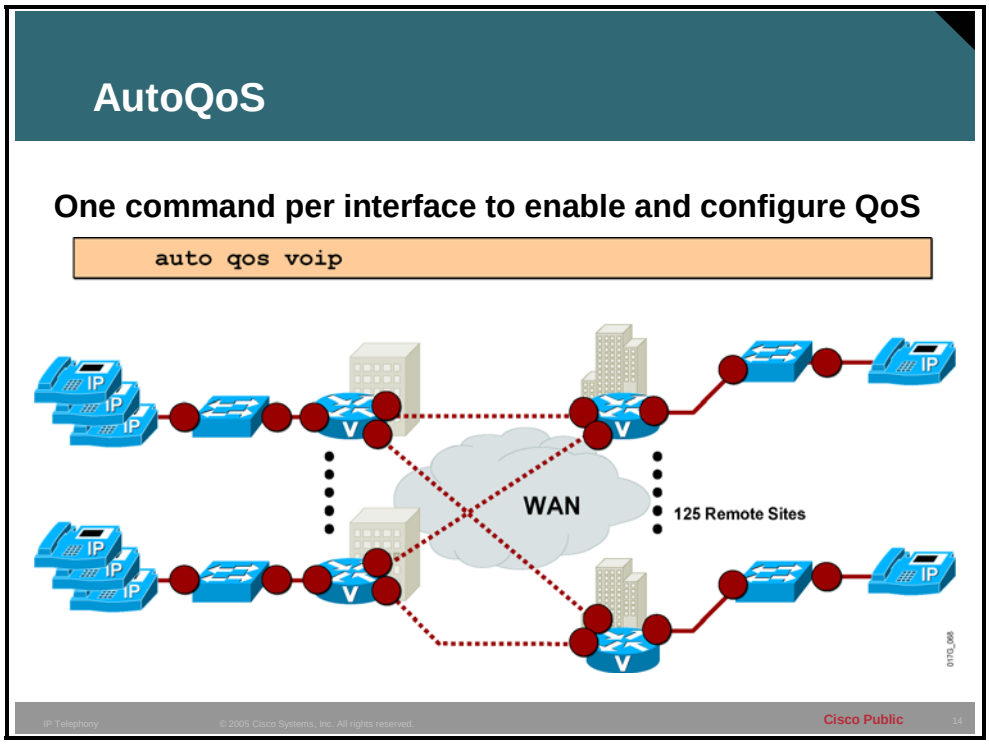
Implementing AutoQoS

AutoQoS

This topic describes the basic purpose and function of AutoQoS.

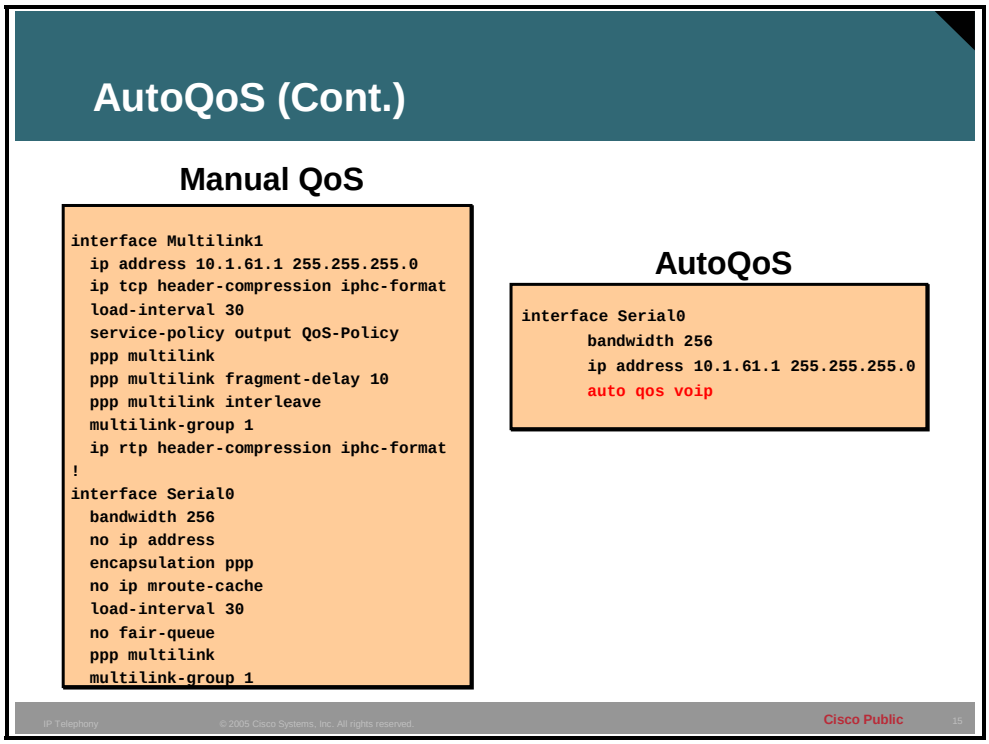


AutoQoS enables customer networks the ability to deploy QoS features for converged IP telephony (IPT) and data networks much faster and more efficiently. It simplifies and automates the Modular QoS CLI (MQC) definition of traffic classes, and the creation and configuration of traffic policies (Cisco AutoQoS generates traffic classes and policy maps CLI templates). Therefore, when AutoQoS is configured at the interface or PVC, the traffic receives the required QoS treatment automatically. In-depth knowledge of the underlying technologies, service policies, link efficiency mechanisms, and Cisco QoS best practice recommendations for voice requirements is not required to configure AutoQoS.

Cisco AutoQoS can be extremely beneficial for the following scenarios:

- Small-to-medium size businesses that need to deploy IPT quickly, but lack the experience and staffing to plan and deploy IP QoS services.
- Large customer enterprises that need to deploy Cisco AVVID on a large scale, while reducing the costs, complexity, and timeframe for deployment and ensuring that the appropriate QoS for voice applications is being set in a consistent fashion.
- International enterprises or service providers requiring QoS for VoIP where little expertise exists in different regions of the world and where provisioning QoS remotely and across different time zones is difficult.

- Service providers requiring a template-driven approach to delivering managed services and QoS for voice traffic to large numbers of customer premise devices.



Cisco AutoQoS automatically creates the QoS-specific features required for supporting the underlying transport mechanism and link speed of an interface or PVC type. For example, traffic shaping (FRTS) would be automatically configured and enabled by Cisco AutoQoS for Frame Relay links. LFI and RTP header compression (cRTP) would be automatically configured via the Cisco AutoQoS template for slow link speeds (less than 768 kbps). Therefore, it is very important that the bandwidth statement be properly set on the interface prior to configuring AutoQoS as the resulting configuration will vary based on this configurable parameter.

Using Cisco AutoQoS, VoIP traffic is automatically provided with the required QoS template for voice traffic by configuring **auto qos voip** on an interface or PVC. Cisco AutoQoS enables the required QoS based on Cisco best practice methodologies (the configuration generated by Cisco AutoQoS can be modified if desired).

AutoQoS (Cont.)

- **Application Classification**
  - **Automatically discovers applications and provides appropriate QoS treatment**
- **Policy Generation**
  - **Automatically generates initial an ongoing QoS policies**
- **Configuration**
  - **Provides high level business knobs, and multi-device / domain automation for QoS**
- **Monitoring & Reporting**
  - **Generates intelligent, automatic alerts and summary reports**
- **Consistency**
  - **Enables automatic, seamless interoperability among all QoS features and parameters across a network topology – LAN, MAN, and WAN**

Cisco AutoQoS simplifies and shortens the Quality of Service deployment cycle. Cisco AutoQoS helps in all five major aspects of successful QoS deployments:

- **Application Classification:** Cisco AutoQoS leverages intelligent classification on routers, utilizing Cisco Network-Based Application Recognition (nBAR) to provide deep and stateful packet inspection. Cisco AutoQoS uses Cisco Discovery Protocol (CDP) for voice packets, ensuring that the device attached to the local area network (LAN) is really an IP phone.
- **Policy Generation:** Cisco AutoQoS evaluates the network environment and generates an initial policy. It automatically determines WAN settings for fragmentation, compression, encapsulation, and Frame Relay-ATM interworking, eliminating the need to understand QoS theory and design practices in various scenarios. Customers can meet additional or special requirements by modifying the initial policy as they normally would.

  The first release of Cisco AutoQoS provides the necessary AutoQoS-VoIP feature to automate QoS settings for VoIP deployments. This feature automatically generates interface configurations, policy maps, class maps, and ACLs. AutoQoS-VoIP will automatically employ Cisco nBAR to classify voice traffic, and mark it with the appropriate differentiated services code point (DSCP) value. AutoQoS-VoIP can be instructed to rely on, or trust, the DSCP markings previously applied to the packets.
- **Configuration:** With one command, Cisco AutoQoS configures the port to prioritize voice traffic without affecting other network traffic, while still offering the flexibility to adjust QoS settings for unique network requirements.

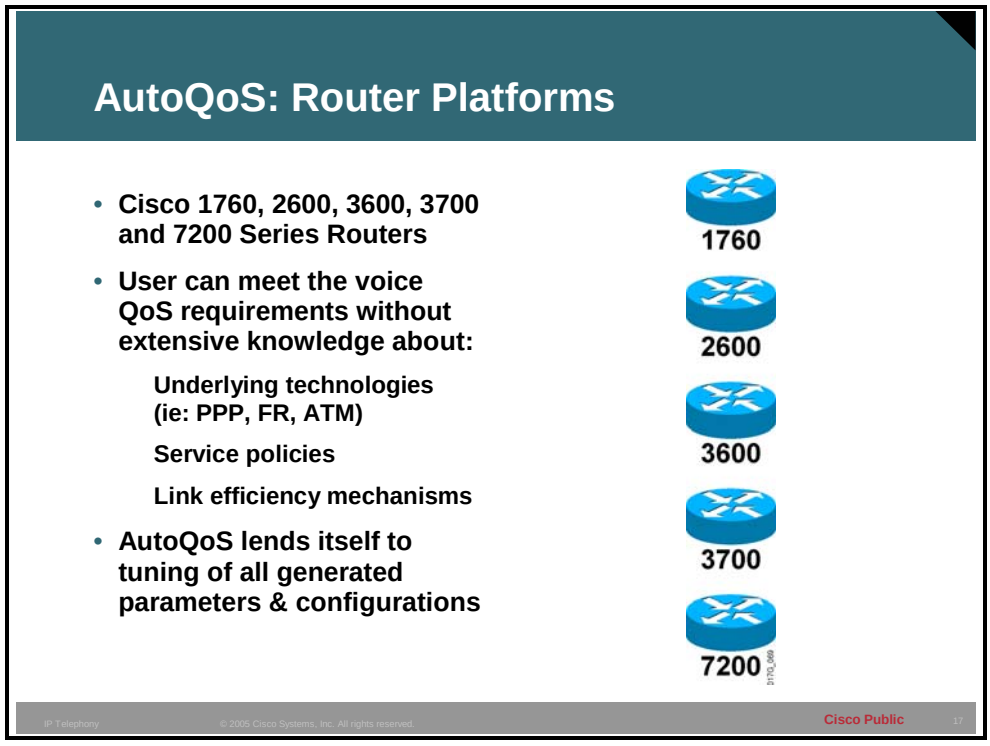
  Not only will Cisco AutoQoS automatically detect Cisco IP Phones and enable QoS settings, it will disable the QoS settings when a Cisco IP phone is relocated or moved to prevent malicious activity.

AutoQoS generated router and switch configurations are customizable using the standard Cisco IOS CLI.

- **Monitoring & Reporting:** Cisco AutoQoS provides visibility into the classes of service deployed via system logging and Simple Network Management Protocol (SNMP) traps, with notification of abnormal events (ie: VoIP packet drops).

AutoQoS: Router Platforms

This topic identifies the router and switch platforms on which AutoQoS will operate.



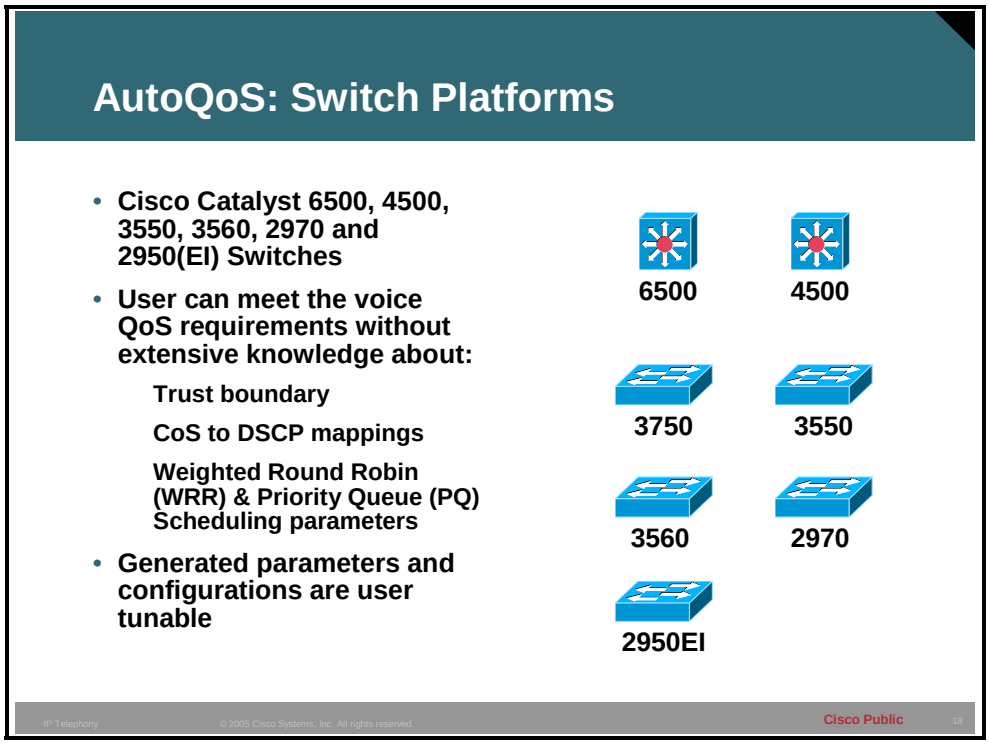
Initial support for AutoQoS includes the Cisco 2600, 2600-XM, 3600, 3700, and 7200 series routers. Support for additional platforms will become available.

Cisco AutoQoS VoIP feature is supported only on the following interfaces and PVCs:

- Serial interfaces with Point-to-Point (PPP) or High-Level Data Link Control (HDLC)
- Frame Relay DLCIs (point-to-point sub-interfaces only)
  - Cisco AutoQoS does not support Frame Relay multipoint interfaces
- ATM PVCs
  - Cisco AutoQoS VoIP is supported on low-speed ATM PVCs on point-to-point sub-interfaces only (link bandwidth less than 768 kbps)
  - Cisco AutoQoS VoIP is fully supported on high-speed ATM PVCs (link bandwidth greater than 768 kbps)

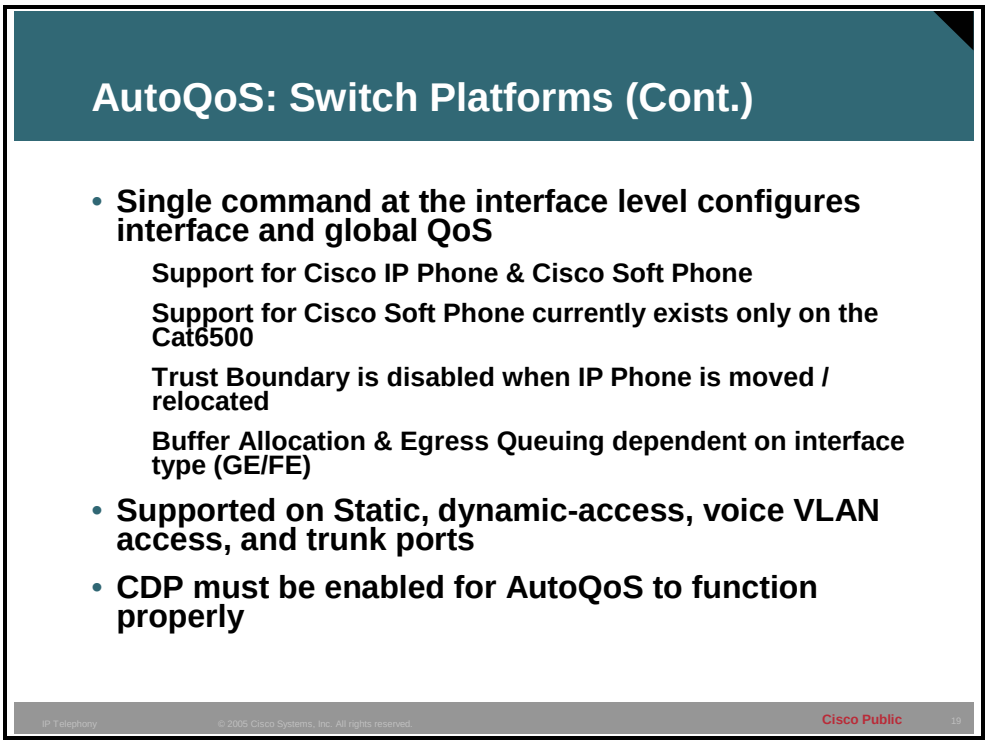
AutoQoS: Switch Platforms

This topic identifies the switch platforms on which AutoQoS will operate.



Initial support for AutoQoS includes the Cisco Catalyst 6500, 4500, 3550, 3560, 2970 and 2950EI series switches. Support for additional platforms including the Cisco Catalyst 4000 will become available.

The Enhanced Image (EI) is required on the Cisco Catalyst 2950 Series Switches.



To configure the QoS settings and the trusted boundary feature on the Cisco IP Phone, you must enable Cisco Discovery Protocol (CDP) version 2 or later on the port. If you enable the trusted boundary feature, a syslog warning message displays if CDP is not enabled or if CDP is running version 1.

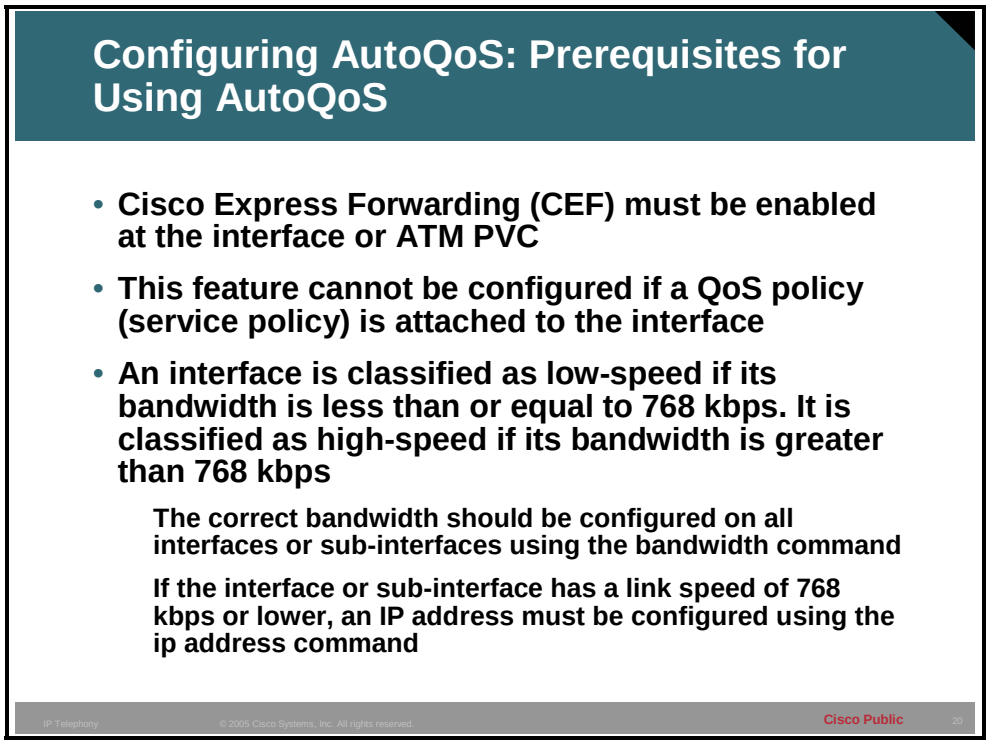
You need to enable CDP only for the **ciscoipphone** QoS configuration; CDP does not affect the other components of the automatic QoS features. When you use the **ciscoipphone** keyword with the port-specific automatic QoS feature, a warning displays if the port does not have CDP enabled.

When executing the port-specific automatic QoS command with the **ciscoipphone** keyword without the trust option, the trust-device feature is enabled. The trust-device feature is dependent on CDP. If CDP is not enabled or not running version 2, a warning message displays as follows:

```
Console> (enable) set port qos 4/1 autoqos voip ciscoipphone
Warning: CDP is disabled or CDP version 1 is in use. Ensure
that CDP version 2 is enabled globally, and also ensure that
CDP is enabled on the port(s) you wish to configure autoqos
on.
Port 4/1 ingress QoS configured for ciscoipphone.
It is recommended to execute the "set qos autoqos" global
command if not executed previously.
Console> (enable)
```

AutoQoS Prerequisites

This topic describes some of the key prerequisites for using AutoQoS.



Before configuring AutoQoS, the following prerequisites must be met:

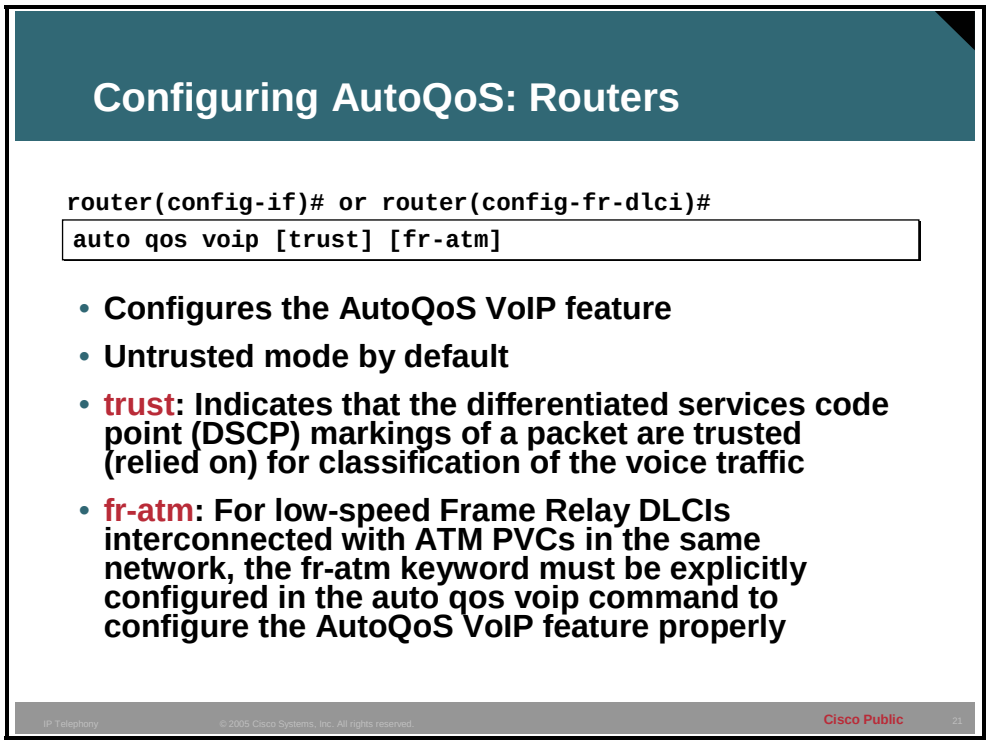
- Cisco Express Forwarding (CEF) must be enabled at the interface or ATM PVC. Cisco AutoQoS uses Network Based Application Recognition (NBAR) to identify various applications and traffic types and CEF is a prerequisite for NBAR.
- Ensure that no QoS policies (service policies) are attached to the interface. This feature cannot be configured if a QoS policy (service policy) is attached to the interface.
- AutoQoS classifies links as either low-speed or high-speed depending upon the link bandwidth. Remember that on a serial interface, the default bandwidth if not specified is 1.544 Mbps. Therefore, it is important that the correct bandwidth be specified on the interface or sub-interface where AutoQoS is to be enabled.
  - For all interfaces or sub-interfaces, be sure to properly configure the bandwidth by using the bandwidth command. The amount of bandwidth allocated should be based on the link speed of the interface.
  - If the interface or sub-interface has a link speed of 768 kbps or lower, an IP address must be configured on the interface or sub-interface using the **ip address** command. By default, AutoQoS will enable multilink PPP and copy the configured IP address to the multilink bundle interface.

In addition to the AutoQoS prerequisites, the following are recommendations and requirements when configuring AutoQoS. Be aware that these may change with Cisco IOS releases and should be verified before implementing AutoQoS in your environment.

- Cisco AutoQoS VoIP feature is supported only on the following interfaces and PVCs:
  - Serial interfaces with Point-to-Point (PPP) or High-Level Data Link Control (HDLC)
  - Frame Relay DLCIs (point-to-point sub-interfaces only)
    - Cisco AutoQoS does not support Frame Relay multipoint interfaces
  - ATM PVCs
- Configuration template (CLI) generated by configuring Cisco AutoQoS on an interface or PVC can be tuned manually (via CLI configuration) if desired.
- Cisco AutoQoS cannot be configured if a QoS service-policy is already configured and attached to the interface or PVC.
- Multi-link PPP (MLP) is configured automatically for a serial interface with low-speed link. The serial interface must have an IP address and this IP address is removed and put on the MLP bundle. Cisco AutoQoS VoIP must also be configured on the other side of the link
- The **no auto qos voip** command removes Cisco AutoQoS. However, if the interface or PVC Cisco AutoQoS generated QoS configuration is deleted without configuring the **no auto qos voip** command, Cisco AutoQoS VoIP will not be completely removed from the configuration properly.
- Cisco AutoQoS SNMP traps are only delivered when an SNMP server is used in conjunction with Cisco AutoQoS.
- The SNMP community string "AutoQoS" should have "write" permissions.
- If the device is reloaded with the saved configuration after configuring Cisco AutoQoS and saving the configuration to NVRAM, some warning messages may be generated by RMON threshold commands. These warnings messages can be ignored (to avoid further warning messages, save the configuration to NVRAM again without making any changes to the QoS configuration).
- By default, Cisco 7200 Series routers and below that support MQC QoS, reserve up to 75% of the interface bandwidth for user defined classes. The remaining bandwidth is used for the default class. However, the entire remaining bandwidth is not guaranteed to the default class. This bandwidth is shared proportionately between the different flows in the default class and excess traffic from other bandwidth classes. At least one percent of the available bandwidth is reserved and guaranteed for class default traffic by default (up to 99% can be allocated to the other classes) on Cisco 7500 Series Routers

Configuring AutoQoS

This topic describes how to configure AutoQoS.



To configure the AutoQoS VoIP feature on an interface, use the **auto qos voip** command in interface configuration mode or Frame Relay DLCI configuration mode. To remove the AutoQoS VoIP feature from an interface, use the **no** form of the **auto qos voip** command.

auto qos voip [trust] [fr-atm]

no auto qos voip [trust] [fr-atm]

Syntax Description

Parameter	Description
trust	(Optional) Indicates that the differentiated services code point (DSCP) markings of a packet are trusted (relied on) for classification of the voice traffic. If the optional trust keyword is not specified, the voice traffic is classified using Network-Based Application Recognition (NBAR), and the packets are marked with the appropriate DSCP value.
fr-atm	(Optional) Enables the AutoQoS – VoIP feature for the Frame Relay-to-ATM links. This option is available on the Frame Relay data-link connection identifiers (DLCIs) for Frame Relay-to-ATM interworking only.

The bandwidth of the serial interface is used to determine the speed of the link. The speed of the link is one element used to determine the configuration generated by the AutoQoS VoIP feature. The AutoQoS VoIP feature uses the bandwidth at the time the feature is configured and does not respond to changes made to bandwidth after the feature is configured.

For example, if the auto **qos voip** command is used to configure the AutoQoS VoIP feature on an interface with 1000 Kbps, the AutoQoS VoIP feature generates configurations for high-speed interfaces. However, if the bandwidth is later changed to 500 Kbps, the AutoQoS VoIP feature will not use the lower bandwidth. The AutoQoS VoIP feature retains the higher bandwidth and continues to use the generated configurations for high-speed interfaces.

To force the AutoQoS VoIP feature to use the lower bandwidth (and thus generate configurations for the low-speed interfaces), use the **no auto qos voip** command to remove the AutoQoS VoIP feature and then reconfigure the feature.

Example: Configuring the AutoQoS VoIP Feature on a High-Speed Serial Interface

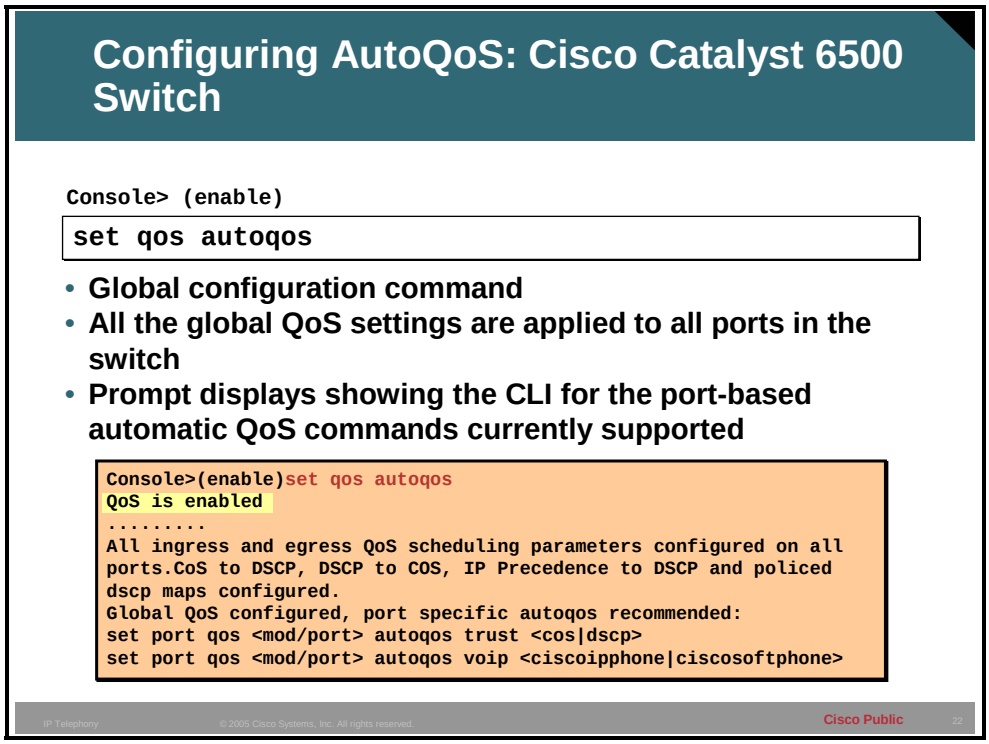
In this example, the AutoQoS VoIP feature is configured on the high-speed serial interface s1/2.

```
Router> enable
Router# configure terminal
Router(config)# interface s1/2
Router(config-if)# bandwidth 1540
Router(config-if)# ip address 10.10.100.1 255.255.255.0
Router(config-if)# auto qos voip
Router(config-if)# exit
```

Example: Configuring the AutoQoS VoIP Feature on a Low-Speed Serial Interface Example

In this example, the AutoQoS VoIP feature is configured on the low-speed serial interface s1/3.

```
Router# configure terminal
Router(config)# interface s1/3
Router(config-if)# bandwidth 512
Router(config-if)# ip address 10.10.100.1 255.255.255.0
Router(config-if# auto qos voip
Router(config-if)# exit
```



When you execute the global automatic QoS macro, all the global QoS settings are applied to all ports in the switch. After completion, a prompt displays showing the CLI for the port-based automatic QoS commands currently supported.

Configuring AutoQoS: Cisco Catalyst 6500 Switch (Cont.)

```
Console> (enable)
set port qos autoqos <mod/port> trust [cos|dscp]
```

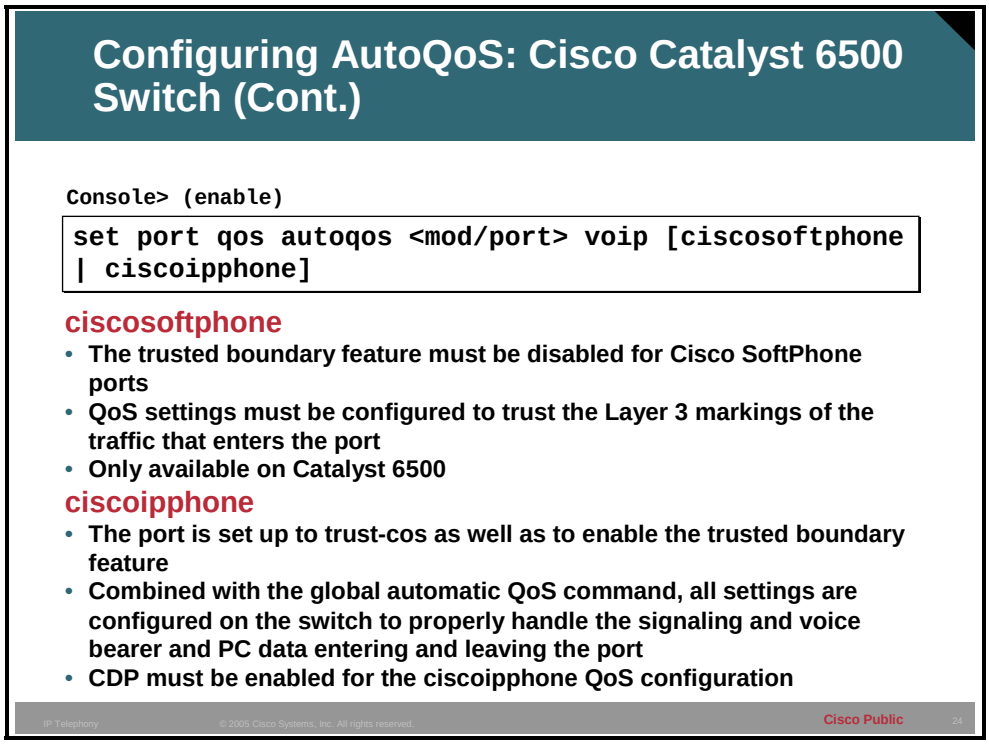
- **trust dscp and trust cos are automatic QoS keywords used for ports requiring a "trust all" type of solution.**
- **trust dscp should be used only on ports that connect to other switches or known servers as the port will be trusting all inbound traffic marking Layer 3 (DSCP)**
- **trust cos should only be used on ports connecting other switches or known servers as the port trusts all inbound traffic marking in Layer 2 (CoS).**
- **The trusted boundary feature is disabled and no QoS policing is configured on these types of ports**

The port-specific automatic QoS macro handles all inbound QoS configuration that is specific to a particular port.

The QoS ingress port specific settings include port trust, default CoS, classification, and policing but does not include scheduling. Input scheduling is programmed through the global automatic QoS macro. Together with the global automatic QoS macro command, all QoS settings are configured properly for a specific QoS traffic type.

Any existing QoS ACLs that are already associated with a port are removed if AutoQoS modifies ACL mappings on that port. The ACL names and instances are not changed.

If the trust dscp or trust cos keywords are used, the trusted boundary feature is disabled. This means an IP Phone will not rewrite the dscp or cos values from an attached PC.



The port-specific automatic QoS macro accepts a *mod/port* combination and must include an AVVID-type keyword. The **ciscoipphone**, **ciscosoftphone**, and **trust** keywords are supported.

With the **ciscoipphone** keyword, the port is set up to trust-cos as well as to enable the trusted boundary feature. Combined with the global automatic QoS command, all settings are configured on the switch to properly handle the signaling and voice bearer and PC data entering and leaving the port.

In addition to the switch-side QoS settings covered by the global automatic QoS command, the phone has a few QoS features that need to be configured for proper labeling to occur. QoS configuration information is sent to the phone through CDP from the switch. The QoS values that need to be configured are the trust settings of the "PC port" on the phone (trust or untrusted) and the CoS value that is used by the phone to remark packets in case the port is untrusted (ext-cos).

Only the Catalyst 6500 supports AutoQoS for Cisco SoftPhone. On the ports that connect to a Cisco SoftPhone, QoS settings must be configured to trust the Layer 3 markings of the traffic that enters the port. Trusting all Layer 3 markings is a security risk because PC users could send non-priority traffic with DSCP 46 and gain unauthorized performance benefits. Although not configured by AutoQos, policing on all inbound traffic can be used to prevent malicious users from obtaining unauthorized bandwidth from the network. Policing is accomplished by rate limiting the DSCP 46 (EF) inbound traffic to the codec rate used by the Cisco SoftPhone application (worst case G.723). Any traffic that exceeds this rate is marked down to the default traffic rate (DSCP 0 - BE). Signaling traffic (DSCP 24) is also policed and marked down to zero if excess signaling traffic is detected. All other inbound traffic types are reclassified to default traffic (DSCP 0 - BE).

Note	You must disable the trusted boundary feature for Cisco SoftPhone ports.

Example: Using the Port-Specific AutoQoS Macro

This example shows how to use the **ciscoipphone** keyword:

```
Console> (enable) set port qos 3/1 autoqos help
Usage: set port qos <mod/port> autoqos trust <cos|dscp>
set port qos <mod/port> autoqos voip
<ciscoipphone|ciscosoftphone>
Console> (enable) set port qos 3/1 autoqos voip ciscoipphone
Port 3/1 ingress QoS configured for Cisco IP Phone.
It is recommended to execute the "set qos autoqos" global
command if not executed previously.
Console> (enable)
```

This example shows how to use the **ciscosoftphone** keyword:

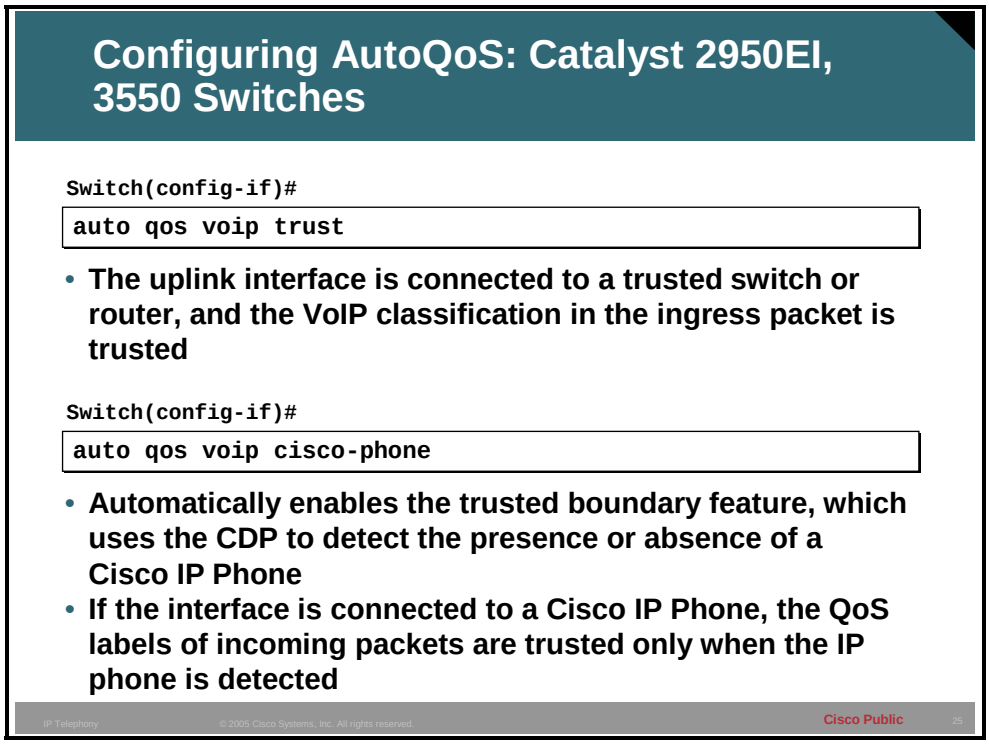
```
Console> (enable) set port qos 3/1 autoqos voip ciscosoftphone
Port 3/1 ingress QoS configured for Cisco Softphone.
It is recommended to execute the "set qos autoqos" global
command if not executed previously.
Console> (enable)
```

This example shows how to use the **trust cos** keyword:

```
Console> (enable) set port qos 3/1 autoqos trust cos
Port 3/1 QoS configured to trust all incoming CoS marking.
It is recommended to execute the "set qos autoqos" global
command if not executed previously.
Console> (enable)
```

This example shows how to use the **trust dscp** keyword:

```
Console> (enable) set port qos 3/1 autoqos trust dscp
Port 3/1 QoS configured to trust all incoming DSCP marking.
It is recommended to execute the "set qos autoqos" global
command if not executed previously.
Console> (enable)
```



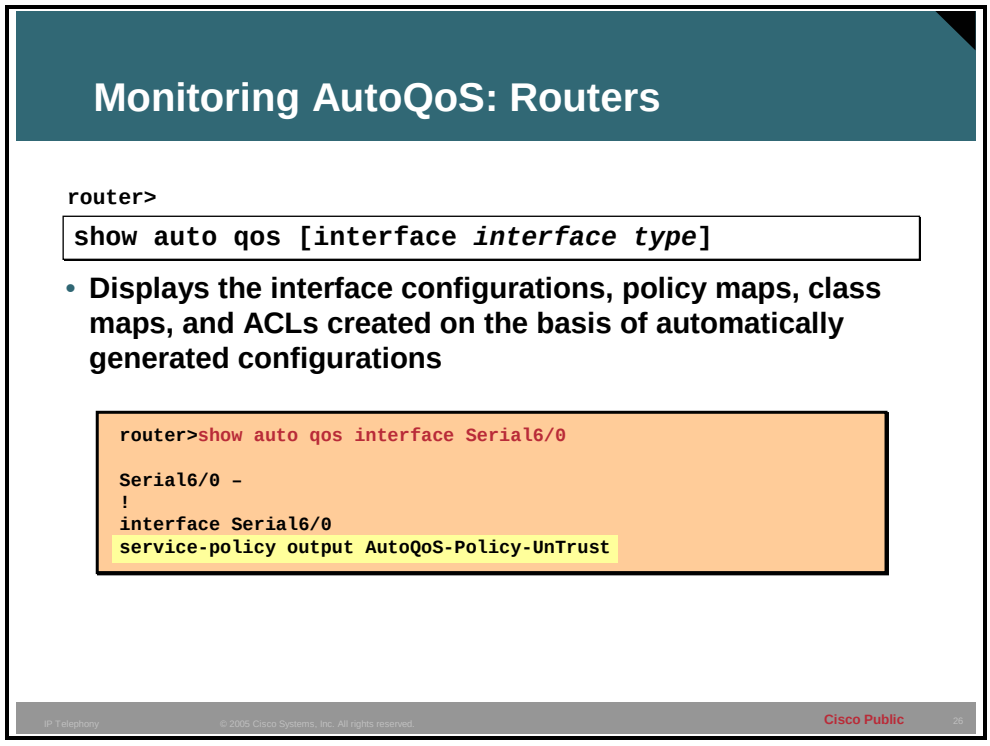
When you enable the AutoQoS feature on the first interface, QoS is globally enabled (**mls qos** global configuration command).

When you enter the **auto qos voip trust** interface configuration command, the ingress classification on the interface is set to trust the CoS QoS label received in the packet, and the egress queues on the interface are reconfigured. QoS Labels in ingress packets are trusted

When you enter the **auto qos voip cisco-phone** interface configuration command, the trusted boundary feature is enabled. It uses the Cisco Discovery Protocol (CDP) to detect the presence or absence of a Cisco IP phone. When a Cisco IP phone is detected, the ingress classification on the interface is set to trust the QoS label received in the packet. When a Cisco IP phone is absent, the ingress classification is set to not trust the QoS label in the packet. The egress queues on the interface are also reconfigured. This command extends the trust boundary if IP Phone detected.

Monitoring AutoQoS

This topic describes the commands used to monitor AutoQoS configurations.



When the **auto qos voip** command is used to configure the AutoQoS VoIP feature, configurations are generated for each interface or permanent virtual circuit (PVC). These configurations are then used to create the interface configurations, policy maps, class maps, and access control lists (ACLs). The **show auto qos** command can be used to verify the contents of the interface configurations, policy maps, class maps, and ACLs.

The **show auto qos interface** command can be used with Frame Relay data-link connection identifiers (DLCIs) and ATM PVCs.

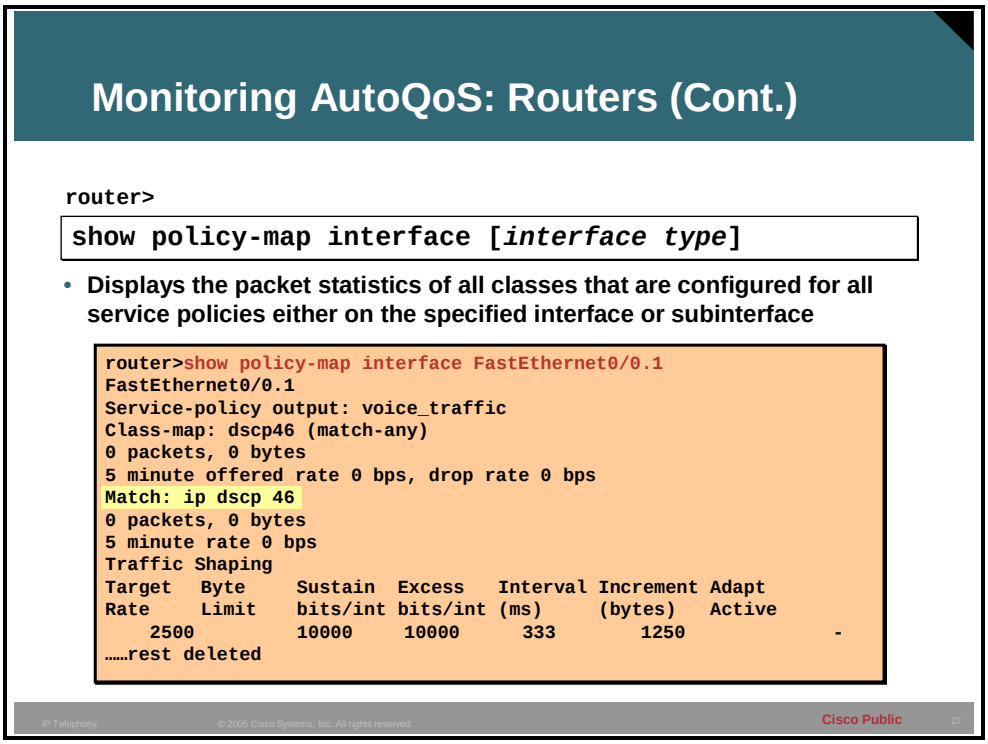
When the **interface** keyword is used along with the corresponding interface type argument, the **show auto qos interface** [*interface type*] command displays the configurations created by the AutoQoS VoIP feature on the specified interface.

When the **interface** keyword is used but an interface type is not specified, the **show auto qos interface** command displays the configurations created by the AutoQoS VoIP feature on all the interfaces or PVCs on which the AutoQoS VoIP feature is enabled.

Example: Show Auto QoS and Show Auto QoS Interface

The **show auto qos** command displays all of the configurations created by the AutoQoS VoIP feature.

```
Router# show auto qos
Serial6/1.1: DLCI 100 -
!
interface Serial6/1
frame-relay traffic-shaping
!
interface Serial6/1.1 point-to-point
frame-relay interface-dlci 100
class AutoQoS-VoIP-FR-Serial6/1-100
frame-relay ip rtp header-compression
!
map-class frame-relay AutoQoS-VoIP-FR-Serial6/1-100
frame-relay cir 512000
frame-relay bc 5120
frame-relay be 0
frame-relay mincir 512000
service-policy output AutoQoS-Policy-UnTrust
frame-relay fragment 640
```

To display the configuration of all classes configured for all service policies on the specified interface or to display the classes for the service policy for a specific permanent virtual circuit (PVC) on the interface, use the **show policy-map interface** EXEC or privileged EXEC command.

show policy-map interface interface-name [**vc** [***vpi/***] ***vci***][**dlci** ***dlci***] [**input | output**]

Monitoring AutoQoS: Switches

```
Switch#
show auto qos [interface interface-id]
```

- **Displays the auto-QoS configuration that was initially applied**
- **Does not display any user changes to the configuration that might be in effect**

```
Switch#show auto qos
Initial configuration applied by AutoQoS:
wrr-queue bandwidth 20 1 80 0
no wrr-queue cos-map
wrr-queue cos 1 0 1 2 4
wrr-queue cos 3 3 6 7
wrr-queue cos 4 5
mls qos map cos-dscp 0 8 16 26 32 46 48 56
!
interface FastEthernet0/3
mls qos trust device cisco-phone
mls qos trust cos
```


To display the inital auto-QoS configuration, use the **show auto qos** [**interface** [*interface-id*]] privileged EXEC command. To display any user changes to that configuration, use the **show running-config** privileged EXEC command. You can compare the **show auto qos** and the **show running-config** command output to identify the user-defined QoS settings.

Monitoring AutoQoS: Switches (Cont.)

```
Switch#
show mls qos interface [interface-id | vlan vlan-id]
[buffers | policers | queueing | statistics]
[ | {begin | exclude | include} expression]
```

- **Displays QoS information at the interface level**

```
Switch#show mls qos interface gigabitethernet0/1 statistics
Ingress
    dscp: incoming  no_change     classified      policed        dropped (in bytes)
      1 : 0         0             0               0              0
Others: 203216935   24234242      178982693       0              0

Egress
    dscp: incoming  no_change     classified      policed       dropped (in bytes)
      1 : 0         n/a           n/a             0             0

WRED drop counts:
      qid           thresh1   thresh2   FreeQ
     1 :  0         0         1024
     2 :  0         0         1024
……rest deleted
```

IP Telephony © 2005 Cisco Systems, Inc. All rights reserved. Cisco Public 29

Display QoS information at the interface level, including the configuration of the egress queues and the CoS-to-egress-queue map, which interfaces have configured policers, and ingress and egress statistics (including the number of bytes dropped).

If no keyword is specified with the **show mls qos interface** command, the port QoS mode (DSCP trusted, CoS trusted, untrusted, and so forth), default class of service (CoS) value, DSCP-to-DSCP-mutation map (if any) attached to the port, and policy map (if any) attached to the interface are displayed. If a specific interface is not specified, the information for all interfaces is displayed.

Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* are not displayed, but the lines that do not contain *output* are displayed.

Monitoring AutoQoS: Switches (Cont.)

```
Switch#
show mls qos maps [cos-dscp | dscp-cos | dscp-
mutation dscp-mutation-name | dscp-switch-priority |
ip-prec-dscp | policed-dscp] [ | {begin | exclude |
include} expression
```

- **Maps are used to generate an internal Differentiated Services Code Point (DSCP) value, which represents the priority of the traffic**

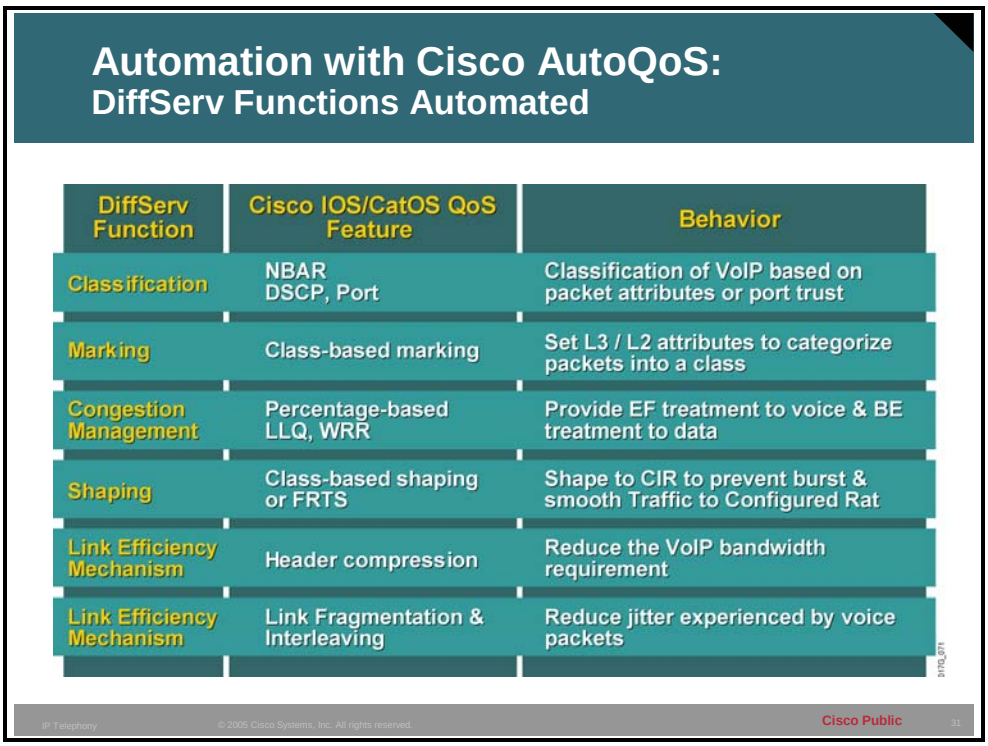
```
Switch#show mls qos maps dscp-cos

Dscp-cos map:
   dscp: 0 8 10 16 18 24 26 32 34 40 46 48 56
         ------------------------------------------
    cos: 0 1 1 2 2 3 7 4 4 5 5 7 7
```


This command shows the current mapping of DSCP to CoS.

Automation with Cisco AutoQoS

This topic identifies several of the QoS technologies that are automatically implemented on the network when using AutoQoS.



Cisco AutoQoS performs the following functions:

WAN:

- Automatically classify RTP payload and VoIP control packets (H.323, H.225 Unicast, Skinny, SIP, MGCP)
- Build service policies for VoIP traffic that are based on Cisco Modular QoS CLI (MQC)
- Provision Low Latency Queuing (LLQ) - Priority Queuing for VoIP bearer and bandwidth guarantees for control traffic
- Enable WAN traffic shaping that adheres to Cisco best practices, where required
- Enable link efficiency mechanisms, such as Link Fragmentation and Interleaving (LFI), and RTP header compression (cRTP) where required
- Provide SNMP and SYSLOG alerts for VoIP packet drops

LAN:

- Enforce the trust boundary on Cisco Catalyst switch access ports and uplinks/downlinks
- Enable Cisco Catalyst strict priority queuing (also known as expedite queuing) with weighted round robin (WRR) scheduling for voice and data traffic, where appropriate
- Configure queue admission criteria (Map CoS values in incoming packets to the appropriate queues)
- Modify queue sizes and weights where required