Cisco APIC-EM QoS

The Roles of APIC-EM QoS

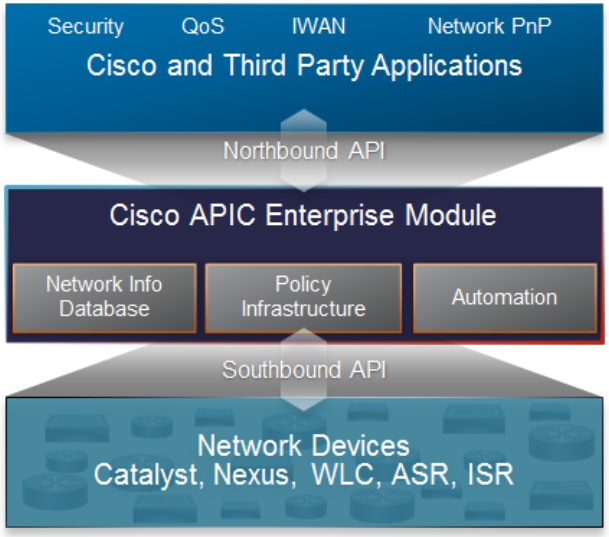
QoS is one of the most widely-deployed technologies in the enterprise and needs to be deployed in a holistic, integrated, end-to-end manner to ensure maximum effectiveness. As such, it is a prime candidate technology to showcase the value-add of Software Defined Networking (SDN), which allows for:

- Integrating applications with the network infrastructure
- Capturing business intent of QoS policies so as to articulate an end-to-end QoS strategy
- Abstracting platform-specific implementation details, while maintaining cross-platform consistency
- Dynamic QoS policies based on application requirements and events

Integrating Applications with the Network

A key objective of SDN is to allow for communication between applications and the network. This is done by supporting (Northbound) Application Programming Interfaces (APIs) between software applications and the network controller, such as Cisco's Application Policy Infrastructure Controller-Enterprise Module (APIC-EM). In this manner, the network can adapt policies to application's requirements, as well as provide feedback so that applications can also make intelligent decisions based on dynamic network conditions.

Figure 1 Cisco APIC-EM Architecture



Capturing Business Intent and Articulating QoS Strategy

Without a centralized controller, application policies (such as QoS) have to be independently configured on individual network devices and it would be up to the administrator to ensure compatibility and cohesiveness across the network.

However, a controller-based approach allows for administrators to centrally define QoS policies, by expressing the business-relevance of applications. With this information, the controller can then articulate a end-to-end strategy that is to be deployed across ***all*** network devices in a consistent manner.

Abstracting Platform-Specific Implementation Details

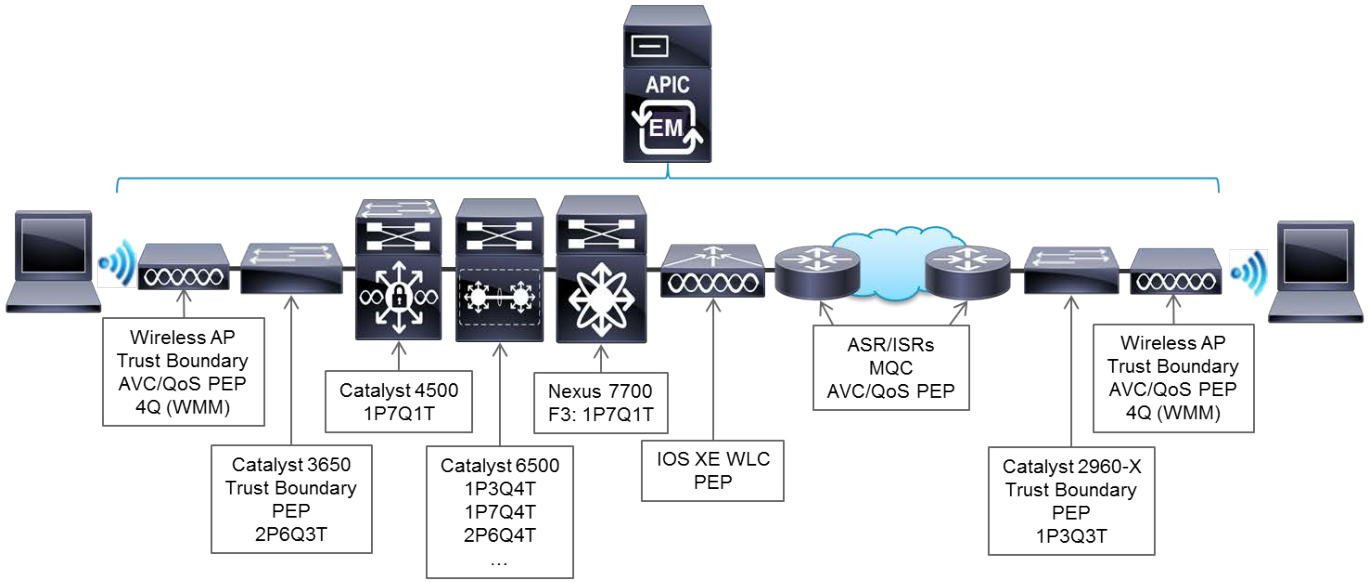
With a central QoS strategy defined, the controller can then apply Cisco Validated Design (CVD) best-practices to translate the policy to device-specific configurations, which it then pushes down to all network devices via (Southbound) APIs, as shown in Figure 2.

In this manner, device-specific details are completely abstracted from the network operator, who can thus focus on business objectives and results.

Three key design principles are followed when translating the strategic (business-intent) QoS policy into tactical (device-specific) configurations:

- The first is that the primary goal of the tactical QoS policy is to express the strategic QoS policy with ***maximum fidelity,*** subject to any platform-specific technical constraints
- The second is that QoS features will not be enabled simply because these exist, but rather only features that ***directly contribute*** to the strategic policy will be enabled
- The third is that all features that are enabled are done in accordance with ***CVD best-practices***.

Figure 2 APIC-EM Adaption of Business Intent QoS Policies to Platform-Specific Capabilities and Constraints



Dynamic Application-Based QoS Policies

A unique advantage that a controller-based architecture brings to the network is the ability to deploy dynamic QoS policies in a scalable and virtually instantaneous manner.

For example, APIC-EM can integrate via APIs to collaborative multimedia applications, including Cisco Jabber and Microsoft Lync (now Skype for Business). By means of this integration, QoS policies can be dynamically applied throughout the network to prioritize voice and video flows.

Such dynamic QoS policies allow for these applications to have their flows protected with QoS, regardless of whether:

- the endpoint devices are wired or wireless
- the endpoint devices are IT-managed or BYOD
- the media flows are encrypted or not

There are 5 main steps to these dynamic QoS policies:

Step 1: A network operator enters business-intent into APIC-EM, which then articulates a strategic end-to-end QoS policy, as shown in Figure 3.

Step 2: APIC-EM translates the strategic policy into device-specific tactical policies, including classification, marking and queuing policies.

Note: classification policies for ***voice and video*** - which are are access-list (ACL) based - do not (initially) include any access-list entries (ACEs) to discretely identify the IP flows to which these should apply.

Note: Queuing policies (not shown in Figure 3, but expressed in Figure 1) are all DSCP-based.

Step 3: APIC-EM is informed (by either Cisco Unified Call Manager or the Microsoft Lync server) of a proceeding call. This includes the 5-tuple information (IP Source / Destination Addresses and UDP Source / Destination Ports) of the voice and video flows, as shown in Figure 4.

Step 4: APIC-EM dynamically pushes out ACEs to the edge switches hosting the endpoints.

Step 5: APIC-EM is informed of a terminated call.

Step 6: APIC-EM removes the ACEs corresponding to the terminated call. (Steps 5 & 6 are not shown).

Figure 3 APIC-EM Dynamic QoS Policies - Steps 1 (Operator Expresses Business Intent) and 2 (Tactical QoS Policies Deployed)

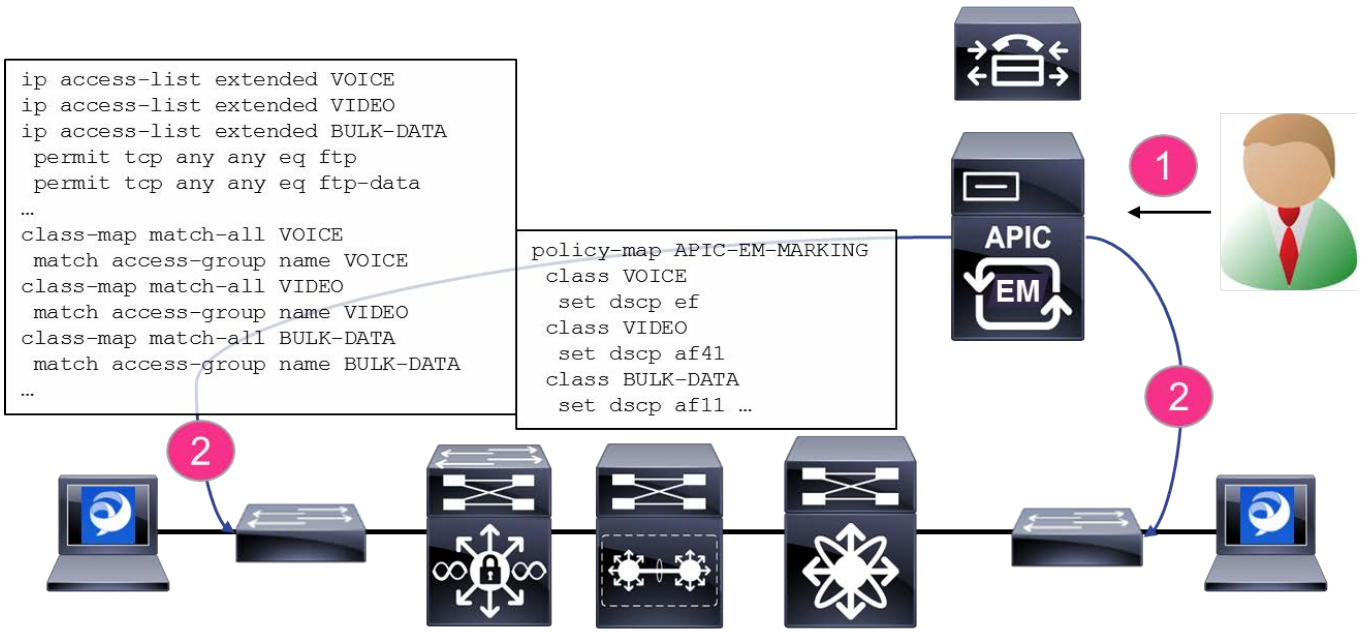
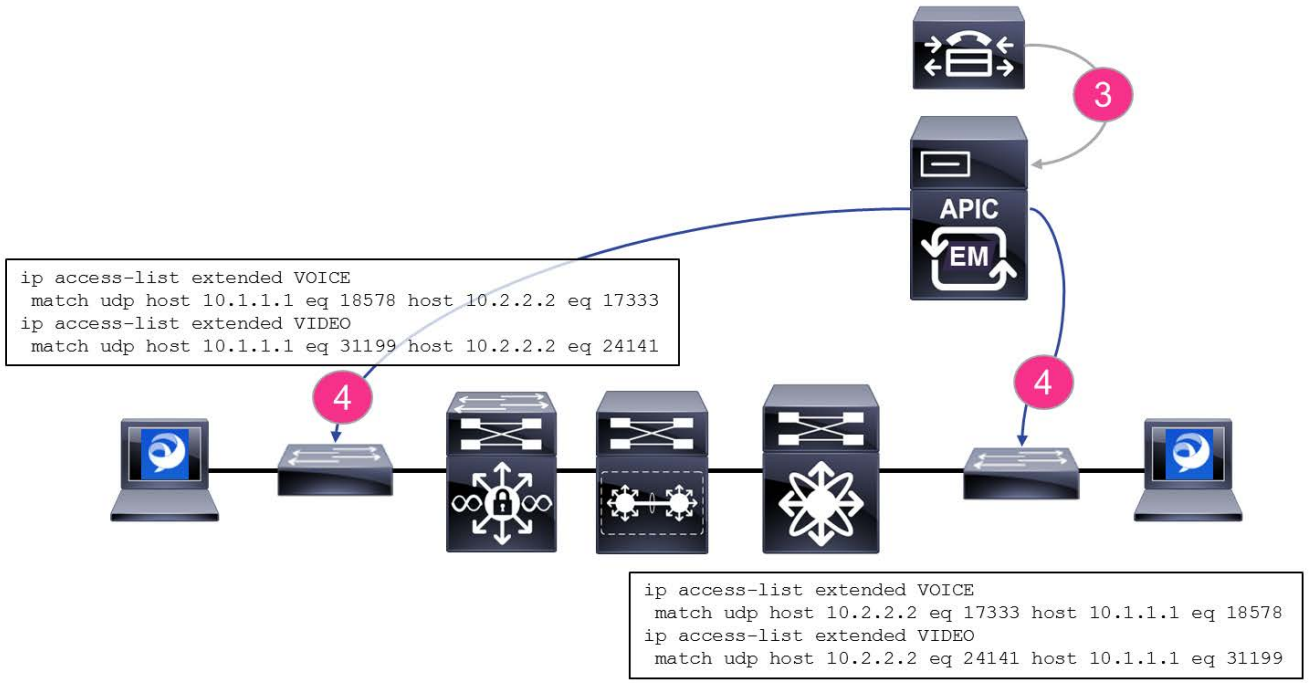


Figure 4 APIC-EM Dynamic QoS Policies - Steps 3 (APIC-EM is Informed of a Proceeding Call) and 4 (Dynamic ACEs are Pushed)



Copyright © 2015 Cisco Systems, Inc. All rights reserved. Cisco, the Cisco logo, Cisco Systems, and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.