We’re ready.
Are you?
The QoS Paradigm Shift

Tim Szigeti
BRKRST-2056
szigeti@cisco.com
@tim_szigeti
http://tinyurl.com/j6cz9rz
October 1
331 B.C.
Gaugamela
October 1
331 B.C.
Gaugamela

Alexander of Macedon
47,000

Darius III of Persia
200,000-
1,000,000
strategy |ˈstrætəjē| noun (pl. strategies)
a plan of action or policy designed to achieve a major or overall aim.

tactic |ˈtaktɪk| noun
an action carefully planned to immediately support a higher-level objective, aiming at an end beyond the immediate action.
Often contrasted with strategy.
## Alexander the Great’s Strategy and Tactics

**Overall Goal:** Conquer Persia, The World

**Strategy:**
- **Priority:** Attack the King
- **Guarantee:** Loyalty of his troops
- **Fairness:** Conquered Subjects
- **Penalize:** Greek mercenaries, rebellion, insurrection

### Tactics @ Granicus
- Attack the King
- Lead from the front & reward the troops
- Fair treatment of conquered subjects
- Greek mercenaries fighting for Persia

### Tactics @ Issus
- Attack the King
- Lead from the front & reward the troops
- Fair treatment of conquered subjects, including VIP prisoners: Darius wife, mother and two daughters
- Greek mercenaries

### Tactics @ Gaugamela
- Attack the King
- Lead from the front & reward troops
- Fair treatment of conquered subjects
- Greek Mercenaries fighting for Persia
- Refrain from action if not aligned to strategy
Session Goals

By the end of this session, you should be able to...

- Apply Cisco’s QoS paradigm shift to meet your business needs
- Deploy Cisco’s most popular campus feature
- Configure QoS for 1400+ apps in a standards-based 12-class model—within 60 lines of (non-macro) CLI
- Appreciate a technology that can unambiguously identify thousands of applications on any network device and without any client software—even if these applications are encrypted!
- Understand the inner-workings of Cisco’s platform for SDN QoS in the enterprise
Agenda

- The QoS Paradigm Shift
- Strategic and Tactical QoS Design Case Study
- AutoQoS SRND4
- NBAR2 QoS Attributes
- DNS-AS
- Prime Infrastructure AVC/QoS Profiles
- APIC-EM EasyQoS (SDN QoS)
- Looking Forward
- Summary and References
The QoS Paradigm Shift
The Why / How / What of Enterprise Networking

Why
Transform our customers’ businesses through powerful yet simple networks.

How

What
Cisco Enterprise Vision
What Do You Consider First?
Where to Begin?

Always, Always, Always Start with Defining Your Business **Goals** of QoS

- *Guaranteeing voice quality* meets enterprise standards
- Ensuring a *high Quality of Experience for video* applications
- *Improving user productivity* by minimizing network response times
- *Managing* business applications that are “**bandwidth hogs**”
- Identifying and *de-prioritizing non-business applications*
- Improving network availability by *protecting the control planes*
- *Hardening the network* infrastructure to deal with abnormal events
Levels of QoS Policy Abstraction

Strategic vs. Tactical

• **Strategic QoS Policy (WHY)**
  - reflects *business intent*
  - *not* constrained by any technical or administrative limitation
  - end-to-end

• **Tactical QoS Policy (HOW)**
  - expresses the strategic business intent with maximum fidelity
  - limited by *tactical constraints*, including:
    - Media (e.g. WLAN has only 4 levels of service)
    - Platform (e.g. Catalyst 3750 has only 4 hardware queues)
    - Interface (e.g. T1 WAN link has limited bandwidth)
    - Role (e.g. CE may need to map into reduced sub-set of SP Classes-of-Service)
Defining the Strategic QoS Policy
Defining the Strategic QoS Policy

Three Step Process

1) Decide the business-relevance of applications

2) Assign the appropriate (RFC 4594) traffic-class for the application

3) Specify target bandwidth allocations per traffic-class
Determining Business Relevance

How Important is an Application to Your Business?

- Relevant
  - These applications directly support business objectives
  - Applications should be classified, marked and treated according to industry best-practice recommendations
  - RFC 4594

- Default
  - These applications may/may not support business objectives (e.g. HTTP/HTTPS/SSL)
  - Applications of this type should be treated with a Default Forwarding service
  - RFC 2474

- Irrelevant
  - These applications do not support business objectives and are typically consumer-oriented
  - Applications of this type should be treated with a “less-than Best Effort” service
  - RFC 3662
**What Do We Do Under-the-Hood?**

Apply RFC 4594-based Marking / Queuing / Dropping Treatments

<table>
<thead>
<tr>
<th>Application Class</th>
<th>Per-Hop Behavior</th>
<th>Queuing &amp; Dropping</th>
<th>Application Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>VoIP Telephony</td>
<td>EF Priority Queue (PQ)</td>
<td>Cisco IP Phones (G.711, G.729)</td>
<td></td>
</tr>
<tr>
<td>Broadcast Video</td>
<td>CS5 (Optional) PQ</td>
<td>Cisco IP Video Surveillance / Cisco Enterprise TV</td>
<td></td>
</tr>
<tr>
<td>Real-Time Interactive</td>
<td>CS4 (Optional) PQ</td>
<td>Cisco TelePresence</td>
<td></td>
</tr>
<tr>
<td>Multimedia Conferencing</td>
<td>AF4 BW Queue + DSCP WRED</td>
<td>Cisco Jabber, Cisco WebEx</td>
<td></td>
</tr>
<tr>
<td>Multimedia Streaming</td>
<td>AF3 BW Queue + DSCP WRED</td>
<td>Cisco Digital Media System (VoDs)</td>
<td></td>
</tr>
<tr>
<td>Network Control</td>
<td>CS6 BW Queue</td>
<td>EIGRP, OSPF, BGP, HSRP, IKE</td>
<td></td>
</tr>
<tr>
<td>Signaling</td>
<td>CS3 BW Queue</td>
<td>SCCP, SIP, H.323</td>
<td></td>
</tr>
<tr>
<td>Ops / Admin / Mgmt (OAM)</td>
<td>CS2 BW Queue</td>
<td>SNMP, SSH, Syslog</td>
<td></td>
</tr>
<tr>
<td>Transactional Data</td>
<td>AF2 BW Queue + DSCP WRED</td>
<td>ERP Apps, CRM Apps, Database Apps</td>
<td></td>
</tr>
<tr>
<td>Bulk Data</td>
<td>AF1 BW Queue + DSCP WRED</td>
<td>E-mail, FTP, Backup Apps, Content Distribution</td>
<td></td>
</tr>
<tr>
<td>Default Forwarding</td>
<td>DF Default Queue + RED</td>
<td>Default Class</td>
<td></td>
</tr>
<tr>
<td>Scavenger</td>
<td>CS1 Min BW Queue (Deferential)</td>
<td>YouTube, Netflix, iTunes, BitTorrent, Xbox Live</td>
<td></td>
</tr>
</tbody>
</table>

**Relevant**

**Default**

**Irrelevant**

Apply RFC 4594-based Marking / Queuing / Dropping Treatments
<table>
<thead>
<tr>
<th>Application Class</th>
<th>Per-Hop Behavior</th>
<th>Queuing &amp; Dropping</th>
<th>Application Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>VoIP Telephony</td>
<td>EF</td>
<td>Priority Queue (PQ)</td>
<td>Cisco IP Phones (G.711, G.729)</td>
</tr>
<tr>
<td>Broadcast Video</td>
<td>CS5</td>
<td>(Optional) PQ</td>
<td>Cisco IP Video Surveillance / Cisco Enterprise TV</td>
</tr>
<tr>
<td>Real-Time Interactive</td>
<td>CS4</td>
<td>(Optional) PQ</td>
<td>Cisco TelePresence</td>
</tr>
<tr>
<td>Multimedia Conferencing</td>
<td>AF4</td>
<td>BW Queue + DSCP WRED</td>
<td>Cisco Jabber, Cisco WebEx</td>
</tr>
<tr>
<td>Multimedia Streaming</td>
<td>AF3</td>
<td>BW Queue + DSCP WRED</td>
<td>Cisco Digital Media System (VoDs)</td>
</tr>
<tr>
<td>Network Control</td>
<td>CS6</td>
<td>BW Queue</td>
<td>EIGRP, OSPF, BGP, HSRP, IKE</td>
</tr>
<tr>
<td>Signaling</td>
<td>CS3</td>
<td>BW Queue</td>
<td>SCCP, SIP, H.323</td>
</tr>
<tr>
<td>Ops / Admin / Mgmt (OAM)</td>
<td>CS2</td>
<td>BW Queue</td>
<td>SNMP, SSH, Syslog</td>
</tr>
<tr>
<td>Transactional Data</td>
<td>AF2</td>
<td>BW Queue + DSCP WRED</td>
<td>ERP Apps, CRM Apps, Database Apps</td>
</tr>
<tr>
<td>Bulk Data</td>
<td>AF1</td>
<td>BW Queue + DSCP WRED</td>
<td>E-mail, FTP, Backup Apps, Content Distribution</td>
</tr>
<tr>
<td>Default Forwarding</td>
<td>DF</td>
<td>Default Queue + RED</td>
<td>Default Class</td>
</tr>
<tr>
<td>Scavenger</td>
<td>CS1</td>
<td>Min BW Queue (Deferential)</td>
<td>YouTube, Netflix, iTunes, BitTorrent, Xbox Live</td>
</tr>
</tbody>
</table>
Application Classification Rules

Is the Protocol a Control Plane Protocol?

- Network Control protocol?
  - network routing and control-plane protocols
    - E.g. BGP, OSPF, EIGRP, HSRP, IKE, etc.

- Signaling protocol?
  - call signaling / bandwidth reservation protocols
    - E.g. SIP, Skinny, H.323, RSVP etc.

- Operations / Administration / Management protocol?
  - network management protocols (e.g. SNMP, Telnet, SSH, Syslog, NetFlow, etc.)
Application Classification Rules (cont.)

Is the Application Voice?

- Voice?
  - Audio-only media (e.g. G.711, G.729 etc.)
    - Note: This class may be used for the audio-component of multimedia applications, such as Cisco Jabber and/or Spark; however, this option should ONLY be considered if this causes no conflict with your overall Call Admission Control strategy and voice-queue provisioning.
Application Classification Rules (cont.)

Is the Application Video?

- Video?
  - Is the application is unidirectional or bidirectional?
  - Is the application is elastic (i.e. adaptive to congestion/drops) or inelastic?

---

- Multimedia-Streaming
- Broadcast Video
- Multimedia-Conferencing
- Realtime-Interactive
Application Classification Rules (cont.)

Is the Application Data?

- Data?
  - Is the application foreground or background?
    - Foreground applications will directly impact user-productivity with network delays
    - Background applications will not (as these are typically machine-to-machine flows)
      - However, these apps can be very bandwidth intensive (if unrestrained)
      - If it is not known if a data app is foreground, then assume it is background
  - Otherwise – the application/protocol remains in the default class (Best Effort)
Strategic Target Bandwidth Allotment Example

- Voice: 10%
- Broadcast Video: 10%
- Real-Time Interactive: 13%
- Network Control: 2%
- OAM: 3%
- Signaling: 2%
- Multimedia Conferencing: 10%
- Multimedia Streaming: 10%
- Transactional Data: 10%
- Bulk Data: 4%
- Scavenger: 1%
- Best Effort: 25%
- Transactional Data: 10%
- Bulk Data: 4%
Strategic QoS At-A-Glance

The Quality of Service Challenge
Today there is an urgent need for multimedia applications on the IP network. This explosion of content and media traffic, both business-related and unsupervised, requires network architects to take a new look at their network design.

Step 1: Articulate Business Intent and Application Relevance
The first step may be obvious, but in actuality it is crucial: clearly define the business objectives that your QoS solutions will serve. These may include any of the following:

- Guaranteeing voice quality meets enterprise standards
- Ensuring a high level of Quality of Experience (QoE) for video
- Providing guaranteed network resource response times for interactive applications
- Managing applications that are "business-critical"
- Identifying and prioritizing consumer applications
- Increasing network availability
- Maintaining network reliability

With these goals in mind, network architects can clearly identify and address the specific requirements of the business. Conversely, this exercise will also make visible which applications are not relevant to achieving business objectives. Such applications may require consumer-oriented or for-entertainment-oriented options.

Finally, there may be applications that are not in the current business environment. For example, in the public sector, there may be early business applications that do not require QoS. In such cases, deep packet inspection technologies may be able to identify, prioritize, and classify traffic, such that QoS is properly classified in the business objectives.

Figure 2: Determining Application Business Relevance

Strategic QoS Design

The key to a successful QoS design is to look at the traffic streams from an application perspective.

Figure 3: Control Plane Traffic Classes

Step 2: Define an End-to-End QoS Design Strategy
This design strategy is based on meeting the requirements of the above business objectives and standards. Business applications can be grouped into one of four main categories:

- Voice applications
- Video applications
- Data applications

These guidelines are to be used as industry best-practice recommendations. As such, enterprises and service providers are encouraged to adopt these practices and provide the necessary adaptations and implementations to ensure QoS consistency, comparability, and reproducibility. In addition, it should be noted that these guidelines are not intended to mandate as such, they may be revised or modified as conditions evolve.

Thus, to meet specific business requirements, QoS has been designed to provide a flexible network that can be configured to meet the needs of the business. Specifically, the implementation of Call Signaling and Broadcast Video is based on QoS and QCI. As a result, QoS and QCI are necessary. A summary of the Cisco implementation of RFC 4544 is shown in Figure 2.

RFC 4544 also provides some application classification rules to help network designers to assign traffic to the traffic classes, which are summarized in the following sections.

Figure 4: Video Traffic Classifications

Business relevant traffic can be grouped into one of the following categories:

- Connect guest profiles
- VoIP applications
- Video applications
- Data applications

(Step 2 continues on the next page.)
Defining Tactical QoS Policies
Defining the Tactical QoS Policy

Objectives and Method

• The **principle goal** of the tactical QoS policy is to **express the strategic QoS policy to the maximum capacity possible**, given the relevant tactical constraints
  • e.g. if more than 4 classes of traffic are considered business relevant and a platform has only 4 hardware queues, then these will be mapped as efficiently as possible into the platform’s queuing model

• QoS features should only be selectively enabled if they directly contribute to expressing the strategic policy on a given platform
  • i.e. QoS features will not be enabled simply for the sake of enabling features

• QoS design **best practices** will be used to generate platform-specific configurations to **reflect the strategic QoS policy with maximum fidelity**
QoS Design Best Practices

Classification & Marking Best Practices

- Always enable QoS policies in hardware—rather than software—whenever a choice exists.
- Classify and mark applications as close to their sources as technically and administratively feasible.
- Use DSCP marking whenever possible.
- Follow standards-based DSCP PHB markings to ensure interoperability and future expansion.

A QoS Tools Review is included in the Appendix.

IPv4 Packet

<table>
<thead>
<tr>
<th>Version/Header_Len</th>
<th>ToS/Byte</th>
<th>Length</th>
<th>ID</th>
<th>Offset</th>
<th>TTL</th>
<th>Protocol</th>
<th>FCS</th>
<th>IP SA</th>
<th>IP DA</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DiffServ Code Point (DSCP)</td>
<td>IP ECN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
QoS Design Best Practices

Policing and Remarking Best Practices

• Police traffic flows as close to their source as possible
• Whenever possible, markdown according to standards-based rules
• For Example: Assured Forwarding Traffic (AF21 example)
  • Conforming AF21 traffic is marked/remarked AF21
  • Exceeding AF21 traffic is remarked AF22
  • Violating AF21 traffic is remarked AF23

![Diagram of QoS Design Best Practices]

Packet of Size B

B>Tp

PIR

PBS

No

Yes

Violate

Action

B>Tc

CIR

CBS

No

Yes

Exceed

Action

Conform

Action
QoS Design Best Practices

Queuing Best Practices

• Enable queuing policies at every node that has the potential for congestion
• Whenever possible, assign each application class to its own dedicated queue
• Use only platforms and/or service providers that offer a minimum of four standards-based queuing behaviors:
  • An RFC 3246 Expedited Forwarding Per-Hop Behavior
  • An RFC 2597 Assured Forwarding Per-Hop Behavior
  • An RFC 2474 Default Forwarding Per-Hop Behavior
  • An RFC 3662 Lower Effort Per-Domain Behavior
QoS Design Best Practices

WRED Principles

• Enable DSCP-based WRED on AF queues and DF queue
• Do not enable DSCP-based WRED on the EF queue
• Do not enable WRED on control traffic application class queues
• WRED is not required on the Scavenger queue

• Optional: Tune WRED thresholds consistently—for example:
  • Set the minimum WRED thresholds for AFx3 to 60% of the queue depth
  • Set the minimum WRED thresholds for AFx2 to 70% of the queue depth
  • Set the minimum WRED thresholds for AFx1 to 80% of the queue depth
  • Set all maximum WRED thresholds to 100%
QoS Design Best Practices

Per-Hop Behavior Principles

• **EF Queue Recommendations:**
  • Limit the amount of strict priority queuing to 33% of link bandwidth capacity
  • Govern strict-priority traffic with an admission control mechanism
  • Do not enable WRED on this queue

• **AF Queue Recommendations:**
  • Provision guaranteed bandwidth allocations according to application requirements
  • Enable DSCP-based WRED on this queue(s)

• **DF Queue Recommendations:**
  • Provision at least 25 percent of link bandwidth for the default Best Effort class
  • Enable WRED (effectively RED) on the default class

• **Scavenger Queue Recommendations:**
  • Assign minimum bandwidth to the Scavenger-class queue
  • WRED is not required on the Scavenger-class queue
Trust Boundaries

The trust boundary is the edge where
- Layer 2 (CoS / UP) and/or
- Layer 3 (DSCP)
markings are accepted or rejected.

- **Untrusted / User-Administered Devices**
  - `no mls qos trust`

- **Trusted Centrally-Administered Devices**
  - `mls qos trust dscp`

- **Centrally-Administered & Conditionally-Trusted Devices**
  - `mls qos trust device`
  - `cisco-phone`
  - `cts`
  - `ip-camera`
  - `media-player`
Policy Enforcement Points (PEPs)

- The Policy Enforcement Point (PEP) is the edge where classification and marking policies are enforced.
- The PEP may or may not be the same as the trust boundary.
- Multiple PEPs may exist for different types of network devices:
  - e.g. switch PEP vs. router PEP.

Note: For the sake of simplification, in this deck PEP will refer to classification and marking policy enforcement points (only) and will not include other policy enforcement points (e.g. queuing).
Tactical QoS Design At-A-Glance

Cisco live!

https://cisco.box.com/s/8izevlg4k6gaggh3cmrc16lugm6sdr8y
Agenda

- The QoS Paradigm Shift
- **Strategic and Tactical QoS Design Case Study**
- AutoQoS SRND4
- NBAR2 QoS Attributes
- DNS-AS
- Prime Infrastructure AVC/QoS Profiles
- APIC-EM EasyQoS (SDN QoS)
- Looking Forward
- Summary and References
Strategic and Tactical QoS Design
Case Study

All Case Study detailed chapters *with full-configs* are posted at:
https://cisco.box.com/s/8izevlg4k6gaggh3cmrc16lugm6sdr8y
Case Study: Tifosi Software
Original Four-Class QoS and Queuing Models

<table>
<thead>
<tr>
<th>4-Class Model</th>
<th>DSCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>EF</td>
</tr>
<tr>
<td>Signaling</td>
<td>CS3</td>
</tr>
<tr>
<td>“Mission-Critical Data”</td>
<td>AF31</td>
</tr>
<tr>
<td>Best Effort</td>
<td>DF</td>
</tr>
</tbody>
</table>

Pie chart showing:
- Voice: 33%
- “Mission-Critical Data”: 35%
- Signaling: 7%
- Best Effort: 25%
Case Study: Tifosi Software

Current Business Requirements

• The imminent deployment of two dozen Cisco TelePresence Systems
  • one each in every major engineering and sales office
  • with future plans for more to come

• The emerging popularity of multimedia collaboration applications
  • including Cisco WebEx, Cisco Jabber, as well as Microsoft Lync

• Too many applications classified as “mission critical”
  • including email, file-transfers, backup operations, etc.

• The identification of “substantial” amounts of non-business traffic on the network during work hours
  • including Netflix, YouTube, BitTorrent and iTunes downloads, as well as gaming traffic

• A desire for greater overall QoS policy-consistency
Case Study: Tifosi Software
Proposed Eight-Class Strategic QoS Model

<table>
<thead>
<tr>
<th>8-Class Model</th>
<th>DSCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>EF</td>
</tr>
<tr>
<td>Real-Time Interactive</td>
<td>CS4</td>
</tr>
<tr>
<td>Signaling</td>
<td>CS3</td>
</tr>
<tr>
<td>Multimedia Conferencing</td>
<td>AF41</td>
</tr>
<tr>
<td>Transactional Data</td>
<td>AF21</td>
</tr>
<tr>
<td>Bulk Data</td>
<td>AF11</td>
</tr>
<tr>
<td>Scavenger</td>
<td>CS1</td>
</tr>
<tr>
<td>Best Effort</td>
<td>DF</td>
</tr>
</tbody>
</table>

- Voice: 10%
- Real-Time Interactive: 23%
- Signaling: 2%
- Multimedia Conferencing: 10%
- Transactional Data: 25%
- Bulk Data: 4%
- Scavenger: 1%
- Best Effort: 25%
- Mission Critical Data: CS3 AF21 EF DSCP CS1 DF AF11 CS4
Case Study: Tifosi Software
Campus Access Catalyst 3750 Eight-Class (1P3Q3T) Egress Queuing Model

Application Classes
- Voice
- Realtime Interactive
- Multimedia Conferencing
- Signaling
- Transactional Data
- Bulk Data
- Scavenger
- Best Effort

DSCP
- EF
- CS4
- AF4
- CS3
- AF2
- AF1
- CS1
- DF

1P3Q3T
- AF1 Queue 4 Q4T2
- CS1 (5%) Q4T1
- Default Queue
- Queue 3 (35%)
- CS3 Queue 2 Q2T2
- AF4 (30%) Q2T1
- AF2
- EF Q1 Priority Queue
- CS4

1P3Q3T=
1 Priority Queue
3 (Non-Priority) Queues
(each with)
3 Drop Thresholds

Q2T1=
Queue 2, Threshold 1
# Case Study: Tifosi Software

Campus Distribution Catalyst 4500 Eight-Class (1P7Q1T+DBL) Queuing Model

<table>
<thead>
<tr>
<th>Application Classes</th>
<th>DSCP</th>
<th>1P7Q1T + DBL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>EF</td>
<td>EF</td>
</tr>
<tr>
<td>Realtime Interactive</td>
<td>CS4</td>
<td>CS4</td>
</tr>
<tr>
<td>Multimedia Conferencing</td>
<td>AF4</td>
<td>Multimedia Conferencing Queue (10% BWR + DBL)</td>
</tr>
<tr>
<td>Signaling</td>
<td>CS3</td>
<td>Signaling Queue (2% BWR)</td>
</tr>
<tr>
<td>Transactional Data</td>
<td>AF2</td>
<td>Transactional Data Queue (25% BWR + DBL)</td>
</tr>
<tr>
<td>Bulk Data</td>
<td>AF1</td>
<td>Bulk Data Queue (4% BWR + DBL)</td>
</tr>
<tr>
<td>Scavenger</td>
<td>CS1</td>
<td>Scavenger (1% BWR)</td>
</tr>
<tr>
<td>Best Effort</td>
<td>DF</td>
<td>Default Queue (25% BWR + DBL)</td>
</tr>
</tbody>
</table>

**Notes:**
- **DBL** = Dynamic Buffer Limiting
- **BWR** = Bandwidth Remaining

**Case Study:**
Tifosi Software Campus Distribution Catalyst 4500 Eight-Class (1P7Q1T+DBL) Queuing Model
Case Study: Tifosi Software
Campus Core Catalyst 6500 Eight-Class (8Q4T & 1P7Q4T) Queuing Models

<table>
<thead>
<tr>
<th>Application Classes</th>
<th>DSCP</th>
<th>8Q4T / 1P7Q4T + WRED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>EF</td>
<td>EF</td>
</tr>
<tr>
<td>Realtime Interactive</td>
<td>CS4</td>
<td>CS4 (33% BW/Priority)</td>
</tr>
<tr>
<td>Signaling</td>
<td>CS3</td>
<td>CS3 (2% BW/BWR)</td>
</tr>
<tr>
<td>Multimedia Conferencing</td>
<td>AF4</td>
<td>AF4 (10% BW/BWR + DSCP-based WRED)</td>
</tr>
<tr>
<td>Transactional Data</td>
<td>AF2</td>
<td>AF2 (25% BW/BWR + DSCP-based WRED)</td>
</tr>
<tr>
<td>Bulk Data</td>
<td>AF1</td>
<td>AF1 (4% BW/BWR + DSCP-based WRED)</td>
</tr>
<tr>
<td>Scavenger</td>
<td>CS1</td>
<td>CS1 (1% BW/BWR)</td>
</tr>
<tr>
<td>Best Effort</td>
<td>DF</td>
<td>DF (25% BW/BWR + WRED)</td>
</tr>
</tbody>
</table>

- Realtime-Queue (33% BW/Priority)
- Signaling Queue (2% BW/BWR)
- Multimedia Conferencing Queue (10% BW/BWR + DSCP-based WRED)
- Transactional Data Queue (25% BW/BWR + DSCP-based WRED)
- Bulk Data Queue (4% BW/BWR + DSCP-based WRED)
- Scavenger Queue (1% BW/BWR)
- Default Queue (25% BW/BWR + WRED)
Case Study: Tifosi Software
Centralized Cisco 5508 Wireless LAN Controller (8.1MR) 802.11e WMM Model

<table>
<thead>
<tr>
<th>Application Classes</th>
<th>DSCP</th>
<th>802.11e User Priorities (UP) &amp; WLC Access Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>EF → UP 6</td>
<td>UP 7</td>
</tr>
<tr>
<td>Realtime Interactive</td>
<td>CS4 → UP 5</td>
<td>UP 6</td>
</tr>
<tr>
<td>Signaling</td>
<td>CS3 → UP 4</td>
<td>UP 5</td>
</tr>
<tr>
<td>Multimedia Conferencing</td>
<td>AF4</td>
<td>UP 4</td>
</tr>
<tr>
<td>Transactional Data</td>
<td>AF2 → UP 3</td>
<td>UP 3</td>
</tr>
<tr>
<td>Bulk Data</td>
<td>AF1 → UP 2</td>
<td>UP 0</td>
</tr>
<tr>
<td>Scavenger</td>
<td>CS1</td>
<td>UP 2</td>
</tr>
<tr>
<td>Best Effort</td>
<td>DF</td>
<td>UP 1</td>
</tr>
</tbody>
</table>
# Case Study: Tifosi Software

DC Fabric Cisco Nexus 7000 F2 (nq-7e: 4Q1T / 1P3Q1T) Queuing Model

<table>
<thead>
<tr>
<th>Application Class</th>
<th>DSCP</th>
<th>CoS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Control</td>
<td>N/A</td>
<td>CoS 7</td>
</tr>
<tr>
<td>Internetwork Control</td>
<td>CS6</td>
<td>CoS 6</td>
</tr>
<tr>
<td>Voice / Realtime Interactive</td>
<td>EF / CS4</td>
<td>CoS 5</td>
</tr>
<tr>
<td>Video / Signaling</td>
<td>AF4 / CS3*</td>
<td>CoS 4</td>
</tr>
<tr>
<td>FCoE</td>
<td>N/A</td>
<td>CoS 3</td>
</tr>
<tr>
<td>Transactional Data</td>
<td>AF2</td>
<td>CoS 2</td>
</tr>
<tr>
<td>Bulk Data / vMotion</td>
<td>AF1 / N/A</td>
<td>CoS 1*</td>
</tr>
<tr>
<td>Best Effort</td>
<td>DF</td>
<td>CoS 0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4Q1T / 1P3Q1T</th>
</tr>
</thead>
<tbody>
<tr>
<td>CoS 7</td>
</tr>
<tr>
<td>In-Q1 / Out-PQ1</td>
</tr>
<tr>
<td>4Q1T: 25% BW + 7% QL</td>
</tr>
<tr>
<td>CoS 6</td>
</tr>
<tr>
<td>4Q1T: 25% BW + 31% QL</td>
</tr>
<tr>
<td>CoS 5</td>
</tr>
<tr>
<td>1P3Q1T: Priority Level 1</td>
</tr>
<tr>
<td>CoS 4</td>
</tr>
<tr>
<td>In-Q3 / Out-Q3</td>
</tr>
<tr>
<td>4Q1T: 25% BW + 31% QL</td>
</tr>
<tr>
<td>CoS 2</td>
</tr>
<tr>
<td>1P3Q1T: 20% BWR</td>
</tr>
<tr>
<td>CoS 3</td>
</tr>
<tr>
<td>In-Q4 / Out-Q2</td>
</tr>
<tr>
<td>4Q1T: 25% BW + 30% QL</td>
</tr>
<tr>
<td>No Drop</td>
</tr>
<tr>
<td>1P3Q1T: 40% BWR</td>
</tr>
<tr>
<td>CoS 1*</td>
</tr>
<tr>
<td>Q-Default</td>
</tr>
<tr>
<td>(In-Q2 / Out-Q4)</td>
</tr>
<tr>
<td>4Q1T: 25% BW + 32% QL</td>
</tr>
<tr>
<td>CoS 0</td>
</tr>
<tr>
<td>1P3Q1T: 40% BWR</td>
</tr>
</tbody>
</table>
## Case Study: Tifosi Software

**MPLS VPN Customer-Edge Enterprise-to-Service Provider Mapping**

<table>
<thead>
<tr>
<th>Customer 8-Class Model</th>
<th>DSCP</th>
<th>SP Six-Class Model Classes-of-Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>EF</td>
<td>EF, CS5</td>
</tr>
<tr>
<td>Realtime Interactive</td>
<td>CS4</td>
<td>SP-REALTIME-CLASS (RTP) LLQ 10%</td>
</tr>
<tr>
<td>Signaling</td>
<td>CS3 → CS4</td>
<td>AF41, CS4</td>
</tr>
<tr>
<td>Multimedia Conferencing</td>
<td>AF41 → AF31</td>
<td>SP-AF4-CLASS (RTP) CBWFQ 25% BW + DSCP-WRED</td>
</tr>
<tr>
<td>Transactional Data</td>
<td>AF21</td>
<td>SP-AF3-CLASS (UDP) CBWFQ 10% BW + DSCP-WRED</td>
</tr>
<tr>
<td>Bulk Data</td>
<td>AF11</td>
<td>SP-AF2-CLASS (TCP) CBWFQ 25% BW + DSCP-WRED</td>
</tr>
<tr>
<td>Scavenger</td>
<td>CS1</td>
<td>SP-AF1-CLASS (Control) CBWFQ 5% BW + DSCP-WRED</td>
</tr>
<tr>
<td>Best Effort</td>
<td>DF</td>
<td>SP-DEFAULT-CLASS CBWFQ 25% BW + WRED</td>
</tr>
</tbody>
</table>
Agenda

• The QoS Paradigm Shift
• Strategic and Tactical QoS Design Case Study
• AutoQoS SRND4
• NBAR2 QoS Attributes
• DNS-AS
• Prime Infrastructure AVC/QoS Profiles
• APIC-EM EasyQoS (SDN QoS)
• Looking Forward
• Summary and References
AutoQoS SRND4
“The biggest obstacle to deploying QoS is the complexity.

“QoS is complicated enough to begin with and then you make it different on every platform!”

Cisco Customers
AutoQoS SRND4 Overview

- AutoQoS features are based on QoS Design Guides
- Cisco has provided AutoQoS for VoIP since 2002
- Cisco has expanded AutoQoS to include:
  - Cisco TelePresence
  - Cisco IP Video Surveillance
  - Multimedia conferencing applications
  - Multimedia streaming applications
  - Transactional data applications
  - Bulk data applications
  - Scavenger applications
- An administrator can automatically provision platform-specific best-practice designs via a single interface-level command
  
  AutoQoS is the most deployed feature on Cisco Catalyst switches (26%)
AutoQoS SRND4

1P1Q3T Ingress Queuing Policies

1P3Q3T Egress Queuing Policies

auto qos voip [ cisco-phone | cisco-softphone | trust ]

auto qos trust { cos | dscp }

auto qos video [ cts | ip-camera ]
AutoQoS SRND4—VoIP Models

1P3Q3T Ingress Queuing Policies

1P3Q3T Egress Queuing Policies

VoIP Classifier
- Mark EF
- VoIP Policer (<128 kbps)

Signaling Classifier
- Mark CS3
- Signaling Policer (<32 kbps)

Best Effort (Class-Default)
- Mark DF
- Best Effort Policer (<10 Mbps)

VoIP Classifier
- Mark EF
- VoIP Policer (<128 kbps)

Signaling Classifier
- Mark CS3
- Signaling Policer (<32 kbps)

Multimedia Conferencing Classifier
- Mark AF41
- MM-Conf Policer (<5 Mbps)

Signaling Classifier
- Mark CS3
- Signaling Policer (<32 kbps)

Transactional Data Classifier
- Mark AF21
- Trans-Data Policer (<10 Mbps)

Bulk Data Classifier
- Mark AF11
- Bulk Data Policer (<10 Mbps)

Scavenger Classifier
- Mark CS1
- Scavenger Policer (<10 Mbps)

Best Effort (Class-Default)
- Mark DF
- Best Effort Policer (<10 Mbps)

Best Effort (Class-Default)
- Mark DF
- Best Effort Policer (<10 Mbps)

VoIP Participant
- Mark EF
- VoIP Policer (<128 kbps)

Signaling Participant
- Mark CS3
- Signaling Policer (<32 kbps)

VoIP Call
- Mark AF41
- MM-Conf Policer (<5 Mbps)

Signaling Call
- Mark CS3
- Signaling Policer (<32 kbps)

Optical Network Unit
- Mark AF21
- Trans-Data Policer (<10 Mbps)

Data Center
- Mark AF11
- Bulk Data Policer (<10 Mbps)

Network Access Point
- Mark CS1
- Scavenger Policer (<10 Mbps)

Best Effort (Class-Default)
- Mark DF
- Best Effort Policer (<10 Mbps)

1P3Q3T Ingress Queuing Policies

1P3Q3T Egress Queuing Policies

VoIP Classifier
- Mark EF
- VoIP Policer (<128 kbps)

Signaling Classifier
- Mark CS3
- Signaling Policer (<32 kbps)

Best Effort (Class-Default)
- Mark DF
- Best Effort Policer (<10 Mbps)

VoIP Classifier
- Mark EF
- VoIP Policer (<128 kbps)

Signaling Classifier
- Mark CS3
- Signaling Policer (<32 kbps)

Multimedia Conferencing Classifier
- Mark AF41
- MM-Conf Policer (<5 Mbps)

Signaling Classifier
- Mark CS3
- Signaling Policer (<32 kbps)

Transactional Data Classifier
- Mark AF21
- Trans-Data Policer (<10 Mbps)

Bulk Data Classifier
- Mark AF11
- Bulk Data Policer (<10 Mbps)

Scavenger Classifier
- Mark CS1
- Scavenger Policer (<10 Mbps)

Best Effort (Class-Default)
- Mark DF
- Best Effort Policer (<10 Mbps)
AutoQoS SRND 4 At-A-Glance

The QoS Challenge for Campus Networks

Today there is a virtual explosion of media applications on the Internet due to a myriad of popular web, video, and data applications. For example, online streaming on-demand video sources are giving rise to a new wave of streaming media services that are becoming increasingly popular. As a result, network administrators are faced with the challenge of managing QoS for these applications.

To address this challenge, Cisco has developed the Cisco QoS solution, which includes the following features:

1. Classifying and policing traffic
2. Marking traffic
3. Shaping traffic
4. Rate limiting and policing
5. Mapping traffic to interface with appropriate QoS services
6. Implementing QoS policies
7. Monitoring QoS operations

AutoQoS for Campus Networks

AutoQoS is a comprehensive solution that provides end-to-end QoS for campus networks. It includes the following features:

1. Easy-to-use graphical user interface
2. Automatic configuration of QoS policies
3. Real-time monitoring of QoS operations
4. Integration with other Cisco products

AutoQoS Classification

AutoQoS Classification is a key component of the AutoQoS solution. It includes the following features:

1. Automatic classification of traffic
2. Classification based on traffic patterns
3. Classification based on application
4. Classification based on network topology

AutoQoS Video

AutoQoS Video is a key component of the AutoQoS solution. It includes the following features:

1. Automatic classification of video traffic
2. Classification based on video type
3. Classification based on video quality
4. Classification based on video stream

AutoQoS Voice

AutoQoS Voice is a key component of the AutoQoS solution. It includes the following features:

1. Automatic classification of voice traffic
2. Classification based on voice type
3. Classification based on voice quality
4. Classification based on voice stream

AutoQoS VPN

AutoQoS VPN is a key component of the AutoQoS solution. It includes the following features:

1. Automatic classification of VPN traffic
2. Classification based on VPN type
3. Classification based on VPN quality
4. Classification based on VPN stream

AutoQoS Data

AutoQoS Data is a key component of the AutoQoS solution. It includes the following features:

1. Automatic classification of data traffic
2. Classification based on data type
3. Classification based on data quality
4. Classification based on data stream

AutoQoS PCRF

AutoQoS PCRF is a key component of the AutoQoS solution. It includes the following features:

1. Automatic classification of PCRF traffic
2. Classification based on PCRF type
3. Classification based on PCRF quality
4. Classification based on PCRF stream

Some key terms to remember:

- Cisco QoS: A comprehensive solution for managing QoS in campus networks
- AutoQoS: A key component of the Cisco QoS solution
- AutoQoS Classification: A key component of the AutoQoS solution
- AutoQoS Video: A key component of the AutoQoS solution
- AutoQoS Voice: A key component of the AutoQoS solution
- AutoQoS Data: A key component of the AutoQoS solution
- AutoQoS PCRF: A key component of the AutoQoS solution

For more information, visit Cisco’s website at https://www.cisco.com.
Agenda

• The QoS Paradigm Shift
• Strategic and Tactical QoS Design Case Study
• AutoQoS SRND4
• **NBAR2 QoS Attributes**
• DNS-AS
• Prime Infrastructure AVC/QoS Profiles
• APIC-EM EasyQoS (SDN QoS)
• Looking Forward
• Summary and References
NBAR2 QoS Attributes

IOS 15.5(3)M and IOS XE 3.16S
## NBAR2 Application Library

### Deployment Challenge

- NBAR2 library is very large (~1400 apps)
- While **powerful** this toolset is **not simple** to wield
- To make the library more wieldy, every application has descriptive attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>First level grouping of applications with similar functionalities</td>
</tr>
<tr>
<td>Sub-category</td>
<td>Second level grouping of applications with similar functionalities</td>
</tr>
<tr>
<td>Application-group</td>
<td>Grouping of applications based on brand or application suite</td>
</tr>
<tr>
<td>P2P-technology?</td>
<td>Indicates application is peer-to-peer</td>
</tr>
<tr>
<td>Encrypted?</td>
<td>Indicates application is encrypted</td>
</tr>
<tr>
<td>Tunneled?</td>
<td>Indicates application uses tunneling technique</td>
</tr>
</tbody>
</table>
show ip nbar protocol-attribute skype
# NBAR2 Attributes

## New QoS Attributes: Traffic-Class and Business-Relevance

```
show ip nbar protocol-attribute skype
```

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>encrypted</td>
<td>encrypted-yes</td>
</tr>
<tr>
<td>tunnel</td>
<td>tunnel-no</td>
</tr>
<tr>
<td>category</td>
<td>voice-and-video</td>
</tr>
<tr>
<td>sub-category</td>
<td>consumer-multimedia-messaging</td>
</tr>
<tr>
<td>application-group</td>
<td>skype-group</td>
</tr>
<tr>
<td>p2p-technology</td>
<td>p2p-tech-yes</td>
</tr>
<tr>
<td><strong>traffic-class</strong></td>
<td>voip-telephony</td>
</tr>
<tr>
<td><strong>business-relevance</strong></td>
<td>business-irrelevant</td>
</tr>
</tbody>
</table>

*Cisco Live!*
# NBAR2 Traffic-Class Attribute Options

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>voip-telephony</td>
<td>VoIP telephony (bearer-only) traffic</td>
</tr>
<tr>
<td>broadcast-video</td>
<td>Broadcast TV, live events, video surveillance</td>
</tr>
<tr>
<td>real-time-interactive</td>
<td>High-definition interactive video applications</td>
</tr>
<tr>
<td>multimedia-conferencing</td>
<td>Desktop software multimedia collaboration applications</td>
</tr>
<tr>
<td>multimedia-streaming</td>
<td>Video-on-Demand (VoD) streaming video</td>
</tr>
<tr>
<td>network-control</td>
<td>Network control plane traffic</td>
</tr>
<tr>
<td>signaling</td>
<td>Signaling traffic that supports IP voice and video telephony</td>
</tr>
<tr>
<td>ops-admin-mgmt</td>
<td>Network operations, administration, and management traffic</td>
</tr>
<tr>
<td>transactional-data</td>
<td>Interactive data applications</td>
</tr>
<tr>
<td>bulk-data</td>
<td>Non-interactive data applications</td>
</tr>
</tbody>
</table>
## NBAR2 Business-Relevance Attribute Options

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>business-relevant</td>
<td>Business critical applications</td>
</tr>
<tr>
<td>default</td>
<td>Related business applications</td>
</tr>
<tr>
<td>business-irrelevant</td>
<td>Non business applications</td>
</tr>
</tbody>
</table>
Changing a Business-Relevancy Setting

Step 1: Create an Attribute-Map with the Desired Setting

```
ip nbar attribute-map BUSINESS-RELEVANT attribute business-relevance business-relevant
```

Step 2: Associate the Application with the Desired Attribute-Map

```
ip nbar attribute-set skype BUSINESS-RELEVANT
```
Changing Application Business-Relevance
Protocol Pack 14+ (All Options)

Scenario 1: Making an Application **Business-Relevant**

```
ip nbar attribute-map APIC_EM-ATTRIBUTE_MAP-RELEVANT attribute business-relevance business-relevant
ip nbar attribute-set application-name APIC_EM-ATTRIBUTE_MAP-RELEVANT
```

Scenario 2: Making an Application **Default**

```
ip nbar attribute-map APIC_EM-ATTRIBUTE_MAP-DEFAULT attribute business-relevance default
ip nbar attribute-set application-name APIC_EM-ATTRIBUTE_MAP-DEFAULT
```

Scenario 3: Making an Application **Business-Irrelevant**

```
ip nbar attribute-map APIC_EM-ATTRIBUTE_MAP-SCAVERGER attribute business-relevance business-irrelevant
ip nbar attribute-set application-name APIC_EM-ATTRIBUTE_MAP-SCAVERGER
```
class-map match-all VOICE
  match protocol attribute traffic-class voip-telephony
  match protocol attribute business-relevance business-relevant

class-map match-all BROADCAST-VIDEO
  match protocol attribute traffic-class broadcast-video
  match protocol attribute business-relevance business-relevant

class-map match-all REAL-TIME-INTERACTIVE
  match protocol attribute traffic-class real-time-interactive
  match protocol attribute business-relevance business-relevant

class-map match-all MULTIMEDIA-CONFERENCING
  match protocol attribute traffic-class multimedia-conferencing
  match protocol attribute business-relevance business-relevant

class-map match-all MULTIMEDIA-STREAMING
  match protocol attribute traffic-class multimedia-streaming
  match protocol attribute business-relevance business-relevant

class-map match-all SIGNALING
  match protocol attribute traffic-class signaling
  match protocol attribute business-relevance business-relevant

class-map match-all NETWORK-CONTROL
  match protocol attribute traffic-class network-control
  match protocol attribute business-relevance business-relevant

class-map match-all NETWORK-MANAGEMENT
  match protocol attribute traffic-class ops-admin-mgmt
  match protocol attribute business-relevance business-relevant

class-map match-all TRANSACTIONAL-DATA
  match protocol attribute traffic-class transactional-data
  match protocol attribute business-relevance business-relevant

class-map match-all BULK-DATA
  match protocol attribute traffic-class bulk-data
  match protocol attribute business-relevance business-relevant

policy-map MARKING
  class VOICE
    set dscp ef
  class BROADCAST-VIDEO
    set dscp cs5
  class REAL-TIME-INTERACTIVE
    set dscp cs4
  class MULTIMEDIA-CONFERENCING
    set dscp af41
  class MULTIMEDIA-STREAMING
    set dscp af31
  class SIGNALING
    set dscp cs3
  class NETWORK-CONTROL
    set dscp cs6
  class NETWORK-MANAGEMENT
    set dscp cs2
  class TRANSACTIONAL-DATA
    set dscp af21
  class BULK-DATA
    set dscp af11
  class SCAVENGER
    set dscp cs1
  class class-default
    set dscp default
“The solution to government surveillance is to encrypt everything”

Eric Schmidt
Executive Chairman of Google
What do you do when your DPI reports look like this?

- 25-30% of enterprise apps are encrypted
- And growing…
NBAR2 DNS-Based Custom App

Two Step Solution:
1) DNS sniffing
2) Traffic classification based on DNS information

```bash
ip nbar custom CUSTOM_DNS_CISCO dns domain-name "*.cisco.com"
```

```
class-map CISCO.COM
match protocol CUSTOM_DNS_CISCO
```

---

Tabular representation:

<table>
<thead>
<tr>
<th>Domain</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>cisco.com</td>
<td>77.163.4.161</td>
</tr>
</tbody>
</table>
NBAR2 SSL-Based Custom Application

- NBAR2 now includes a SSL optimized parser
- SSL custom application based on unique-name
  - server-name in client-hello or common-name in certificate

NBAR2 recognizes 140+ encrypted applications
Looking Ahead: Advanced Heuristics

- Decryption is **not required** for classification.
- Classification of known applications can provide a statistical base for comparison and heuristics to classify new encrypted flows.
NBAR2 QoS Attributes At-A-Glance

Cisco NBAR2 Business-Relevance and Traffic-Class Attributes

**Business-Relevance Attribute**

- **Name**: NBAR2 Business-Relevance
- **Description**: This attribute allows an administrator to classify an application to one of three levels of business-relevance, as shown in Table 1.

<table>
<thead>
<tr>
<th>Business-Relevance</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relevant</td>
<td>Business is critical to an organization's operations.</td>
</tr>
<tr>
<td>Maps to LEGACY/REL</td>
<td>Business is important for mission-critical operations.</td>
</tr>
<tr>
<td>Default (NA)</td>
<td>Business is not considered critical.</td>
</tr>
</tbody>
</table>

**Traffic-Class Attribute**

- **Name**: NBAR2 Traffic-Class
- **Description**: This attribute is used to classify traffic based on its business-relevance. It can be used to assign specific QoS attributes to traffic based on its relevance to the business.

For example, in Table 2, theCBR (Class-Based Routing) attribute can be used to prioritize traffic based on its business-relevance. The CBP (Class-Based Priority) attribute can be used to assign different priority levels to different traffic classes. The CBX (Class-Based eXtensive) attribute can be used to assign additional attributes to traffic based on its business-relevance.

**Note**: The CBX attribute is not shown in the table, but it can be used to assign additional attributes to traffic based on its business-relevance.

---

**Step 1**: Configure NBAR2 Business-Relevance and Traffic-Class Class Maps

**Step 2**: Configure Mapping Policy Map

https://cisco.box.com/s/8izevlg4k6gaggh3cmrc16lugu6sdr8y
Agenda

- The QoS Paradigm Shift
- Strategic and Tactical QoS Design Case Study
- AutoQoS SRND4
- NBAR2 QoS Attributes
- **DNS-AS**
  - Prime Infrastructure AVC/QoS Profiles
  - APIC-EM EasyQoS (SDN QoS)
- Looking Forward
- Summary and References
DNS-AS

IOS XE 3.17
DNS-Authoritative Source (DNS-AS)

What Does DNS-AS Provide?

- **Application visibility** end-to-end in the network
- **Light-weight** application detection process
- A scalable means of identifying encrypted & cloud applications
- An efficient means to distribute application metadata
- **No client software** requirement
- **Simplified** end-to-end policy enforcement
DNS-AS Operation

**Internal** Applications

1) Client requests a DNS Lookup
2) Access Switch examines the DNS request
3) Internal DNS Server returns a DNS response (A-Record)
4) Access Switch requests application metadata information by generating *its own* DNS query
5) Internal DNS Server returns application metadata (A-Record + TXT Record)
6) Access Switch maintains a Binding Table of application metadata

<table>
<thead>
<tr>
<th>IP Address</th>
<th>PTR</th>
<th>App-ID</th>
<th>App-Class</th>
<th>Business-Relevance</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.0.7</td>
<td>mail.timco.com</td>
<td>378</td>
<td>Bulk Data</td>
<td>YES</td>
</tr>
</tbody>
</table>
DNS-AS Operation

**External** Applications (with no metadata)

1) Client requests a DNS Lookup
2) Access Switch examines the DNS request
3) External DNS Server returns a DNS response (A-Record)
4) Access Switch requests application metadata information (via a TXT record)
5) External DNS Server has no TXT Record with application metadata
6) Internet Edge router notices the request for a TXT record without response
DNS-AS Operation

**External Applications (with no metadata)**

1) Client requests a DNS Lookup
2) Access Switch examines the DNS request
3) External DNS Server returns a DNS response (A-Record)
4) Access Switch requests application metadata information (via a TXT record)
5) External DNS Server has no TXT Record with application metadata
6) Internet Edge router notices the request for a TXT record without response

**First Flow:**
IE router uses NBAR2 to perform DPI to identify the flow and makes an entry in its local Binding Table
**DNS-AS Operation**

**External Applications (with no metadata)**

1) Client requests a DNS Lookup
2) Access Switch examines the DNS request
3) External DNS Server returns a DNS response (A-Record)
4) Access Switch requests application metadata information (via a TXT record)
5) External DNS Server has no TXT Record with application metadata
6) Internet Edge router notices the request for a TXT record without response
   **First Flow:**
   IE router uses NBAR2 to perform DPI to identify the flow and makes an entry in its local Binding Table
   **Subsequent Flows:**
   IE router responds (as a DNS-Proxy) to the request for application metadata (by inserting a TXT record into the DNS response from the External DNS server)

7) Access Switch maintains a Binding Table of application metadata

<table>
<thead>
<tr>
<th>IP Address</th>
<th>PTR</th>
<th>App-ID</th>
<th>App-Class</th>
<th>Business-Relevance</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.99.120.37</td>
<td>app.cloudco.com</td>
<td>3789</td>
<td>Transactional Data</td>
<td>YES</td>
</tr>
</tbody>
</table>
DNS-AS At-A-Glance

The Role of DNS-AS
An increasing number of applications are being engineered, which limits the effectiveness of deep-packet inspection technologies. Additionally, many applications are multiplexing their media streams, making them increasingly difficult to distinguish and block differently.

Providing application metadata can address both of these challenges and enhance the utility of network QoS, security, performance routing, and other policies.

The challenge then becomes how to distribute such application metadata. For instance, applications running on devices need to communicate such metadata to the network. This would require a phenomenal amount of cross-platform software development and maintenance.

However, DNS is not only a trusted source of information (as it is centrally administered, either by an enterprise or by a service provider), but it is also flexible and extensible. As such, it may be used as an authoritative source of application metadata.

Thus, DNS-AS can provide the following value to enterprise networks:
- accurately identify encrypted applications
- identify thousands of applications (e.g., by leveraging OpenAppID)
- provide a way to network devices that have no deep-packet inspection capabilities
- reduce configuration complexity on network devices for differentiation
- require no software updates to endgpoint devices, applications, or operating systems

Consider two main DNS-AS use-cases:
- identifying internal applications
- identifying external applications

Identifying Internal Applications
As internal DNS servers are centrally administered by the enterprise IT department, these may be modified to include DNS TXT records that reflect application metadata, such as:
- application name
- application ID
- QoS/WAN traffic classification
- Business relevance, etc.

With this application metadata in place in the local DNS server database, then, for example, a network access switch with no deep-packet inspection capabilities can leverage DNS-AS to correctly classify and apply QoS (and other types of policies) to any internal application.

The DNS-AS operational steps to identify external applications are:
1. A client requests a DNS Lookup, as shown in Figure 1.
2. The access switch intercepts and checks the DNS request.
3. The internal DNS Server returns a DNS response (A-Record).
4. The access switch requests application metadata information via a TXT record, as shown in Figure 2.
5. The internal DNS Server returns a TXT Record with application metadata information.
6. The access switch maintains a Binding Table of application metadata.

At this point, the access switch can apply QoS policies or security or routing or other types of policies to the flow.

Identifying External Applications
A few additional steps are required when identifying external applications that have no application metadata in their DNS records. In this model, the Internet edge router plays a key role as a DNS-AS Proxy.

The DNS-AS operational steps to identify external applications are:
1. A client requests a DNS Lookup, as shown in Figure 3.
2. The access switch intercepts and checks the DNS request.
3. The external DNS Server returns a DNS response (A-Record).
4. The access switch requests application metadata information (via a TXT record).
5. The external DNS Server has no TXT Record with application metadata information.
6. The Internet edge router notices the request for a TXT Record without response and:
   a. On the first flow:
      - The Internet edge router uses NBAR2 to perform deep-packet inspection to identify the flow and makes an entry in its local Binding Table.
   b. On subsequent flows:
      - The Internet edge router uses DNS as a DNS-AS Proxy for the request for application metadata (by inserting a TXT Record into the DNS response from the external DNS server).
7. The access switch maintains a Binding Table of application metadata.

Cisco Domain Name System-Authoritative Source (DNS-AS)

https://cisco.box.com/s/8izevlq4k6gaggh3cmrc16lugm6sdr8y
Agenda

- The QoS Paradigm Shift
- Strategic and Tactical QoS Design Case Study
- AutoQoS SRND4
- NBAR2 QoS Attributes
- DNS-AS
- **Prime Infrastructure AVC/QoS Profiles**
- APIC-EM EasyQoS (SDN QoS)
- Looking Forward
- Summary and References
Cisco Prime Infrastructure—AVC/QoS Profiles
Prime Infrastructure AVC/QoS Profiles

Step 1: Classification and Marking Profiles

![Diagram of AVC Profiles]

**QoS Classification Profiles**
- nbar-12-cl (Recommended)
- nbar-5-cl
- nbar-8-cl

**QoS Action Profiles**
- egress-12-a
- egress-5-c
- egress-8-c

**App Visibility Profiles**
<table>
<thead>
<tr>
<th>QoS Class</th>
<th>QoS Action</th>
<th>BW Percentage</th>
<th>Egress DSCP marking</th>
</tr>
</thead>
<tbody>
<tr>
<td>VOICE</td>
<td>Priority Queue</td>
<td>10%</td>
<td>Keep Original</td>
</tr>
<tr>
<td>BROADCAST-VIDEO</td>
<td>Priority Queue</td>
<td>10%</td>
<td>Keep Original</td>
</tr>
<tr>
<td>INTERACTIVE-VIDEO</td>
<td>Priority Queue</td>
<td>13%</td>
<td>Keep Original</td>
</tr>
<tr>
<td>MULTIMEDIA-CONFERENCING</td>
<td>CBWFQ</td>
<td>10%</td>
<td>Keep Original</td>
</tr>
<tr>
<td>MULTIMEDIA-STREAMING</td>
<td>CBWFQ</td>
<td>10%</td>
<td>Keep Original</td>
</tr>
<tr>
<td>SIGNALING</td>
<td>CBWFQ</td>
<td>2%</td>
<td>Keep Original</td>
</tr>
<tr>
<td>NETWORK-CONTROL</td>
<td>CBWFQ</td>
<td>2%</td>
<td>Keep Original</td>
</tr>
<tr>
<td>NETWORK-MANAGEMENT</td>
<td>CBWFQ</td>
<td>3%</td>
<td>Keep Original</td>
</tr>
<tr>
<td>TRANSACTIONAL-DATA</td>
<td>CBWFQ</td>
<td>10%</td>
<td>Keep Original</td>
</tr>
<tr>
<td>BULK-DATA</td>
<td>CBWFQ</td>
<td>4%</td>
<td>Keep Original</td>
</tr>
<tr>
<td>SCAVENGER</td>
<td>CBWFQ</td>
<td>1%</td>
<td>Keep Original</td>
</tr>
<tr>
<td>CLASS-DEFAULT</td>
<td>CBWFQ</td>
<td>25%</td>
<td>Keep Original</td>
</tr>
</tbody>
</table>

In this diagram, we can see the QoS Action Profiles for each QoS class. The table shows the QoS Action, BW Percentage, and Egress DSCP marking for each category.
Cisco Prime Infrastructure—AVC/QoS Profiles At-A-Glance

Step 1) Configure a QoS Classification Profile

Step 2) Select a QoS Action Profile

Step 3) Deploy QoS to the Network Interfaces

https://cisco.box.com/s/8izevlg4k6gaggh3cmrc16lugm6sdr8y
Agenda

• The QoS Paradigm Shift
• Strategic and Tactical QoS Design Case Study
• AutoQoS SRND4
• NBAR2 QoS Attributes
• DNS-AS
• Prime Infrastructure AVC/QoS Profiles
  • **APIC-EM EasyQoS**
• Looking Forward
• Summary and References
APIC-EM EasyQoS
“It takes [us] 4 months and $1M to push a QoS change…
I view the administrator as being a business analyst via a central station without needing to have any understanding of QoS models and low level device attributes”

—Wall Street Financial Customer
“It took us 3 months to deploy a 2 line ACL change across 10K devices, which slowed down onboarding of our Jabber application.”

—Enterprise Network Architect
Why Develop a SDN QoS Solution?

- QoS is application-centric
- QoS is pervasive
- QoS is complex
- SDN presents new QoS capabilities (e.g. dynamic QoS for applications)
Business Value of EasyQoS

- Provides **End-to-End Orchestration** of QoS in the Enterprise Network

- **Simple and easy to deploy** with an operator expressing business relevance for applications and the controller doing the rest “under-the-hood”

- Works for and both **Greenfield** and **Brownfield** deployments

- **Business Intent Driven** while abstracting platform/media/capability details

- **End-to-End provisioning done in minutes** (vs. months) leveraging industry standards and Cisco Validated Designs

- **Reduces time** to onboard new applications and allows SLA compliance
EasyQoS Solution

Applications can interact with APIC-EM via Northbound APIs, informing the network of application-specific and dynamic QoS requirements.

Southbound APIs translate business-intent to platform-specific configurations.

Network Operators express high-level business-intent to APIC-EM EasyQoS.

Applications can interact with APIC-EM via Northbound APIs, informing the network of application-specific and dynamic QoS requirements.

Southbound APIs translate business-intent to platform-specific configurations.

Network Operators express high-level business-intent to APIC-EM EasyQoS.
EasyQoS GUI

Step 1: Select a Scope for Policy Application
EasyQoS GUI

Step 1: Select a Scope for Policy Application
EasyQoS GUI
Step 2: (Optional) Change Application Business-Relevance
EasyQoS GUI

Step 3: (Optional) Add Custom Applications
What Happens “Under-the-Hood”?
Establish Trust Boundaries and Policy Enforcement Points (PEPs)

- The Trust Boundary is the point where Layer 2 or Layer 3 markings are accepted or rejected.
- The Policy Enforcement Point (PEP) is the edge where classification and marking policies are enforced.
  - The PEP may or may not be the same as the trust boundary.
  - Multiple PEPs may exist for different types of network devices.

EasyQoS will deploy:
- Wired and wireless trust boundaries at the network edges.
- Policy Enforcement Points at the network edges as well as at strategic locations (where extended classification technologies may be available).

Guiding Mandate:
Each device will be configured to express the business-intent with maximum fidelity to the best of its capabilities.
EasyQoS seamlessly interconnects all types of hardware and software queuing models to achieve consistent and compatible end-to-end treatments aligned with the expressed business-intent.
Business Value of Dynamic QoS

- No need to open a wide UDP port-range in your trust boundary, making your network more secure
- No Need for DPI at the edge
- Classification becomes application-aware, yet lightweight
- Support wireless & BYOD devices without client software upgrades
- Supports brownfield deployments
EasyQoS GUI

Step 4: (Optional) Enabling Dynamic QoS
Dynamic QoS Workflow
Part 1: Proceeding Voice/Video Call

CUCM signals APIC-EM of a **proceeding** call via a Northbound Rest API
APIC-EM acknowledges the flow and assigns a Flow-ID
APIC-EM deploys dynamic ACLs for voice and/or video
to the specific switch ports hosting the endpoints

**POST /api/v0/fms/flow:**
```
{"srcIPAddress": "10.1.1.1", "dstIPAddress": "10.2.2.2", "srcPort": 31999, "dstPort": 21141, "mediaType": "video", "qosClassName": "conversational.video.avconf.aq", "averageBandwidth": 0, "peakBandwidth": 0, "appid": "CUCM", "codec": "H.264"}
```

**Ip access-list extended VOICE**
```
permit udp host 10.1.1.1 eq 18578 host 10.2.2.2 eq 17333
```

**Ip access-list extended VIDEO**
```
permit udp host 10.1.1.1 eq 31199 host 10.2.2.2 eq 24141
```

**Ip access-list extended VOICE**
```
permit udp host 10.2.2.2 eq 17333 host 10.1.1.1 eq 18578
```

**Ip access-list extended VIDEO**
```
permit udp host 10.2.2.2 eq 24141 host 10.1.1.1 eq 31199
```
Dynamic QoS Workflow
Part 2: Terminating Voice/Video Call

CUCM signals APIC-EM to delete the Flow-ID of a terminating call
APIC-EM removes the dynamic ACLs for voice and/or video
from the specific switch ports hosting the endpoints

DELETE /api/v0/fms/flow/bc8727b7-76d0-4bac-94b9-fa6b76a1a803

```
ip access-list extended VOICE
   no permit udp host 10.1.1.1 eq 18578 host 10.2.2.2 eq 17333
ip access-list extended VIDEO
   no permit udp host 10.1.1.1 eq 31199 host 10.2.2.2 eq 24141
```

```
ip access-list extended VOICE
   no permit udp host 10.2.2.2 eq 17333 host 10.1.1.1 eq 18578
ip access-list extended VIDEO
   no permit udp host 10.2.2.2 eq 24141 host 10.1.1.1 eq 31199
```
EasyQoS Solution Summary

**Solution Summary**

- Cisco® EasyQoS is a simple, highly secure, and scalable automated network QoS policy deployment solution.
- EasyQoS is business-intent driven, requiring network operators only to confirm which applications are relevant to their business, while abstracting all platform-specific implementation details.
- Cisco APIC-EM is the central controller which supports Northbound APIs that can interface with applications (via REST APIs) and also Southbound APIs to translate application requirement to platform-specific configurations.
- EasyQoS deploys industry-standard best practices via Cisco Validated Designs.

**Benefits**

- Provides end-to-end orchestration of QoS
- Simple and easy to deploy
- Works for both greenfield and brownfield deployments
- Business-intent driven
- End-to-End provisioning done in minutes
- Reduces time to onboard new applications and allows SLA compliance
- Provides dynamic, lightweight, and accurate application-aware classification
- Supports wireless & BYOD devices without client software upgrades.
APIC-EM QoS At-A-Glance

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 robust, policy-based manner to maximize performance and efficiency. As such, it is a prime candidate technology to showcase the benefits of SDN. Cisco’s Application Policy Infrastructure Controller (APIC-EM) supports QoS in a robust, policy-based manner.

Capturing Business Intent and Anticipating QoS Strategy
Without a centralized controller, application policies (such as QoS) have to be independently configured on individual network devices and would have to 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 intent of applications. With this information, the controller can then automate and enforce the QoS policies in a consistent manner.

Abstracting Platform-Specific Implementation Details
With a central QoS strategy defined, the controller can then apply Cisco’s Intelligent Design (CID) to automatically translate the policy to device-specific configurations. In the future, this will integrate into a centralized controller where Cisco’s APIC-EM can focus on policy-based decisions and network conditions.

Cisco APIC-EM QoS
Cisco APIC-EM QoS provides a holistic approach to QoS, enabling enterprises to deploy QoS policies across their networks in a consistent and efficient manner. By leveraging Cisco’s APIC-EM, enterprises can ensure optimal network performance and user experience.

Cisco live!
https://cisco.box.com/s/8izevlg4k6gaggh3cmrc16lugm6sdr8y
Agenda

• The QoS Paradigm Shift
• Strategic and Tactical QoS Design Case Study
• AutoQoS SRND4
• NBAR2 QoS Attributes
• DNS-AS
• Prime Infrastructure AVC/QoS Profiles
• APIC-EM EasyQoS (SDN QoS)

• **Looking Forward**

• Summary and References
Looking Forward
“We want our customers to feel like they’re driving a Ferrari”

Mark Montanez
Cisco Distinguished Consulting Engineer
Enterprise Architecture Lead
Closing the Experience Loop

Defining the Experience

Expressing Business Intent

Deploying the Experience

Translating Business-Intent into QoS/QoE policies

Validating the Experience

Quantitatively Correlating the Delivered Experience with the Expressed Business-Intent

Translate Business Intent into QoS/QoE policies.
Validation of Experience

Stage 1: Instrumentation

Collect all relevant metrics for QoE
Validation of Experience

Stage 2: Telemetry

Get the most relevant metrics off the device to a central repository
Validation of Experience

Stage 3: Monitoring

Real-time / Short-term feedback of QoE events
Validation of Experience
Stage 4: Reporting

Long-Term Storage, Retrieval and Representation of QoE Events
Validation of Experience

Stage 5: Analytics

Identify anomalous QoE trends
Analytics Application for APIC-EM
Part 1—Strategic Policy Analysis

Branch Type: Medium-sized  Region: East Coast

Monitoring and Tuning | Scenario Analysis

- Voice
- Broadcast Video
- Realtime Interactive
- Network Control
- OAM
- Signaling
- Multimedia Streaming
- Multimedia Conferencing
- Transactional Data
- Bulk Data
- Scavenger
- Best Effort
Analytics Application for APIC-EM
Part 2—Strategic Policy Recommendations

Suggested Re-configuration:

<table>
<thead>
<tr>
<th>Category</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>10%</td>
</tr>
<tr>
<td>Network Control</td>
<td>2%</td>
</tr>
<tr>
<td>Multimedia Streaming</td>
<td>8%</td>
</tr>
<tr>
<td>Bulk Data</td>
<td>4%</td>
</tr>
<tr>
<td>Broadcast Video</td>
<td>10%</td>
</tr>
<tr>
<td>OAM</td>
<td>3%</td>
</tr>
<tr>
<td>Multimedia Conferencing</td>
<td>10%</td>
</tr>
<tr>
<td>Scavenger</td>
<td>1%</td>
</tr>
<tr>
<td>Realtime Interactive</td>
<td>13%</td>
</tr>
<tr>
<td>Signaling</td>
<td>2%</td>
</tr>
<tr>
<td>Transactional Data</td>
<td>10%</td>
</tr>
<tr>
<td>Best Effort</td>
<td>25%</td>
</tr>
</tbody>
</table>

Traffic Class: Multimedia Conferencing

Branch Type: Medium-sized
Region: East Coast

Fri, 20 Mar 2015 00:00:00 GMT
Multimedia Conferencing Peak Util: 153 Mbps
Validation of Experience

Stage 6: Troubleshooting

Identifying the root cause of anomalies
Validation of Experience
Stage 7: Self-Remediation

Automating the correction of the root cause
What to *you* want to see?

Come tell us—
we’re listening:

- MTE
- WebEx
- Email:
  
  Tim  szigeti@cisco.com
  
  Murali  merragun@cisco.com
“A Ferrari that doesn’t win is not a Ferrari”

Sergio Marchionne
CEO of Fiat Chrysler Automobiles
(Parent Company of Ferrari)
Agenda

• The QoS Paradigm Shift
• Strategic and Tactical QoS Design Case Study
• AutoQoS SRND4
• NBAR2 QoS Attributes
• DNS-AS
• Prime Infrastructure AVC/QoS Profiles
• APIC-EM EasyQoS (SDN QoS)
• Looking Forward

• Summary and References
Summary and References
Session Goals
By the end of this session, you should be able to…

• Apply Cisco’s QoS paradigm shift to meet your business needs
  • Abstract strategic business-intent from tactical platform-specific QoS policies

• Deploy Cisco’s most popular campus feature
  • AutoQoS SRND4

• Configure QoS for 1400+ apps in a 12-class model—within 60 lines of CLI
  • NBAR2 QoS Attributes

• Appreciate a technology that can unambiguously identify thousands of applications on any network device and without any client software—even if these apps are encrypted!
  • DNS-AS

• Understand the inner-workings of Cisco’s platform for SDN QoS
  • APIC-EM QoS
Case-Study Details

Case-Studies from Cisco Press book: End-to-End QoS Network Design (v2)

- CH12 Strategic QoS Design Case Study
- CH17 Campus QoS Design Case Study
  - Catalyst 3750, 4500, 6500
- CH21 WLAN QoS Design Case Study
  - Cisco CT5760 WLC + Catalyst 3650/3850
- CH26 Data Center QoS Design Case Study
  - Cisco Nexus 7000, 5000, 2000, 1000V
- CH30 WAN & Branch QoS Design Case Study
  - Cisco ISR G2, ASR 1000
- CH35 MPLS VPN QoS Design Case Study
  - Cisco ISR, ASR 1000, ASR 9000, CRS-3

Cisco live! https://cisco.box.com/s/8izevlg4k6gaggh3cmrc16lugm6sdr8y
Recommended Reading
End-to-End QoS (v2)

• Release Date: Jan 2014
• Page Count: 1040
• Comprehensive QoS design guidance for PINs and platforms:
  • Campus Catalyst 3750/4500/6500
  • WLAN WLC 5508 / Catalyst 3850 NGWC
  • Data Center Nexus 1000V/2000/5500/7000
  • WAN & Branch Cisco ASR 1000 / ISR G2
  • MPLS VPN Cisco ASR 9000 / CRS-3
  • IPSec VPNs Cisco ISR G2
• ISBN: 1-58714-369-0
Recommended Reading
End-to-End QoS (v2)

Amazon.com Overall Rating: ★★★★★


“AWESOME RESUME OF QoS TECHNOLOGIES”

“I strongly recommend this book to anyone working with Cisco infrastructure.”

“This book is an all-encompassing presentation and tutorial on Cisco Quality of Service (QoS)”

“QoS is intimidating; however, this book is a tremendous resource that will ease your anxiety.”

“This book is kept in my cubicle and is already filled with highlights, notes in the margin, and many dog-eared pages.”

“QOS is often misunderstood, and he explains it very well. The explanations are thorough to help understand each case”

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco 2016 T-Shirt by completing the Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site http://showcase.genie-connect.com/ciscolivemelbourne2016/
- Visit any Cisco Live Internet Station located throughout the venue

T-Shirts can be collected Friday 11 March at Registration

Learn online with Cisco Live!
Visit us online after the conference for full access to session videos and presentations.
www.CiscoLiveAPAC.com
Thank you
Appendix A: QoS Tools Review
QoS Tools Review: Classification & Marking Tools

Classification vs. Marking

- Classification:
  - An action that organizes packets into different traffic types, to which different policies can then be applied
  - Classification of packets can happen without marking

- Marking:
  - Writes a value into the packet header
  - Establishes a trust boundary at the network edge
  - Can be used in other locations in the network and is not always used solely for purposes of classification
QoS Tools Review: Classification & Marking Tools

Classification and Marking Options

- **Classification can be done on:**
  - Layer 1 criteria—such as ingress physical interface
  - Layer 2 criteria—such as IEEE 802.1Q/p CoS
  - Layer 3 criteria—such as IP DSCP
  - Layer 4 criteria—such as TCP/UDP port(s)
  - Layer 7 criteria—such as NBAR application signatures

- **Marking can be done on:**
  - Layer 2 fields—such as IEEE 802.1Q/p CoS
  - Layer “2.5” fields—such as MPLS EXP
  - Layer 3 fields—such as IP DSCP
  - Internal fields—such as QoS Group
802.1p User Priority field also called Class of Service (CoS)

Different types of traffic are assigned different CoS values

CoS 6 and 7 are reserved for network use

- Class-map VOICE
  - match cos 5

- Policy-map MARK-COS
  - class VIDEO
  - set cos 4
QoS Tools Review: Classification & Marking Tools

Layer 3 Marking: IP Type of Service (ToS) Byte

- **IP Precedence (relegated):** Three most significant bits of ToS byte are called IP Precedence (IPP)—other bits unused
- **Differentiated Services:** Six most significant bits of ToS byte are called DiffServ Code Point (DSCP)—remaining two bits used for Explicit Congestion Notification (ECN)
- DSCP and ECN are also used in IPv6
### QoS Tools Review: Classification & Marking Tools

#### Layer 3 Marking: DSCP Per-Hop Behaviors (PHBs)

**Per-Hop Behaviors (PHB)**

- **Expedited Forwarding**
  - RFC 3246
  - DSCP: 101110

- **Assured Forwarding**
  - RFC 2597
  - DSCP: 001000

- **Default Forwarding**
  - (Best Effort)
  - RFC 2474
  - DSCP: 000000

#### DiffServ Code Points (DSCP)

<table>
<thead>
<tr>
<th>Value</th>
<th>0</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>001010</td>
<td>10</td>
<td>001100</td>
</tr>
<tr>
<td>001110</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>010001</td>
<td>18</td>
<td></td>
</tr>
<tr>
<td>001010</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>010100</td>
<td>22</td>
<td></td>
</tr>
<tr>
<td>011010</td>
<td>26</td>
<td></td>
</tr>
<tr>
<td>011110</td>
<td>28</td>
<td></td>
</tr>
<tr>
<td>011010</td>
<td>30</td>
<td></td>
</tr>
<tr>
<td>010010</td>
<td>32</td>
<td></td>
</tr>
<tr>
<td>001010</td>
<td>34</td>
<td></td>
</tr>
<tr>
<td>010100</td>
<td>36</td>
<td></td>
</tr>
<tr>
<td>011110</td>
<td>38</td>
<td></td>
</tr>
<tr>
<td>100010</td>
<td>40</td>
<td></td>
</tr>
<tr>
<td>100100</td>
<td>42</td>
<td></td>
</tr>
<tr>
<td>100110</td>
<td>44</td>
<td></td>
</tr>
</tbody>
</table>

**DSCP (Class-Map VOICE)**

- match dscp ef

**DSCP (Class-Map VIDEO)**

- set dscp af41

---

*Cisco Live!*
QoS Tools Review: Classification & Marking Tools
Layer 2.5 Marking: MPLS Experimental (EXP) Bits

Frame Encapsulation

MPLS Shim Header

Label Stack
Label Header
Label Header
Payload

Label
Stack

EXP S

TTL

S=Bottom of Stack bit

MPLS EXP

MPLS Experimental bits

class-map VOICE
match mpls experimental 5

policy-map SET-MPLS-EXP
class VIDEO
set mpls experimental imposition 4
<or>
set mpls experimental topmost 4
QoS Tools Review: Classification & Marking Tools
Layer 7 Classification: Network Based Application Recognition (NBAR/NBAR2)

- Identifies over 1000 applications and protocols
- Application payload deep packet inspection
- Supports application media-sub-component classification

class-map CISCO-JABBER-VOICE
  match protocol cisco-jabber-audio

class-map CISCO-JABBER-VIDEO
  match protocol cisco-jabber-video

class-map CISCO-JABBER-MESSAGING
  match protocol cisco-jabber-im

class-map CISCO-JABBER-SIGNALING
  match protocol cisco-jabber-control
QoS Tools Review: Policing & Shaping Tools

Policers vs. Shapers

- Policers:
  - perform checks for traffic violations against a configured rate and take immediate prescribed actions (such as remarking or dropping)
  - policers do not delay traffic
  - policers may be applied to the data plane or the control plane

- Shapers:
  - smooth out traffic flows so that it never exceeds the configured rate
  - if the offered traffic momentarily spikes above the contracted rate, the excess traffic is buffered and delayed until the offered traffic once again dips below the defined rate
  - shapers usually are employed to meet a Service Level Agreement (SLA)
QoS Tools Review: Policing & Shaping Tools
RFC 2697 Single-Rate Three-Color Marker

Packet of Size B

- CIR
- CBS

B<Tc

Conform

Yes

Conform

Action

Policy-map RFC2697-POLICER
class CLASS-1
  police cir 500000 bc 10000 be 10000
  conform-action set-dscp-transmit af31
  exceed-action set-dscp-transmit af32
  violate-action set-dscp-transmit af33
QoS Tools Review: Policing & Shaping Tools
RFC 2698 Two-Rate Three-Color Marker

Packet of Size B

B>Tp

PIR

PBS

Yes

No

Violate

Action

policy-map RFC2698-POLICER
class CLASS-2
  police cir 500000 bc 10000 pir 100000 be 10000
  conform-action set-dscp-transmit af31
  exceed-action set-dscp-transmit af32
  violate-action set-dscp-transmit af33
QoS Tools Review: Policing & Shaping Tools

Shaping Effect on Traffic Patterns

Traffic Shaping Limits the Transmit Rate to a Value Lower Than Line Rate

```
policy-map CLASS-BASED-SHAPER
  class class-default
    shape average 10 Mbps
  <or>
    shape peak 10 Mbps
```
QoS Tools Review: Queuing & Dropping Tools

If the Tx-Ring is filled to capacity, then the IOS software knows that the interface is congested and it should activate any LLQ/CBWFQ policies that have been applied to the interface.
QoS Tools Review: Queuing & Dropping Tools
(Flow-Based) Fair-Queuing

A flow is defined by five matching tuples:
Source Address + Source Port
Destination Address + Destination Port
Layer 4 Protocol (TCP or UDP)
QoS Tools Review: Queuing & Dropping Tools

CBWFQ

Packets In

- Multimedia Conferencing CBWFQ
- Multimedia Streaming CBWFQ
- Call Signaling CBWFQ
- Network Control CBWFQ
- OAM CBWFQ
- Transactional Data CBWFQ
- Bulk Data CBWFQ
- Best Effort / Default CBWFQ
- Scavenger CBWFQ

Packets Out

policy-map CBWFQ
  class NETWORK-CONTROL bandwidth percent 5
  class SIGNALING bandwidth percent 5
  class OAM bandwidth percent 5
  class MM-CONFERENCING bandwidth percent 10 fair-queue

IOS Interface Buffers

CBWFQ Scheduler

Tx-Ring
QoS Tools Review: Queuing & Dropping Tools

LLQ: Single-LLQ Operation and Configuration

- Packets In
- QoS Tools
- CBWFQs
- CBWFQ Scheduler
- FQ Pre-Sorters
- 1 Mbps VOICE Policer
- policy-map LLQ class VOICE 
  priority 1000
- Packets Out
QoS Tools Review: Queuing & Dropping Tools

LLQ: Multi-LLQ Operation and Configuration

*Policy-map MULTI-LLQ*
- class VOICE
  *priority* 1000
- class BROADCAST-VIDEO
  *priority* 4000
- class REALTIME-INTERACTIVE
  *priority* 5000

**CBWFQ Scheduler**

**Tx-Ring**

**CBWFQs**

**LQ**
QoS Tools Review: Queuing & Dropping Tools
The Need for Congestion Avoidance

- all TCP flows synchronize in waves
- TCP synchronization wastes available bandwidth
QoS Tools Review: Queuing & Dropping Tools

DSCP-Based WRED

Maximum WRED Thresholds for AF11, AF12 and AF13 are set to the tail of the queue in this example.

- **AF13 Minimum WRED Threshold:** Begin randomly dropping **AF13** Packets
- **AF12 Minimum WRED Threshold:** Begin randomly dropping **AF12** Packets
- **AF11 Minimum WRED Threshold:** Begin randomly dropping **AF11** Packets

```
policy-map BULK-WRED
class BULK
  bandwidth percent 10
  random-detect dscp-based
```