AutoQoS for Medianet Campus Networks

The QoS Challenge for Medianet Campus Networks

Today there is a virtual explosion of media applications on the IP network with many different types of voice, video, and data applications. For example, voice streams can be standard IP Telephony, high-definition audio, Internet VoIP, or others. Similarly, there are many flavors of video, including on-demand or broadcast desktop video, low-definition interactive video (such as webcams), high-definition interactive video (such as Cisco TelePresence), IP video surveillance, digital signage, and entertainment-oriented video applications. In turn, there are a virtually limitless number of data applications. Managing service levels for these applications is an evolving challenge for administrators.

To meet this challenge, Cisco advocates following relevant industry standards and guidelines whenever possible, as this extends the effectiveness of deployed QoS policies beyond the enterprise edge. A summary of Cisco's RFC 4594-based recommendations for marking and provisioning medianet application classes is presented in Figure 1.

Figure 1 Cisco Differentiated Services (DiffServ) QoS Recommendations for Medianet

Application Class	Per-Hop Behavior	Admission Control	Queuing and Dropping
VoIP Telephony	EF	Required	Priority Queue (PQ)
Broadcast Video	CS5	Required	(Optional) PQ
Real-Time Interactive	CS4	Required	(Optional) PQ
Multimedia Conferencing	AF4	Required	BW Queue + DSCP WRED
Multimedia Streaming	AF3	Recommended	BW Queue + DSCP WRED
Network Control	CS6		BW Queue
Signaling	CS3		BW Queue
Ops/Admin/Mgmt (OAM)	CS2		BW Queue
Transactional Data	AF2		BW Queue + DSCP WRED
Bulk Data	AF1		BW Queue + DSCP WRED
Best Effort	DF		Default Queue + RED
Scavenger	CS1		Min BW Queue

229928

Nonetheless, provisioning (up to) 12 application classes across campus networks can be a daunting challenge for many administrators, especially when considering that many campus QoS features are hardware-specific.

To this end, Cisco has updated and expanded the functionality of its AutoQoS feature to automatically provision QoS best-practice designs for not only voice, but also for IP-based video applications (such as IP Video Surveillance, Cisco TelePresence, conferencing applications, and streaming video applications), as well as multiple types of data applications. An administrator can automatically provision these best-practice designs via a single interface-level command that corresponds to the endpoint-type that the interface is connecting to, such as:

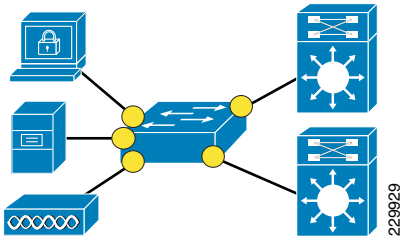
- **auto qos trust {cos | dscp}**—This option configures the port to statically trust either CoS or DSCP. If neither CoS nor DSCP are explicitly specified, then the **auto qos trust** command will configure CoS-trust on Layer 2 switch ports and DSCP-trust on Layer 3 routed interfaces.
- **auto qos video [cts | ip-camera]**—This option provides automatic configuration support for both Cisco TelePresence Systems (via the **cts** keyword) as well as Cisco IP Video Surveillance cameras (via the **ip-camera** keyword).
- **auto qos classify {police}**—This option provides a generic template that can classify and mark up to six classes of medianet traffic, as well as optionally provision data-plane policing/scavenger-class QoS policy-elements for these traffic classes (via the optional **police** keyword).
- **auto qos voip [cisco-phone | cisco-softphone | trust]**—This option provides not only legacy support for Auto QoS VoIP IP Telephony deployments, but also expands on these models to include provisioning for additional classes of rich media applications and to include data-plane policing/scavenger-class QoS policy-elements to protect and secure these applications.

Each of these AutoQoS options—expanded on in the following sections—is automatically complemented by a complete set of ingress and egress queuing configurations.

Auto QoS Trust

This option is well-suited to support endpoints that can mark QoS values (at Layer 2 CoS or Layer 3 DSCP). However, it is recommended that such devices be centrally—and/or securely—administered in order for these markings to be accepted by the network as conforming to policy. Trusted endpoonts can include secure PCs and servers, wireless access points, gateways, and other similar devices. Additionally all interswitch-links, such as access-to-distribution uplinks and downlinks, are recommended to be configured with **auto qos trust dscp**. Switch port interfaces recommended to be configured with **auto qos trust** are illustrated in Figure 2.

Figure 2 Switch Port Interfaces Recommended to be Configured with AutoQoS Trust



Auto QoS Video

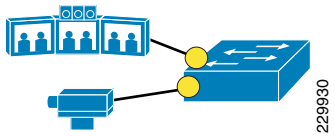
Besides supporting IP Telephony devices, Auto QoS now also supports video devices, such as Cisco TelePresence Systems (CTS) and IP Video-Surveillance cameras, both of which support dynamically-extended conditional trust via Cisco Discovery Protocol (CDP).

Cisco TelePresence Systems mark their video and audio flows at both Layer 2 and Layer 3, to CoS 4 and DSCP CS4, respectively. Furthermore, CTS signaling traffic is marked CoS 3 and DSCP CS3, respectively. The administrator can configure dynamic trust to be extended to CTS devices by using the **auto qos vdeo cts** interface command.

On the other hand, IP Video Surveillance Cameras are only required to mark their video (and if supported, audio) flows at Layer 3, to DSCP CS5. This allows for more flexible deployment models, as these cameras do not therefore have to be deployed in dedicated VLANs connecting to

the access switch via an 802.1Q trunk. As such, the **auto qos video ip-camera** interface command dynamically extends DSCP-trust to these devices once these have successfully identified themselves to the switch via CDP. Switch port interfaces recommended to be configured with **auto qos video** are illustrated in Figure 3.

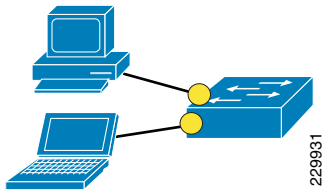
Figure 3 Switch Port Interfaces Recommended to be Configured with AutoQoS Video



Auto QoS Classify

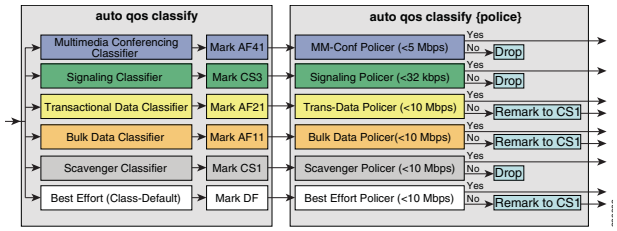
The AutoQoS Classify models provide a generic template to support additional rich media and data applications, providing a classification (and optional policing) model for these. These models are most suitable for switch ports connecting to PC endpoint devices, as shown in Figure 4.

Figure 4 Switch Port Interfaces Recommended to be Configured with AutoQoS Classify



Six application classes (Multimedia-Conferencing, Signaling, Transactional Data, Bulk-Data, Scavenger, and Best-Effort) are automatically defined via class-maps. Each class-map references an assosciated extended IP access-list. These IP access lists define the TCP and UDP port numbers of sample classes of applications. However, it should be noted that these are generic application examples and the administrator can add/change/delete the access-list entries to match on their specific applications. The logic of the AutoQoS Classify models are shown in Figure 5.

Figure 5 AutoQoS Classify Logic Models



Auto QoS VoIP

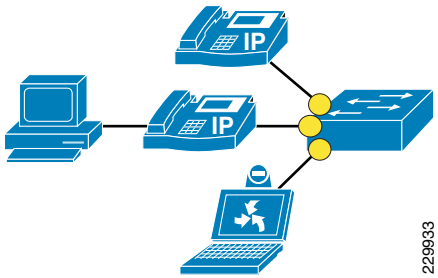
The AutoQoS VoIP models provide not only legacy support for Auto QoS VoIP IP Telephony deployments, but also expand on these models to include provisioning for additional classes of rich media applications and to include data-plane policing/scavenger-class QoS policy-elements to protect and secure these applications.

Three options are available under AutoQoS VoIP:

- **trust**—Functionally equivalent to **auto qos trust**
- **cisco-phone**—Deploys best practice QoS designs to Cisco IP Phones
- **cisco-softphone**—Deploys best-practice QoS designs to PC-based softphones

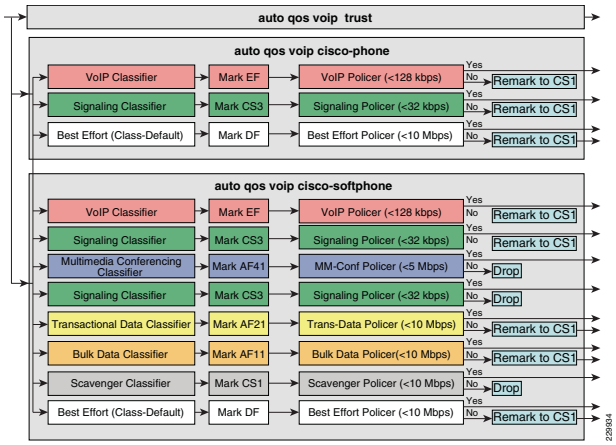
Switch port interfaces recommended to be configured with **auto qos voip** are illustrated in Figure 6.

Figure 6 Switch Port Interfaces Recommended to be Configured with AutoQoS VoIP



AutoQoS VoIP **cisco-phone** and **cisco-softphone** models also include policers to prevent network abuse from devices masquerading as IP telephony devices. The logic of the AutoQoS VoIP models are shown in Figure 7.

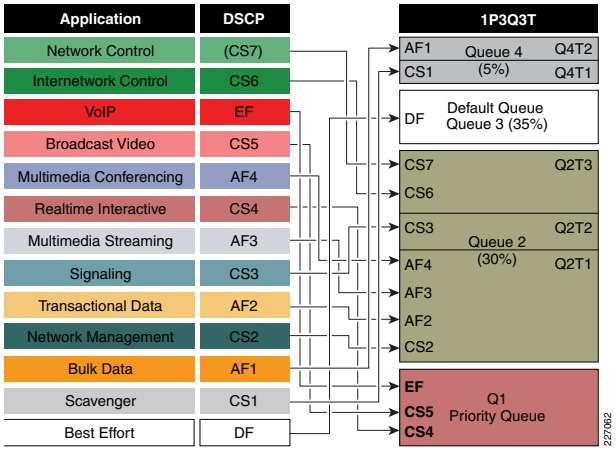
Figure 7 AutoQoS VoIP Logic Models



AutoQoS Queuing Models

Each AutoQoS option automatically provisions both ingress and egress queuing models on every switch port that it is applied on. Figure 8 shows the 1P3Q3T egress queuing model automatically configured by AutoQoS.

Figure 8 AutoQoS 1P3Q3T Egress Queuing Model



Summary

AutoQoS can significantly expedite the deployment of the complex QoS models required to support rich media applications across medianet campus networks.

For more details, see Medianet Campus QoS Design 4.0: http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSCampus_40.html.