WHITE PAPER

AUTOQoS FOR VOICE OVER IP

Last Updated: September 2008

Customer networks exist to service application requirements and end users efficiently. The tremendous growth of the Internet and corporate intranets, the wide variety of new bandwidth-hungry applications, and convergence of data, voice, and video traffic over consolidated IP infrastructures has had a major impact on the ability of networks to provide predictable, measurable, and guaranteed services to these applications. Achieving the required Quality of Service (QoS) through the proper management of network delays, bandwidth requirements, and packet loss parameters, while maintaining simplicity, scalability, and manageability of the network is the fundamental solution to running an infrastructure that serves business applications end-to-end.

Cisco IOS® Software offers a portfolio of QoS features that enable customer networks to address voice, video, and data application requirements, and are extensively deployed by numerous Enterprises and Service Provider networks today. Cisco AutoQoS dramatically simplifies QoS deployment by automating Cisco IOS QoS features for voice traffic in a consistent manner and leveraging the advanced functionality and intelligence of Cisco IOS Software.

Figure 1 illustrates how Cisco AutoQoS provides the user a simple, intelligent Command Line Interface (CLI) for enabling campus LAN and WAN QoS for Voice over IP (VoIP) on Cisco switches and routers. The network administrator does not need to possess extensive knowledge of the underlying network technology (Point-to-Point (PPP), Frame Relay (FR), ATM, ATM to FR internetworking), required for QoS service policies, or link efficiency mechanisms needed to ensure voice quality and reduce latency, jitter, and packet drops.

AUTOQOS WAN BENEFITS

- Supports FR, ATM, PPP, HDLC, and FR-to-ATM internetworking
- Automatically classifies Realtime Transport Protocol (RTP) payload and VoIP control packets (H.323, SIP, MGCP)
- Builds QoS VoIP modular QoS policy in Cisco IOS Software
- Provides Low Latency Queuing (LLQ) for VoIP bearer traffic
- Provides minimum bandwidth guarantees (Class-Based Weighted Fair Queuing [CBWFQ]) for VoIP control traffic
- Enables WAN traffic shaping that adheres to Cisco best practices, where required
- Enables Cisco link efficiency mechanisms such as Link Fragmentation and Interleaving (LFI) and RTP header compression, compressed RTP (cRTP), where required
- Provides SNMP and SYSLOG alerts for VoIP packet drops

AUTOQOS CAMPUS LAN BENEFITS

- Enforces a trust boundary at the Cisco IP phone
- Enforces a trust boundary on Cisco Catalyst® switch access ports and uplinks/downlinks
- Enables Cisco Catalyst strict priority queuing and weighted round robin queuing for voice and data traffic where appropriate
- Modifies queue admission criteria (ie: Class of Service (CoS)-to-queue mapping)
- Modifies queue sizes, as well as queue weights where required
- Modifies CoS-to-DSCP and IP precedence-to-DSCP mappings

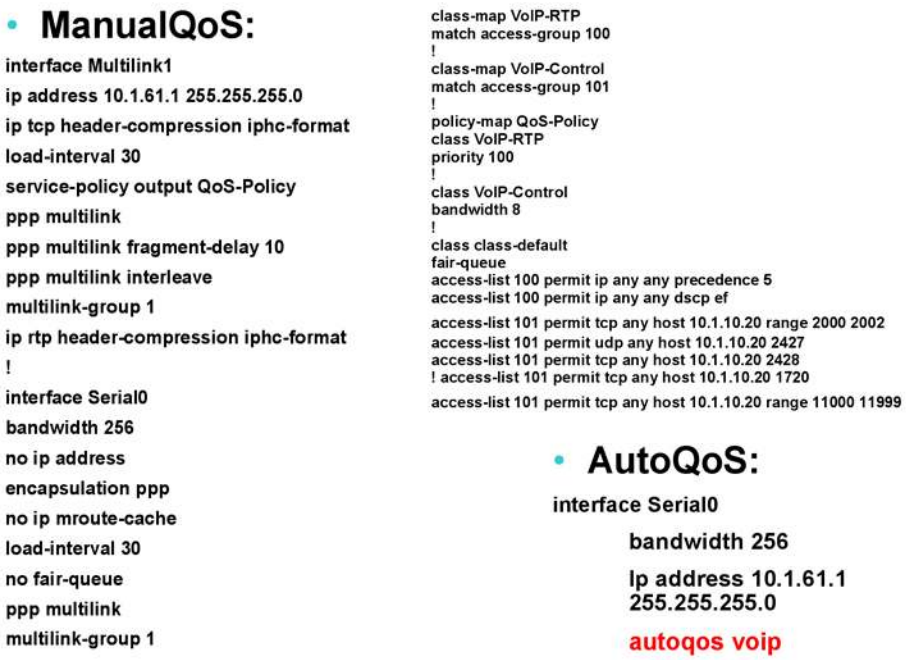
AutoQoS enables customer networks the ability to deploy QoS features for converged IP Telephony (IPT) and data networks much faster and more efficiently. It simplifies and automates the Modular QoS CLI (MQC) definition of traffic classes, creation and configuration of traffic policies (Cisco AutoQoS generates traffic classes and policy map 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 automatically creates the QoS-specific features required for supporting the underlying transport mechanism and link speed of an interface or PVC type. For example, Frame Relay Traffic Shaping (FRTS) would be automatically configured and enabled by Cisco AutoQoS for FR links. LFI and RTP header compression (cRTP) would be automatically configured via the Cisco AutoQoS template for slow link speeds (less than 768 kbps).

Cisco AutoQoS can be extremely beneficial for the following scenarios:

1. Small-to-medium size businesses that need to deploy IPT quickly, but lack the experience and staffing to plan and deploy IP QoS services.
2. 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 are being set in a consistent manner.
3. International Enterprises or Service Providers requiring QoS for VoIP where less expertise exists in different regions of the world and where provisioning QoS remotely and across different time zones is difficult.
4. Service Providers requiring a template-driven approach to delivering managed services and QoS for voice traffic to large numbers of customer premise devices.

Figure 1. Manual QoS vs. AutoQoS Configuration (Low-Speed 256 Kbps Serial Link)



OVERVIEW OF CISCO QOS MECHANISMS

QoS refers to the ability of a network to provide improved service to selected network traffic over various underlying technologies (ie: FR, ATM, Ethernet and 802.1 networks, SONET, and IP-routed networks). QoS features provide improved and more predictable network service with the following capabilities:

- Dedicated bandwidth for VoIP traffic
- Improved loss characteristics
- Congestion avoidance and congestion management
- Network traffic shaping to conform to inconsistencies in ingress/egress speeds
- Differentiated traffic priorities for applications across the network

Customer networks can leverage the extensive range of the Cisco QoS feature portfolio for optimal network efficiency, regardless of whether the network is a small corporation, large enterprise, or an Internet Service Provider (ISP). Different categories of networking users—such as major Enterprises, network Service Providers, and small and medium-sized business networking users—have their own QoS requirements, which overlap in many areas.

Enterprise networks, for example, must provide end-to-end QoS solutions across the various platforms that comprise the network; providing solutions for heterogeneous platforms often requires disparate QoS configuration approaches for each technology. Enterprise networks consistently carry more complex, mission-critical applications, and experience increased traffic from Web multimedia applications. QoS prioritizes this traffic to ensure that each application gets the level of service and bandwidth it needs.

ISPs require assured scalability and performance. For example, ISPs that offer best-effort IP connectivity now also transfer voice, video, and other real-time critical application data. QoS responds to the scalability and performance needs of these ISPs to distinguish different kinds of traffic, enabling them to offer service differentiation to their customers.

In the small and medium sized business segment, managers are experiencing firsthand the rapid growth of business on the Internet. These business networks must also handle increasingly complex business applications. QoS allows the network to handle the difficult task of utilizing an expensive WAN connection in the most efficient way for business applications.

Cisco QoS deployment delivers the following benefits:

- **Resource Control**: Network administrators can control which of their resources are allocated (ie: bandwidth, equipment, wide area facilities). For example, users can limit bandwidth consumed over a backbone link by File Transfer Protocol (FTP) transfers or give priority to an important database access.
- **Tailored Services**: QoS enables ISPs to offer tailored grades of service differentiation to the customer, based on the control and visibility it provides.
- **Coexistence of Mission-Critical Applications with those Applications that Require Less Priority**: Cisco QoS features insure that the WAN is used efficiently by those voice and mission-critical applications that are most important to the business. It can also ensure the availability of bandwidth for time-sensitive multimedia and voice applications, so these application experience only minimum delays (for example, other applications using a shared WAN link get their service without interfering with mission-critical traffic).

Voice traffic has strict requirements concerning packet loss, delay, and delay variation (also known as jitter). To meet the specific Service Level Agreement (SLA) requirements and guarantee voice quality over IP networks, Cisco IOS QoS includes features such as classification, queuing, traffic shaping, cRTP, and Transmission Control Protocol (TCP) header compression. Key elements of this infrastructure that enable Cisco IOS QoS for IP telephony traffic include the following:

- Traffic classification and marking
- Enhanced queuing services

- LFI
- cRTP
- LLQ
- Traffic shaping

QoS features can be separated into three major functional categories:

1. Traffic classification and marking
2. Queuing
3. Network provisioning

CLASSIFICATION AND MARKING

Packet classification features provide the capability to partition network traffic into multiple priority levels or classes of service. For example, by using the IETF defined differentiated services code points (DiffServ, RFC 2474 and 2475), networks can categorize application traffic into a maximum of sixty-four different traffic classes. Once packets are classified, the various QoS features in Cisco IOS Software can be used to assign the appropriate traffic handling policies (ie: congestion management, bandwidth allocation, and delay bounds) for each traffic class.

Packets can also be classified by external sources. For example, a customer or downstream network provider. The network can be enabled to accept the classification, or override it and reclassify the packet according to a policy that the network administrator specifies. Packets can be classified based on policies specified by the network operator. Policies can be set that include classification based on physical port, source or destination IP or MAC address, application port, Network-Based Application Recognition (NBAR) IP protocol type, and other criteria specified with using access lists or extended access lists. The Cisco MQC class-based packet marking capability in Cisco IOS Software provides a user-friendly CLI for efficient packet marking, users can differentiate packets based on the designated markings. For example, Cisco MQC QoS class-based packet classification allows customers to perform the following functions:

- Mark packets by setting IP Differentiated Services Code Point (DSCP) or IP precedence bits in the IP Type of Service (ToS) header
- Mark packets by setting the Layer 2 CoS value or the MPLS experimental bit
- Associate a local QoS group value with a packet
- Set Cell Loss Priority (CLP) bit setting in the ATM header of a packet from 0 to 1
- Set FR Discard Eligible (DE) bit from 0 to 1

Classification tools mark a packet or flow with a specific priority. This marking establishes a trust boundary that must be enforced. Classification should take place at the network edge, typically in the wiring closet switches, within the Cisco IP phones themselves, or at voice endpoints. Packets can be marked as important by using Layer 2 CoS settings in the user priority bits of the 802.1p portion of the 802.1Q header (Figure 2), or the IP precedence/DSCP bits in the ToS Byte of the IPv4 header (Figure 3). All IP phone RTP packets should be tagged with either:

- CoS value of 5 for the Layer 2 802.1p settings, and an DSCP value of Expedited Forwarding (EF) or
- IP precedence value of 5

Additionally, all control packets should be tagged with a Layer 2 CoS value of 3 and a Layer 3 DSCP value of 24-31 (or ToS value of 3). Table 1 lists the respective CoS, IP precedence, and DSCP settings for specifying packet priority.

Figure 2. Layer 2 CoS Settings

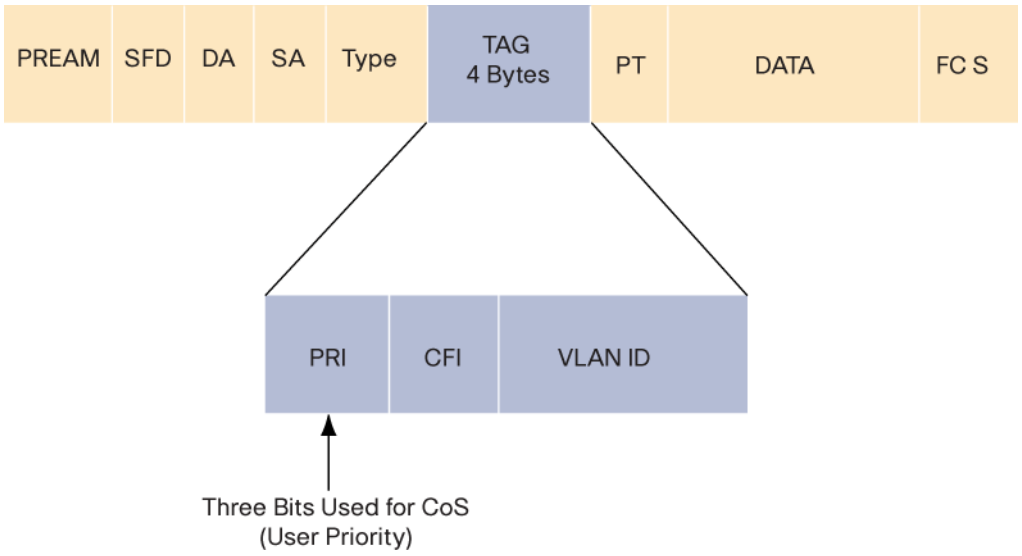


Figure 3. Layer 3 ToS Settings

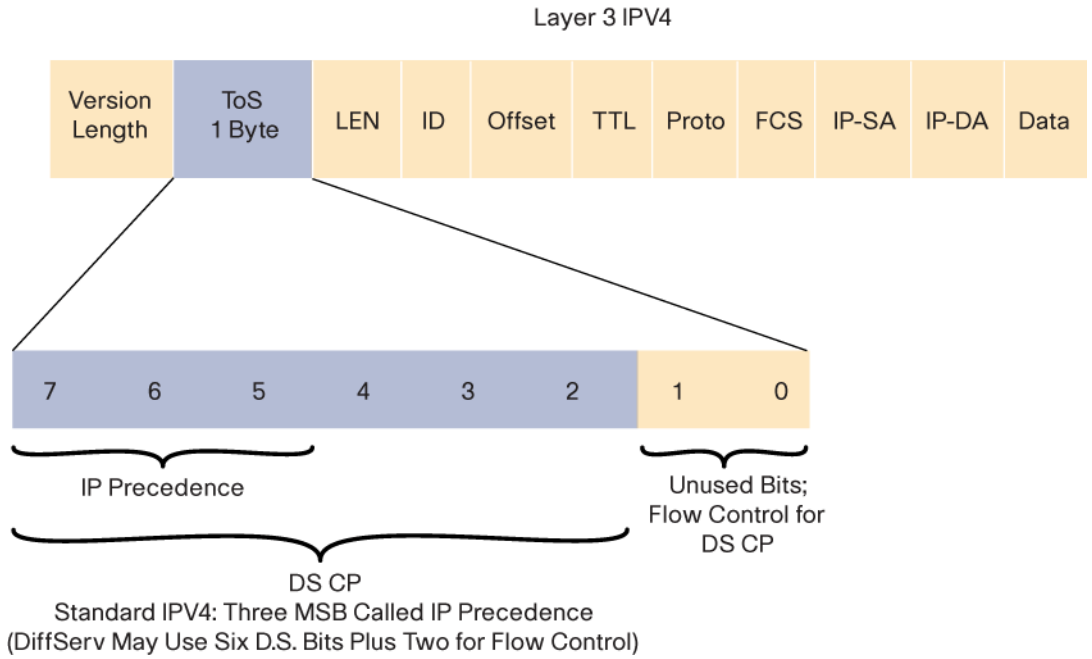


Table 1. Packet Priority Classifications

Layer 2 Class of Service	IP Precedence	DSCP
CoS 0	Routine (IP precedence 0)	0-7
CoS 1	Priority (IP precedence 1)	8-15
CoS 2	Immediate (IP precedence 2)	16-23
CoS 3	Flash (IP precedence 3)	24-31
CoS 4	Flash-override (IP precedence 4)	32-39
CoS 5	Critical (IP precedence 5)	40-47 (EF)
CoS 6	Internet (IP precedence 6)	48-55
CoS 7	Network (IP precedence 7)	56-63

QUEUING

Queuing tools assign a packet or flow to one of several queues, based on classification, for appropriate treatment in the network. When data, voice, and video are placed in the same queue, packet loss and variable delay are more likely to occur. Users can increase the predictability of network behavior and voice quality by using multiple queues on egress interfaces and placing voice packets into a strict priority queue (LLQ) with guaranteed bandwidth, separate from data packets. Congested outbound WAN egress queues and serialization delays with low-speed WAN links (link speeds less than 768 kbps) can result in variable delays and jitter impact on voice traffic (serialization delay is a function of both link speed and packet size). Large emails and data downloads can cause voice quality degradation, even in LAN environments.

A data frame can be sent to the physical wire only at the serialization rate of the interface. The serialization rate is the size of the frame, divided by the clocking speed of the interface. For example, a 1500-byte frame takes 214 ms to serialize on a 56-kbps circuit. If a delay-sensitive voice packet becomes stuck behind a large data packet at the egress WAN interface queue, the end-to-end delay requirements for VoIP quality (150-200 ms) could be exceeded (jitter). Even relatively small frames can adversely affect overall voice quality by simply increasing the jitter to a value greater than the size of the adaptive jitter buffer at the receiver. Cisco IOS Software link efficiency mechanisms (LFI) can fragment the large data frames into regularly sized pieces and interleave voice frames into the flow and the end-to-end delay can be predicted and managed. Cisco AutoQoS VoIP automatically handles the requirements for LFI for various frame sizes and link speeds.

NETWORK PROVISIONING

Network provisioning tools accurately calculate the amount of bandwidth required for voice conversations, data traffic, video applications, and necessary link management overhead, such as routing protocols. When calculating the required amount of bandwidth for running voice over a WAN, it is important to remember that all combined application traffic (voice, video, and data traffic), should equal no more than seventy-five percent of the provisioned bandwidth. The reserved bandwidth is used for overhead, routing protocols, Layer 2 link information, and other miscellaneous traffic.

See the *Consideration, Caveats, and Restriction for AutoQoS VoIP* section of this document for additional information.

CISCO AUTOQOS VOIP REQUIREMENTS AND DESIGN CONSIDERATIONS

The following are the *minimum* required steps to enable Cisco AutoQoS for VoIP traffic for WAN interfaces:

1. Configure an IP address on a low-speed (768 kbps or lower) interface or a sub-interface.
2. Configure “bandwidth” under any participating interfaces or sub-interfaces. For ATM PVC, configure “vbr-nrt” under the PVC.

Note: Asterisks (*) denote the resulting configuration commands (CLI) generated as a result of configuring Cisco AutoQoS.

For low-speed interfaces or PVCs the configured IP address will be moved to the virtual template/multilink interface automatically by Cisco AutoQoS.

Using Cisco AutoQoS, VoIP traffic is automatically provided with the required QoS template for voice traffic by configuring **autoqos 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).

The type and bandwidth of the interface is considered when deciding the appropriate techniques required for the template. The classification is used to differentiate the voice packets from the data packets and handle them appropriately. The LLQ-PQ is applied to the voice packets to meet the latency requirements. LFI reduces the jitter of voice packets by preventing them from becoming stuck behind large, 1,500 byte (Ethernet MTU) data packets. Using cRTP the 40-byte IP header of the voice packet is reduced to 2-4 bytes, thereby reducing voice bandwidth requirements. Please note, for low-speed links (links less than 768 kbps), the AutoQoS command must be applied on both sides of the link.

For Cisco AutoQoS, global templates for policy-map, class-maps, and access-lists are created to classify VoIP packets, and to provide LLQ. Interface templates are created depending on the type of interface and bandwidth configured on the interface.

Cisco AutoQoS VoIP cannot be configured if a pre-existing QoS service policy is already attached to an interface or PVC (see the *Considerations, Caveats, and Restrictions for AutoQoS VoIP* section of this document for more information).

CISCO AUTOQOS VOIP CONFIGURATION (CISCO IOS SOFTWARE)

Cisco AutoQoS automatically provides VoIP traffic with all required QoS features for voice by configuring auto qos voip on the interface or PVC. The appropriate QoS features and optimal QoS values that pertain to each feature are automatically configured (template) to meet voice requirements. Cisco AutoQoS Enterprise available in Cisco IOS Software Release 12.3(7)T can define up to 10 AutoQoS classes.

The following is the configuration syntax for Cisco AutoQoS VoIP on WAN interfaces:

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

The **auto qos voip** interface configuration command enables Cisco AutoQoS VoIP on an interface or PVC (VoIP refers to all voice traffic with RTP carried over IP protocol that requires low delay, jitter, and packet loss). Cisco AutoQoS VoIP relies on interface bandwidth, not clockrate, to determine whether additional QoS features that pertain to low or high speed interfaces or PVCs should be configured or not configured.

The following is the minimum set of QoS features required for VoIP and are accommodated by the Cisco AutoQoS VoIP template:

1. Classify the IP traffic with RTP and audio codec payload type (RFC 1890) as VoIP bearer traffic.
2. Mark VoIP bearer traffic with DSCP EF and VoIP signaling (control) traffic as AF31.
3. Map the Layer 3 marking to the corresponding Layer 2 marking, if applicable.
4. Remark traffic that is marked DSCP EF or AF31 to DSCP 0, if the traffic is not classified as VoIP bearer or signaling (control) traffic.
5. Treat all other non-VoIP traffic types as best effort QoS (excluding control traffic such as routing protocol updates and BPDUs).
6. Put VoIP bearer traffic into a strict priority LLQ with guaranteed bandwidth to accommodate voice traffic.
7. Put VoIP control traffic into a non-priority queue with a minimum bandwidth guarantee to ensure no packet loss.
8. Enable LFI and cRTP for link speeds of less than 768 kbps.

The **trust** optional keyword allows Cisco AutoQoS to trust the DSCP marking of the traffic and use it to classify that particular type of traffic (Cisco AutoQoS default is **non-trust**). If the **trust** keyword is not configured, voice traffic is classified and marked with the appropriate DSCP values using NBAR.

The **fr-atm** optional keyword is only used on FR DLCIs used for FR to ATM internetworking (**auto qos voip fr-atm** must be configured to enable Cisco AutoQoS for FR-to-ATM internetworking links). This is only for low-speed DLCIs, where multi-link PPP over FR (MLPoFR) is created to enable LFI (**NOTE**: **fr-atm** keyword is ignored when configured on high-speed links even if the keyword is configured).

The **no auto qos voip** interface configuration command removes the AutoQoS from the interface (ie: removes the previously created QoS configuration template generated as a result of configuring **auto qos voip**). There is no need to configure the **trust** or **fr-atm** keywords (if used) to remove an AutoQoS configuration when using the **no auto qos voip** configuration command.

While configuring a template for the interface, the user will be notified of any errors (for example, QoS was manually configured on the interface previously). No Cisco AutoQoS configuration will take place if this occurs.

AUTOQOS VOIP CONFIGURATION FOR CISCO CATALYST SWITCHES

There are various LAN commands, depending on the platform and operating system (Cisco IOS Software vs. Cisco Catalyst OS Software). For the Cisco IOS Software based Catalyst 2950 and Catalyst 3550 Series Switches, there are two AutoQoS configuration commands. One command is for the IP phone connections and the other is for trusted connections to other network devices:

```
auto qos voip cisco-phone
auto qos voip trust
```

These commands should not be used if there are previous QoS configurations on the switch. However, the Cisco AutoQoS configuration parameters (Cisco AutoQoS template) generated may be tuned after using the above commands.

There are several AutoQoS commands for the Cisco Catalyst 6500 Series Switch. The following configuration command enables global Cisco AutoQoS settings:

```
set qos autoqos
```

Additionally, one of the following interface commands must be used:

```
set port qos <mod/ports..> autoqos voip ciscoipphone
set port qos <mod/ports..> autoqos voip ciscosoftphone
set port qos <mod/ports..> autoqos trust cos
set port qos <mod/ports..> autoqos trust dscp
```

DISABLING AND REMOVING AUTOQOS VOIP

The **no auto qos voip** global configuration command removes Cisco AutoQoS VoIP from the device. Deleting a sub-interface or PVC without configuring **no auto qos voip** does not remove Cisco AutoQoS VoIP properly (refer to the *Considerations, Caveats, and Restrictions for AutoQoS VoIP* section of this document for additional information).

Cisco AutoQoS for VoIP Configuration Example (Cisco IOS Software)

In this example, Cisco AutoQoS VoIP is configured on the Serial interface 4/0, and both the **trust** and **fr-dlci** keywords are configured:

```
Router> enable
Router# configure terminal
Router(config-if)#interface s4/0
Router(config-if)#auto qos voip trust fr-dlci
Router(config-pmap-c)# exit
```

MONITORING AND VERIFYING AUTOQOS VOIP OUTPUT

When AutoQoS is configured, an asterisk (*) denotes the resulting QoS configuration CLI. This distinguishes the Cisco AutoQoS configuration from any pre-existing user configuration CLI. To display the AutoQoS configuration, issue the following Cisco IOS Software show command:

```
show auto qos interface <<interface name>>
```

Example:

AutoQoS is enabled on a low-speed FR-DLCI with the **autoqos voip fr-atm** configuration command. Issuing the **show autoqos interface s4/1.2** as shown in the example below would display the created template(s) for all the AutoQoS created interfaces:

```
AutoQoS-72#show autoqos interface s4/1.2
Serial4/1.2: DLCI 102 -
!
interface Serial4/1.2 point-to-point
bandwidth 100
no ip mroute-cache
frame-relay interface-dlci 102 ppp Virtual-Template200 *
class AutoQoS-VoIP-FR-Serial4/1-102 *
!
interface Virtual-Template200 *
bandwidth 100 *
description “AutoQoS created”
ip address 111.111.2.2 255.255.255.0 *
service-policy output AutoQoS-Policy *
ppp multilink *
ppp multilink fragment-delay 10 *
ppp multilink interleave *
!
map-class frame-relay AutoQoS-VoIP-FR-Serial4/1-102 *
frame-relay cir 100000 *
frame-relay bc 1000 *
frame-relay be 0 *
frame-relay mincir 100000 *
no frame-relay adaptive-shaping *
```

MONITORING PACKET DROPS IN LLQ TRAFFIC USING AUTOQOS

Thresholds are activated in the Remote Monitoring (RMON) alarm table to monitor drops in LLQ. The following template is used:

```
rmon event AUTOQOS_SNMP_EVENT_ID log trap AUTOQOS_SNMP_COMMUNITY_STRING
description “AutoQoS SNMP traps for Voice” owner AUTOQOS_SNMP_OWNER
rmon alarm AUTOQOS_SNMP_ALARM_ID cbQosCMDropRate.pqid.cqid
AUTOQOS_SNMP_SAMPLE_INTERVAL absolute rising-threshold
AUTOQOS_SNMP_RISING_THRESHOLD falling-threshold
AUTOQOS_SNMP_FALLING_THRESHOLD AUTOQOS_SNMP_EVENT_ID owner
AUTOQOS_SNMP_OWNER
```

Note: The following values/names are used:

```
AUTOQOS_SNMP_EVENT_ID 33333
AUTOQOS_SNMP_COMMUNITY_STRING AutoQoS
AUTOQOS_SNMP_OWNER AutoQoS
AUTOQOS_SNMP_ALARM_ID 33333 onwards
AUTOQOS_SNMP_SAMPLE_INTERVAL 30 seconds
AUTOQOS_SNMP_RISING_THRESHOLD 1 bps
AUTOQOS_SNMP_FALLING_THRESHOLD 0
```

Note: The pqid and cqid values are derived from the instance of the policy map attached to the interface or PVC.

CONSIDERATIONS, CAVEATS, AND RESTRICTIONS FOR AUTOQOS VOIP

1. The Cisco AutoQoS VoIP feature is supported only on the following interfaces and PVCs

- Serial interfaces with PPP or High-Level Data Link Control (HDLC)
- FR DLCIs (point-to-point sub-interfaces only)
  - Cisco AutoQoS does not support FR multipoint interfaces
- ATM PVCs

2. Cisco AutoQoS VoIP is supported on low-speed ATM PVCs, on point-to-point sub-interfaces only (link bandwidth less than 768 kbps).

3. Cisco AutoQoS VoIP is fully supported on high-speed ATM PVCs (link bandwidth greater than 768 kbps).

4. The **auto qos voip** configuration command is only supported on the interfaces/PVCs that support **service-policy** configuration.

5. The **auto qos voip** command is available for FR DLCIs, the command cannot be configured as part of a class-map.

6. The auto qos voip CLI is not supported on router sub-interfaces.

7. Cisco AutoQoS VoIP automatically creates either **AutoQoS-Policy-Trus**t or **AutoQoS-Policy-UnTrust** to handle VoIP traffic on an interface or PVC; the user can tune the configurations within the AutoQoS-created policy map if desired. Users are advised not to attach this policy map by **service-policy** command manually to an interface or PVC, as the above created policy map and its associated class maps and access lists will not be cleaned up if the **no auto qos voip** command is configured (to remove AutoQoS) (when **no auto qos voip** is issued on the interface/PVC and if the user does not attach the corresponding policy map to any other interfaces/PVC manually, all policy maps generated by Cisco AutoQoS and associated class maps and access lists will be removed completely).

8. The configuration template (CLI) generated by configuring Cisco AutoQoS on an interface or PVC can be tuned manually (via CLI configuration) if desired.

9. Cisco AutoQoS cannot be configured if a QoS service-policy is already configured and attached to the interface or PVC.

10. Multi-link PPP (MLP) is configured automatically for a serial interface with a 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.

11. Cisco AutoQoS VoIP cannot be configured on a FR-DLCI if a map-class is already attached to the DLCI.

12. Cisco AutoQoS VoIP is supported only with FR-DLCIs in point-to-point sub-interfaces.

13. If a FR-DLCI is already assigned to one sub-interface, Cisco AutoQoS VoIP cannot be configured from a different sub-interface.

14. For low-speed FR–DLCIs interconnected with ATM-PVCs, the user should explicitly issue "**auto qos voip fr-atm**" for proper operation.

15. Multi-link PPP over Frame Relay (MLPoFR) is configured automatically, for low-speed FR-DLCIs with FR-ATM internetworking. The sub-interface must have an IP address (the IP address is removed and put on the MLP bundle). Cisco AutoQoS VoIP must also be configured on the ATM side of the network connection.

16. Cisco AutoQoS VoIP cannot be configured for low-speed FR-DLCIs with FR-to-ATM internetworking if a virtual template is already configured for the DLCI.

17. Cisco AutoQoS VoIP is only supported on low-speed (links under 768 kbps) ATM PVCs on point-to-point sub-interfaces (Cisco AutoQoS VoIP is fully supported on high-speed ATM PVCs).

18. The **no auto qos voip** command removes Cisco AutoQoS. 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.

19. Cisco AutoQoS SNMP traps are only delivered when an SNMP server is used in conjunction with Cisco AutoQoS.

20. The SNMP community string "AutoQoS" should have "write" permissions.

21. 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 warning messages can be ignored (to avoid further warning messages, save the configuration to NVRAM again without making any changes to the QoS configuration).

22. On the Cisco 7200 Series Routers and below that support MQC QoS, the default class can use twenty-five percent of the available interface bandwidth. However, the entire twenty-five percent is not guaranteed to the default class. This twenty-five percent 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.

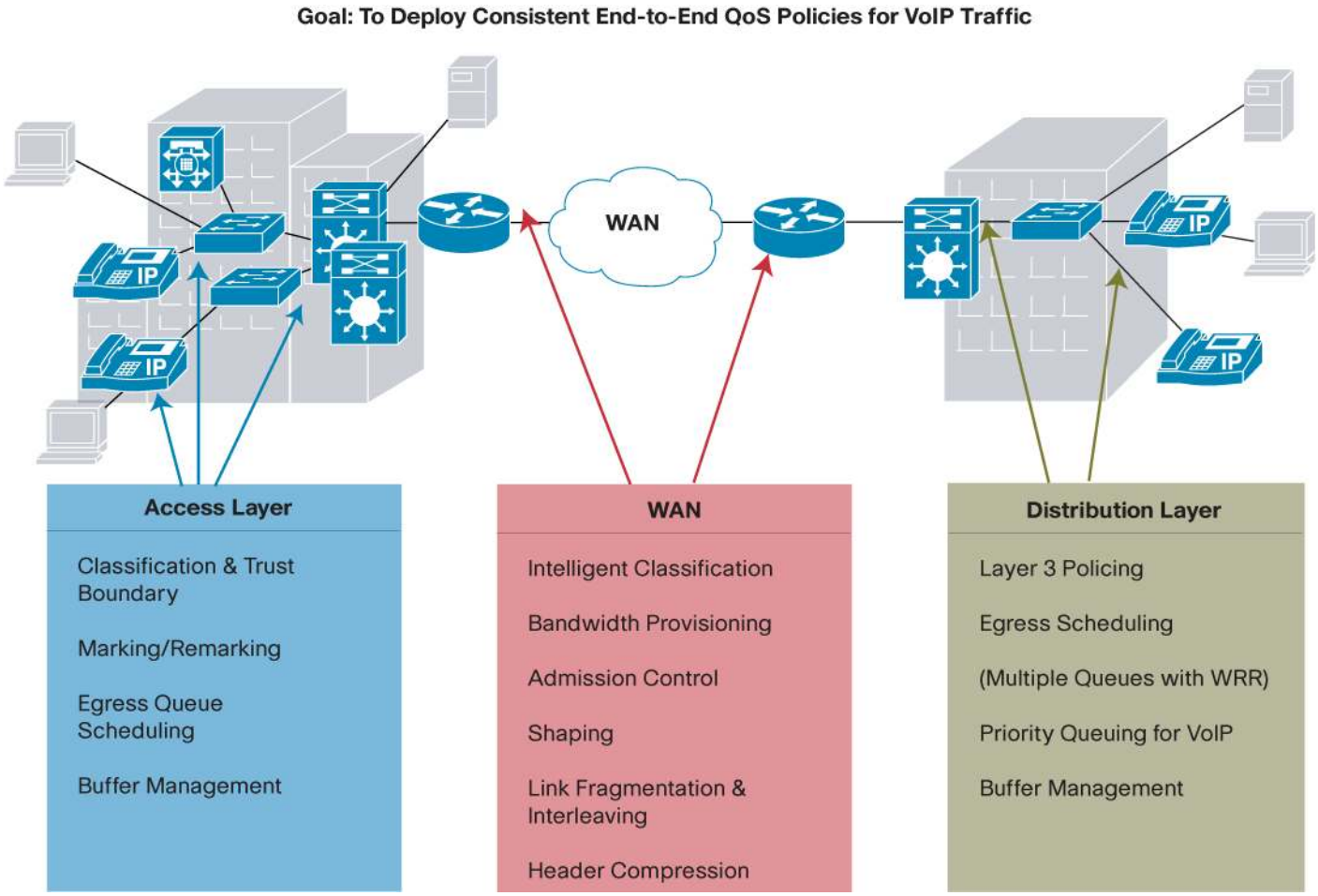
AUTOQOS VOIP DEPLOYMENT CASE STUDY

What are the characteristics of a robust end-to-end QoS solution for VoIP traffic?

- **End-to-End Policy Enforcement**: QoS must be applied end-to-end. Consequently, it must be platform, device, and media independent, while operating at Layer 3 and above to ensure end-to-end functionality across different network devices (ie: routers, switches, firewalls, access servers, gateways) and link layers (ie: ATM, FR, Ethernet).
- **Multiple Parameters**: Policies must be based on how the network is used. Devices must have the flexibility to apply and enforce QoS based on parameters that can closely reflect the policy parameters that network managers define, in order to distinguish traffic flows based on IP or MAC address, application type, time of day, or location within the network (or a combination of these parameters).

- **Centralized Control**: Network-based policy enforcement often results in consistent policy deployment and enforcement.
- **Sophisticated QoS Tools**: There are many different network elements and parameters required to successfully deploy and implement a QoS policy end-to-end, an associated set of advanced function QoS tools, including Cisco AutoQoS, QoS Policy Manager, and Cisco Class-Based QoS MIB must be fully featured to enable network managers to build the intelligent network they need.

Figure 4. QoS Deployment for VoIP Case Study Example



QOS REQUIREMENTS IN THE LAN

1. Identify trust boundary and extended trust boundary
2. Remark traffic based on classification
3. Determine CoS to DSCP and IP precedence to DSCP mappings
4. Map CoS values to the different egress queues
5. Queue size settings and Weighted Round Robin (WRR) weights (ie: appropriated WRR settings for FE ports vs. GE ports)
6. Determine CoS to egress queue mapping
7. Configure QoS on a per port basis

QOS REQUIREMENTS IN THE WAN

1. Identify applications and protocols of interest (un-trusted versus trusted edge)
2. Remark traffic based upon MQC QoS classification
3. Determine the number of classes
4. Determine the queuing methods that should be enabled
5. Individual class bandwidth requirements for QoS to meet voice needs and minimum bandwidth guarantees for other applications
6. Transport specific QoS features

- Traffic shaping
- MLPPP
- TX-ring settings

7. Low-bandwidth (< 768 kbps) specific QoS features

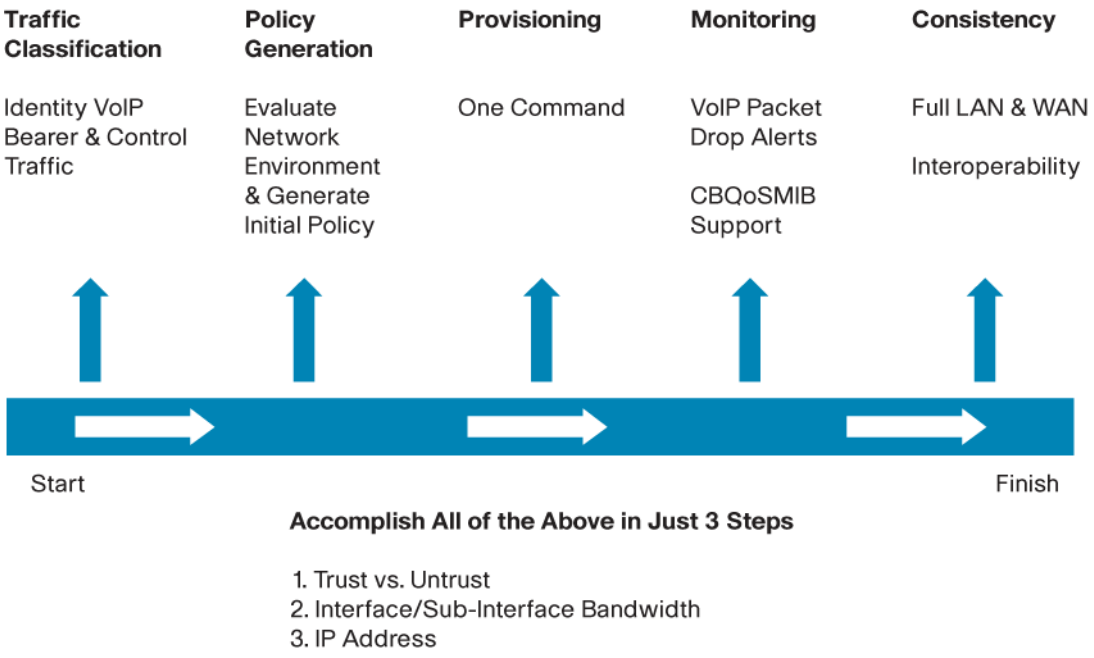
- RTP header compression
- Fragmentation settings (MLP/LFI or FRF.12)

8. Alarm and event settings for monitoring purposes

QOS DEPLOYMENT FOR VOIP TRAFFIC USING CISCO AUTOQOS

Deploying optimal end-to-end QoS for VoIP traffic can be easily accomplished with Cisco AutoQoS as illustrated in Figure 5.

Figure 5. QoS Deployment for VoIP using Cisco AutoQoS



QOS REQUIREMENTS ADDRESSED BY CISCO AUTOQOS IN THE LAN

- Single command enables Cisco AutoQoS for VoIP in LAN (provides support for Cisco IP phone and Cisco softphone)
- Auto-configures QoS parameters and optimal voice performance based upon Cisco best practice recommendations, extensive lab testing, and input from a broad base of AVVID customer installations
- Determines trust and extended trust boundary settings automatically
  - User can bypass telephone and connect PC directly to switch, but trust is disabled when IP phone is removed
- Configures CoS to DSCP to queue mapping
- Determines optimal PQ and WRR configuration settings for static, dynamic-access, voice VLAN and trunk ports

QOS REQUIREMENTS ADDRESSED BY CISCO AUTOQOS IN THE WAN

- Simplifies QoS configuration for VoIP (single configuration command enables Cisco QoS for VoIP)
- End-to-end simplification, automation and intelligence classification, provisioning, policy generation and monitoring
- Classifies VoIP bearer and signaling (H.323, Skinny, SIP and MGCP) traffic
- Provisioning based on Cisco best practices recommendations
- Intelligent policy generation
  - Based on available bandwidth and underlying L2 technology
  - Enables IP RTP header compression, if required
  - Enables FRTS, if required
  - Decides on fragmentation settings (FRF.12, MLP/LFI), if required
  - Supported on FR, ATM, HDLC, PPP and FR-to-ATM links
- Provides RMON alerts if VoIP packets are dropped

NETWORK MANAGEMENT

While Cisco AutoQoS provides QoS provisioning for individual routers and switches, CiscoWorks QoS Policy Manager (QPM) can be used for centralized QoS design, administration, and traffic monitoring that scales to large QoS deployments for voice, video and data.

Leveraging the Cisco intelligent IP network, the QPM management tool contains a step-by-step wizard that guides administrators through the process of configuring QoS for voice in the network, QoS monitoring for voice traffic, and reports including network voice-readiness (devices that have all the required software and hardware to support QoS for voice) and deployment audit. The IP telephony wizard can identify potential network points (device interfaces) where QoS needs to be configured, and select and assign the appropriate QoS policies for each interface on the voice path. QoS policies and properties for voice, included with QPM in a template library, are defined according to the Cisco IP telephony design recommendations. A user can easily modify these predefined templates or reassign default policy assignments as needed to fit the IP network of the organization.

QPM supports the class-based QoS MIB to provide visibility into network operations. Users can measure traffic throughput for top applications and service classes; they can also troubleshoot problems with real-time and historical QoS feedback. Traffic and QoS statistics can be displayed as line or bar charts in bits or packets per second, per interface or policy. QPM enables a user to view graphs before and after QoS deployment, tied to traffic filters and policies, as well as results from QoS policy actions.

QPM enables users to view:

- Statistics matching policies and specific filters, includes Cisco IOS NBAR application filters
- Traffic rate before any QoS policy actions, traffic transmitted after QoS policy actions, and traffic dropped (not transmitted) because of QoS policy drop actions
- QoS action statistics: WRED, policing, traffic shaping, queuing

REFERENCES

QoS Home Page

http://www.cisco.com/go/qos

AutoQoS–VoIP

http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a0080455a3d.html

AutoQoS–Enterprise

http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a0080455a3f.html

---

Ci

ht

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.