- and AF-based traffic marking is quite prevalent. CS codes have no drop precedence.

Traffic Marking

Marking is the process of setting or changing the DSCP or CoS value of a packet based on the traffic type. Cisco Smart Design solutions mark traffic as follows:

- Traffic from attached devices such as servers, network-attached storage (NAS), or surveillance cameras are marked to conform to the traffic classification described in the previous section, if the traffic source marks the traffic differently, or is not trusted.
- Incoming traffic with DSCPs other than those listed in Table 1 are marked to DSCP CS0 (best effort).

Table 1 Traffic Class Names, DSCP, and CoS Values

Traffic Description	Traffic Class Name	DSCP Code (Decimal Value)	CoS
Voice bearer traffic	Voice	EF (46)	5
Streaming video traffic; for example, from video surveillance camera (optional)	Streaming video	CS4 (32)	4
Signaling traffic for voice/video, and so on	Signaling	CS3 (24), AF31 (26)	3
Internetwork control traffic; control packets, such as dynamic routing generated by network devices	Internetwork control	CS6 (48)	6
Traffic from important (transactional) business applications (optional)	Transactional	CS2 (16), AF21 (18)	2
Bridge Protocol Data Unit (BPDU) packets exchanged between switches (only on switches)	BPDU	N/A	7
The rest of the traffic	Best Effort	CS0 (0)	0

Traffic Queuing

Queuing is used to allow various traffic classes to share bandwidth, and allow certain types of traffic (such as voice and video) to get priority treatment over other types of traffic. The Cisco 300 Series switch has four hardware queues. Each of these queues can be defined as a priority queue for expedited forwarding of traffic placed into the queue, or as a weighted round robin (WRR) queue that can share bandwidth with other WRR queues in a configured ratio. In addition, each queue can be individually shaped to a certain maximum rate; excess traffic above the shaped rate is dropped. Note that a switch port can be configured to police traffic as well; in which case, it can also drop traffic exceeding its configured rate. Each WRR queue is configured with a weight (or a bandwidth percentage). The switch forwards traffic from these queues in proportion to their weights, thus ensuring a minimum percentage of available bandwidth to each WRR queue after the priority queues are serviced.

This design assigns the traffic to the four hardware queues of Cisco Sx 300 switches as shown in Table 2 (these values can be changed in a deployment if necessary)

Table 2 Traffic Queuing Assignments

Traffic Class Name	DSCP	Queue #	Queue Type	WRR Weight	Remarks
Voice	EF	4	Priority		Shaped to 10% of line rate
Streaming video	CS4	3	Priority		Shaped to 40% of line rate
Signaling	CS3, AF31				
Internetwork control	CS6				
BPDU	CS7				
Transactional	CS2, AF21	2	WRR	1 (33.33%)	Equivalent to 33.33% of remaining bandwidth after both priority queues are serviced
Best effort	CS0	1	WRR	2 (66.67%)	66.67% of remaining bandwidth

In the design described in Table 2, traffic from queue #4 (priority queue with highest priority) is serviced first. When queue #4 is empty, traffic from queue #3 (the priority queue with lower priority) is serviced. Only when both these queues are empty, the remaining available bandwidth is shared among the WRR queues in proportion to their weights. The weights shown above provide 33.67% of remaining the bandwidth to queue 1 and 66.67% to queue 2.

Policing/Shaping Priority Queues

The priority queues do not have any bandwidth limit in the default configuration; thus, they can potentially use too much bandwidth, starving the other queues. Therefore, this design imposes a rate limit on each priority queue. Although the policing rates of individual priority queues can vary per deployment, a general recommendation is to limit the total priority traffic through any interface to not more than 50% of the interface bandwidth. This design shapes voice and video traffic to 10% and 40% of the interface bandwidth, assuming that the actual expected voice and video traffic will be far below these shaped rates.

TCP Congestion Avoidance (Optional)

The TCP Congestion Avoidance feature mitigates the effect of TCP synchronization that leads to underutilization of the network. This feature helps to improve network performance for TCP-based traffic by randomly dropping packets before network congestion occurs.

Without TCP Congestion Avoidance, when a queue gets full, all further incoming packets are dropped. This sudden spurt in packet drops may affect a large number of TCP applications. All these applications will be simultaneously forced to drastically reduce their sending rate, and then gradually increase it again. When the increasing sending rate exceeds a certain limit that fills up the queues, the queue drops all incoming packets again. This leads to a repeating sequence of overloading and underutilization of the network.

TCP Congestion Avoidance mitigates this issue by randomly dropping packets from the queues much before the queues get full. Rather than waiting to drop all the incoming traffic after the queue gets full. TCP Congestion Avoidance spreads the packet drops over time, thus avoiding simultaneous packet drops for large number of TCP flows.

In Cisco Smart Designs, this feature is essential for the WAN router, but is optional on the LAN switches, because configuring it on the WAN router also covers the traffic flowing through the LAN. However, if the WAN router does not support TCP Congestion Avoidance, it can be enabled on the LAN switches.

Configuration Tips

The configuration described in this section configures each port of a Cisco 300 Series switch (deployed either as an access switch or an aggregation switch in a Cisco Smart Design topology) with queuing features to support the traffic classes defined above. In addition, this configuration demonstrates how to configure a port to police and mark incoming traffic from a device attached to the switch.

Basic and Advanced QoS Modes

Cisco Sx300 switches can be configured to be in either basic or advanced QoS mode. Basic QoS mode supports the required queuing functionality (Priority and WRR queuing) and shaping the priority queues. However, this design uses the advanced QoS mode, because this mode is required to police/mark incoming traffic from specific switchports. It is typical to mark all traffic from traffic sources such as servers, NASes, and video cameras, if they do not mark the traffic, or if they are untrusted (not within the administrative control of the network administrator, or can potentially be exploited by an attacker). Advanced QoS mode allows you to specify the traffic for such policing/marking with great granularity; you can specify the source/destination IP addresses/subnets, their TCP/UDP protocols, and their ports. If such policing/marking of traffic flows is not required in a deployment, basic QoS mode is adequate.

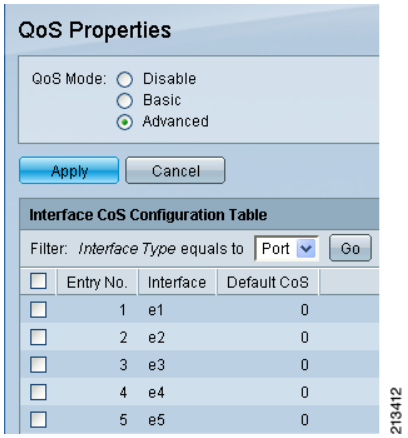
The following configuration steps assume you can access the web-based administration screen of the Cisco SF 300-48P switch. It is also assumed that the Data VLAN and Voice VLAN have been created on the switch and elsewhere in the network as needed, and the switch is connected with the WAN router, as shown in Figure 1.

To configure LAN QoS, complete the following steps:

Step 1 Select **Quality of Service > General > QoS Properties.**

This displays the QoS Properties screen, as shown in Figure 2.

Figure 2 QoS Properties Screen



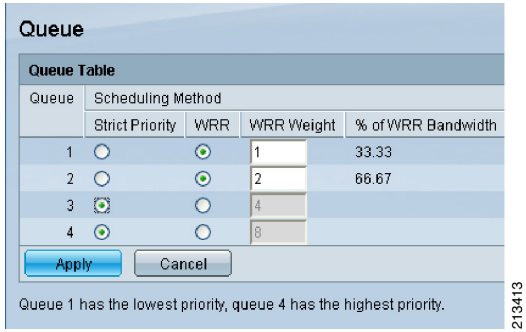
Step 2 Select *Advanced* in the QoS Mode field, and click **Apply**.

In the Interface CoS Configuration table, verify that the default CoS for all the switch ports are 0.

Step 3 Select **Quality of Service > General > QoS Properties > Queue**.

This displays the Queue screen, as shown in Figure 3.

Figure 3 Queue Screen



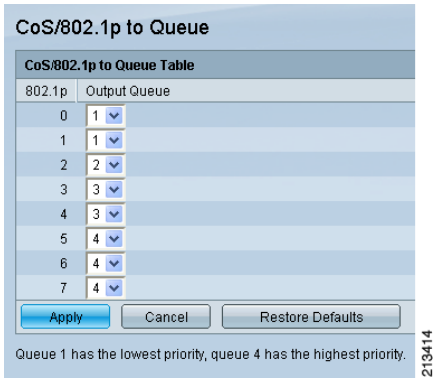
Step 4 In the Queue screen, configure the queues 1 and 2 as WRR queues with weights 1 and 2; configure the queues 3 and 4 as priority queues; and click **Apply**.

Queue 4 is for voice and 3 is for streaming video (if deployed). In addition, queue 3 also carries signaling traffic. Note that configuring these priority queues for voice and video is okay even when voice and video are not deployed, because the priority queues do not reserve any bandwidth; any unused traffic is used by the rest of the traffic classes.

Step 5 Select **Quality of Service > General > QoS Properties > QoS/802.1p to Queue**.

This displays the CoS/802.1P to Queue screen, as shown in Figure 4.

Figure 4 CoS/802.1P to Queue Screen

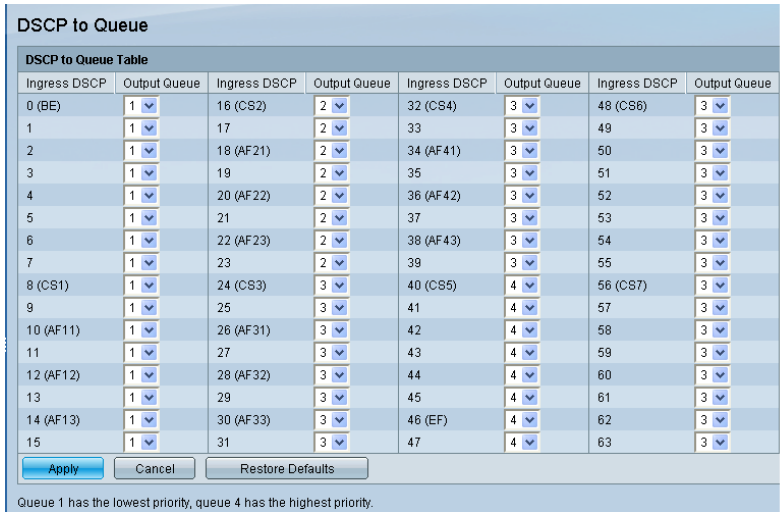


Step 6 Verify that the CoS values are mapped to the queues as in Figure 4, or change the mapping accordingly, and click **Apply**.

Step 7 Select **Quality of Service > General > QoS Properties > DSCP to Queue.**

This displays the DSCP to Queue screen, as shown in Figure 5.

Figure 5 DSCP to Queue Screen

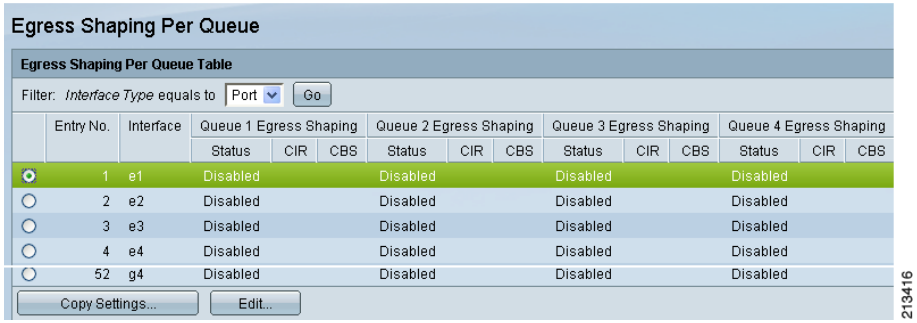


Step 8 Verify that the DSCPs are mapped to the queues as in Figure 5, or change the mapping accordingly, and click **Apply**.

Step 9 Select **Quality of Service > General > QoS Properties > Egress Shaping per Queue.**

This displays the Egress Shaping per Queue screen, as shown in Figure 6.

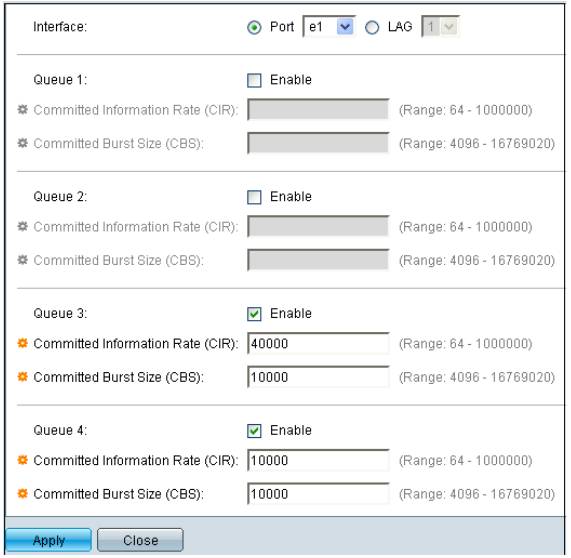
Figure 6 Egress Shaping per Queue Screen



Step 10 In the Egress Shaping Per Queue screen, select the first port E1 as in Figure 6, and click **Edit**.

This displays the popup screen shown in Figure 7.

Figure 7 Popup Screen



Step 11 In the popup screen shown in Figure 7, do the following:

a. Click the selection buttons to enable shaping on queues 3 and 4.

b. Enter values as shown in Figure 7 to shape queue 3 with CIR 40000 Kbps and with CBS 10000.

c. Shape queue 4 with CIR 10000 Kbps and with CBS 10000.

d. Click **Apply**.

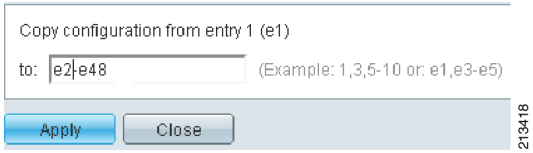
e. When "Success" is displayed, click **Close**.

This closes the popup screen and displays the Egress Shaping Per Queue screen. Verify that the port E1 now shows the shaping values entered in the Egress Shaping per Queue Screen.

Step 12 On the Egress Setting per Queue screen, click **Copy Settings** to copy the shaping configuration of E1 port to all other ports of the switch.

On the popup screen, enter the range of Fast Ethernet ports of the switch, as shown in Figure 8, and click **Apply**.

Figure 8 Copy Configuration Screen



The Copy Configuration popup screen closes. Verify that Egress Shaping Per Queue screen now displays the shaping values for all the switch ports.

Repeat this step for the Gigabit Ethernet ports (G1 to G4). Use CIR=400000 and CBS=100000 for queue 3; and CIR=100000 and CBS=100000 for queue 4.

Optional—This and the following steps are required if you want to police and/or mark incoming traffic from a device connected to the switch. This example polices the traffic from a video surveillance camera (IP address 10.1.20.5) to 500 Kbps. Traffic in excess of 500 Kbps is dropped, while traffic within the policing rate is marked with DSCP CS4.

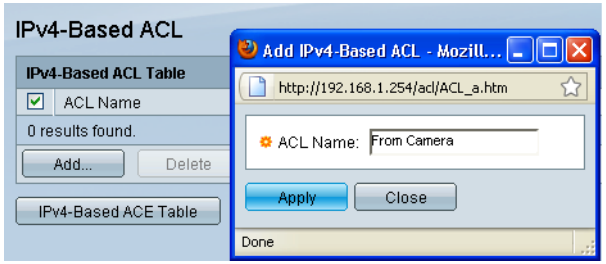
This procedure includes the following main steps:

- Creating a traffic class using an access control list (ACL) that matches the IP address of the video camera
- Creating a QoS policy table that contains one or more policy class maps
- Creating a policy class map that specifies the policing/marking actions to be done for the specific traffic class
- Attaching the policy class map to the switch port that is connected to the video camera

Step 13 To create an ACL that identifies the traffic from the camera, select **Access Control > IPv4 based ACL**.

This displays the IPv4-Based ACL screen, as shown in Figure 9.

Figure 9 IPv4-Based ACL Screen



Step 14 Click the **ACL Name** selection box, and click **Add**.

This displays the Add IPv4-Based ACL popup screen, as shown in Figure 9.

Step 15 Enter the name of the ACL (for example, *From Camera*), and click **Apply**.

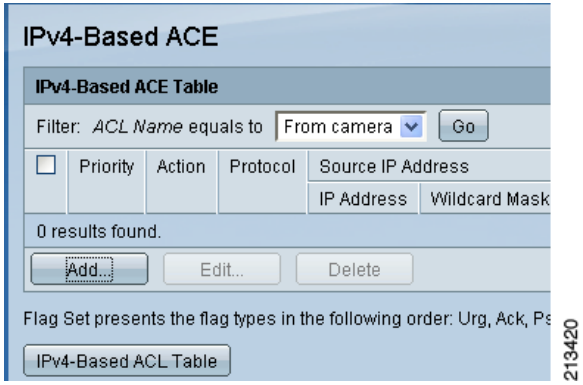
This removes the popup data entry screen, and displays the entered data on the IPv4-Based ACL screen.

Step 16 Click the **IPv4-Based ACE Table** button.

This displays the IPv4-Base ACE screen (partially shown in Figure 10).

Note An ACL consists of one/more access control expressions (ACEs).

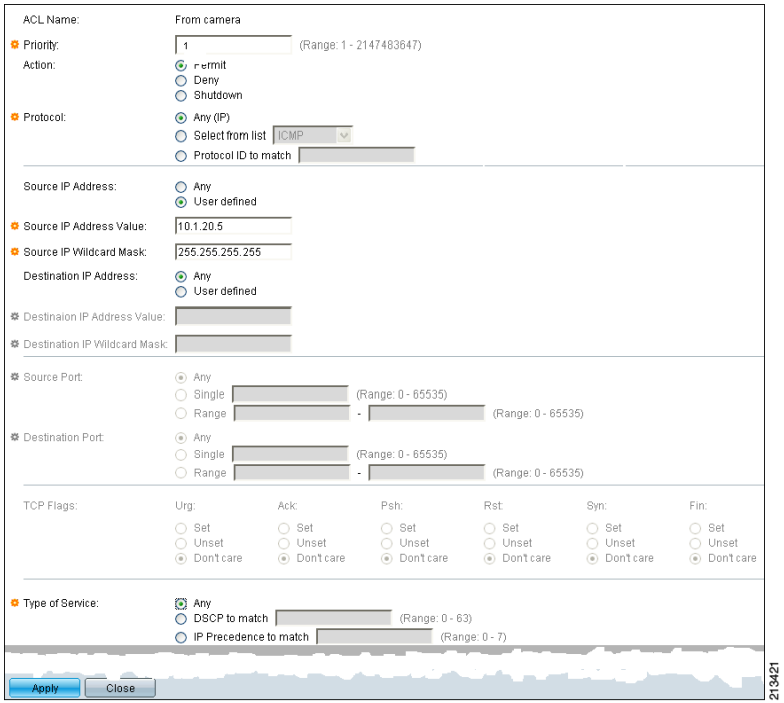
Figure 10 Add IPv4-Based ACE Screen



Step 17 Click **Add**.

This displays the screen partially shown in Figure 11 to enter details of the access control entries (ACE) to be included in the ACL *From Camera*. Multiple ACEs can be included if desired.

Figure 11 Entering ACE Details



Step 18 Enter the ACE data as follows:

a. Priority—1 (priority determines the order in which multiple ACEs, if any, of an ACL are evaluated)

b. Source IP address as that of the camera—10.1.20.5

c. Source IP wildcard mask—255.255.255.255

Step 19 Click **Apply.**

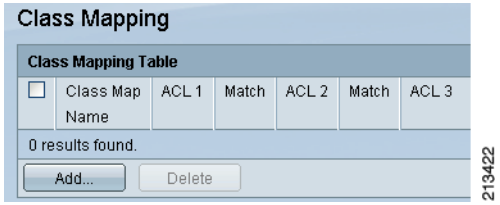
This creates the ACL with the single ACE you just entered.

Note You can additionally specify destination IP address/subnet, protocol, and TCP/UCP port in the ACE entry as applicable for any ACE.

Step 20 Select **Quality of Service > QoS Advanced Mode > Class Mapping.**

This displays the Class Mapping screen, as shown in Figure 12. A class map defines the rule to identify the traffic class (in this case, it uses a predefined ACL to match the traffic from the video camera, as shown below).

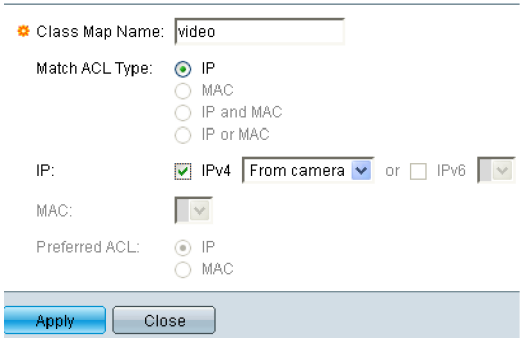
Figure 12 Class Mapping Screen



Step 21 Click **Add** to add a new class map using the ACL just created.

The popup screen to create a new class map appears, as shown in Figure 13.

Figure 13 Creating a New Class Map



Step 22 In the popup screen, do the following:

a. In the Class Map Name field, enter *video*.

b. In the Match ACL Type field, check **IP**.

c. In the IP field, check **IPv4**.

d. Select the **From Camera** ACL from the dropdown list.

e. Click **Apply**, and verify that the operation was successful.

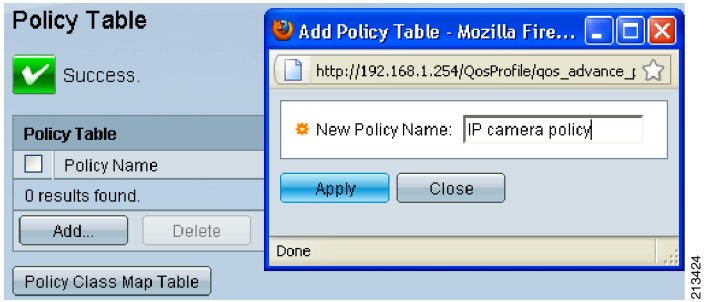
Step 23 Select **Quality of Service > QoS Advanced Mode > Policy Table.**

This displays the Policy Table screen.

Step 24 Click **Add** to add a new policy.

The popup screen shown in Figure 14 is displayed.

Figure 14 Policy Table Screen



Step 25 Enter the policy table name (*IP camera policy* in this example).

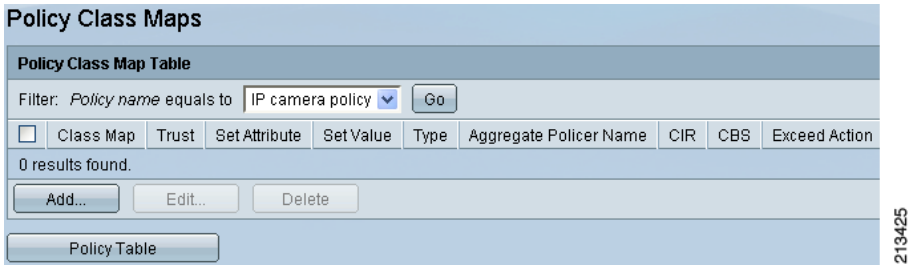
Step 26 Click **Apply**.

This removes the popup screen and displays "Success" on the Policy Table screen, along with the newly created policy name.

Step 27 To add the actual traffic policy (policing, marking, and so on), to be included in the policy table just created, select **Quality of Service > QoS Advanced Mode > Policy Class Map.**

The Policy Class Maps screen appears, as shown in Figure 15.

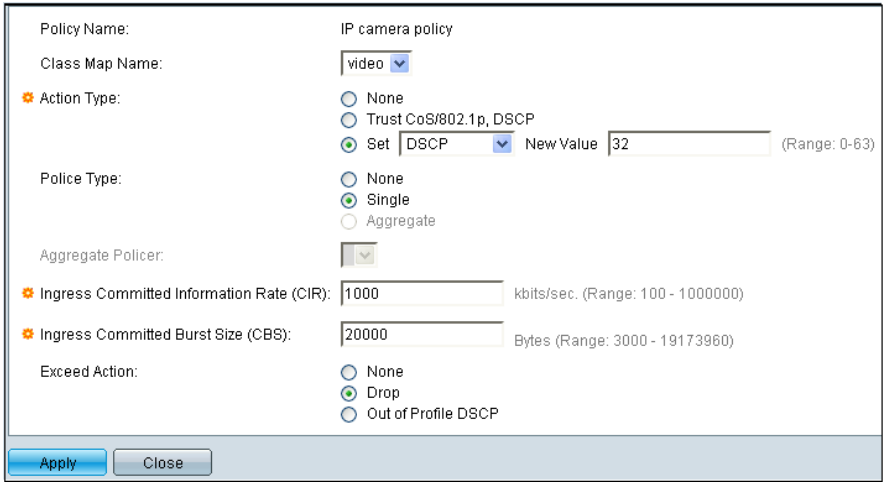
Figure 15 Policy Class Maps Screen



Step 28 Select the policy name (*IP camera policy*) from the dropdown menu and Click **Add**.

This displays the screen shown in Figure 16 to add the policing/marking actions to be taken for traffic matching this policy.

Figure 16 Adding Policing/Marking Actions



Step 29 In the screen shown in Figure 16, do the following:

a. Select the class map **video** from the dropdown list.

b. Click the radio button to select Set operation, and select **DSCP** from the corresponding dropdown list.

c. Enter *32* (that is, DSCP CS4) in the New Value field. This sets the DSCP to CS4 for all traffic matching class map *video*.

d. Assuming you want to police traffic from the IP camera to 1 Mbps, and drop the excess traffic, enter the values *1000 Kbps* in the Ingress Committed Information Rate field, and *20000* in the Ingress Committed Burst Size field.

e. In the Exceed Action field, check **Drop**.

f. Click **Apply**.

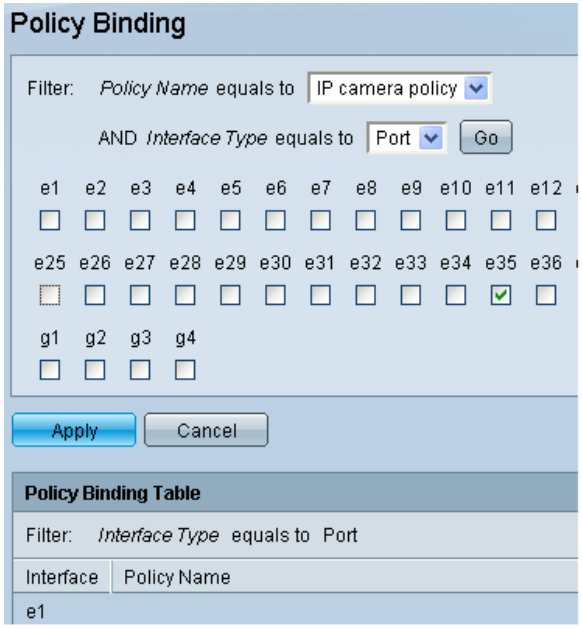
g. Verify that "Success" is displayed to indicate successful operation.

h. Click **Close** to close the popup screen.

Step 30 Select **Quality of Service > QoS Advanced Mode > Policy Binding.**

This displays the Policy Binding screen, as shown in Figure 17.

Figure 17 Policy Binding Screen



This is used to apply the policy you just created to the switch port connected to the IP video surveillance camera (switch port *E35* in this example).

Step 31 In the Policy Binding Screen, do the following:

a. Select the policy name (*IP camera policy*) from the dropdown list of policies to apply.

b. Select the interface type as *port* from the dropdown list.

c. Click the selection box indicating the switch port (*E 35* in this example) where the policy *IP camera policy* is to be applied (you can also apply a single policy on more than one switch ports, if required).

d. Click **Apply**.

On successful operation, this displays "Success" on the screen, and the name of the policy (*IP camera policy*) is displayed against the port E35 in the Policy Binding table.

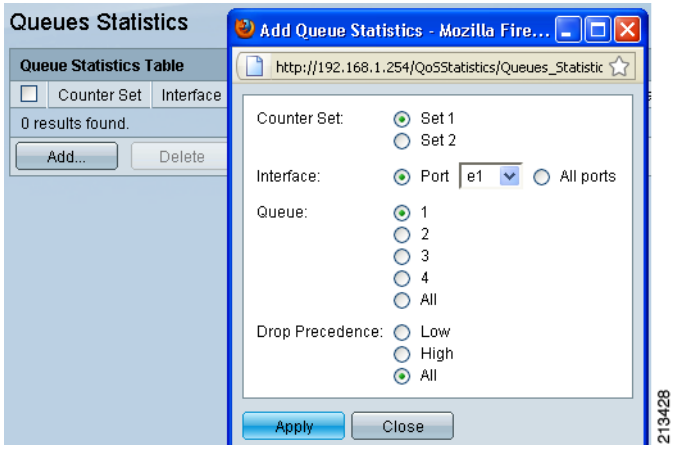
This completes the QoS configuration on the switch.

Verification

Step 1 Select **Quality of Service > QoS Statistics > Queues Statistics.**

This displays the Queues Statistics screen, which allows you to configure up to two sets of packet counters, as shown in Figure 18.

Figure 18 Queues Statistics Screen



Step 2 Click **Add** to add the first counter set.

The Add Queue Statistics popup screen is displayed, as shown in Figure 18.

Step 3 In the Add Queue Statistics popup screen, do the following:

a. Enter values to choose switch port, queue, and drop precedence values for the statistics.

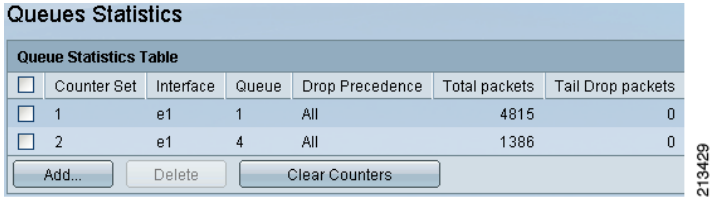
b. Click **Apply**.

c. Verify that "Success" is displayed, indicating successful operation.

d. Click **Close**.

This displays the actual packet counts, as shown in Figure 19.

Figure 19 Checking the Actual Packet Counts



You can clear the counters by checking the **Clear Counters** button. Check periodically that the packet count increase in various queues is per QoS configuration.

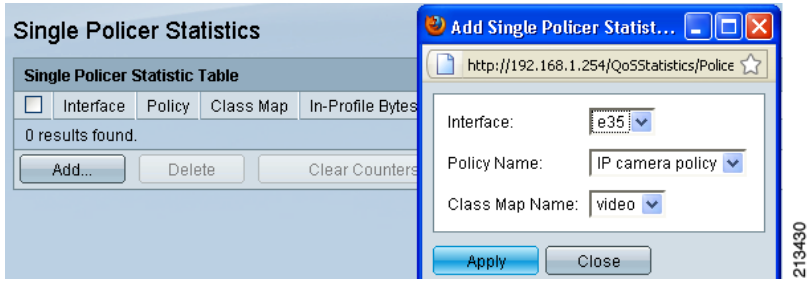
Step 4 Select **Quality of Service > QoS Statistics > Single Policer Statistics.**

This displays the Single Policer Statistics screen, which allows you to specify the port, policy name, and so on, for which statistics are required.

Step 5 Click **Add**.

This displays the Add Single Policer popup screen as shown in Figure 20.

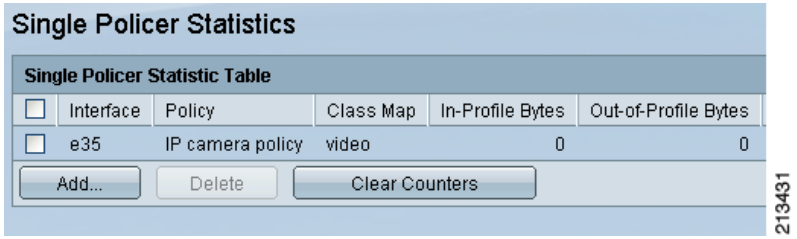
Figure 20 Add Single Policer Popup Screen



Step 6 Enter the switch port name (*E35*), policy name, and class map name you are interested in, and then click **Apply**.

This displays the policing statistics as shown in Figure 21.

Figure 21 Single Policer Statistics Screen



To test whether policing works or not, temporarily set the policing rate to a low value and verify that the excess traffic over the policing rate are counted as Out-of-Profile Bytes.

Summary

This Smart Tip defines the various types of QoS features that can be used within a network, particularly focusing on the LAN. When QoS is configured within the Cisco Small Business 300 Series switches, they can provide the appropriate QoS treatment for the Cisco Smart Design traffic classes. The Cisco 300 Series Managed Switch supports additional QoS functionalities that can be used if required.

For more information on configuring the Cisco 300 Series Managed Switches, see the Administrator Guide at the following URL: http://www.cisco.com/en/US/docs/switches/lan/csbms/sf30x_sg30x/administration_guide/78-19308-01.pdf.