Taming the wild wild west of applications in your network using Cisco DNAC QoS Policies

Gurudatt Pai
Technical Leader
CCIE#28227
BRKRST-3685
Questions?
Use Cisco Webex Teams (formerly Cisco Spark) to chat with the speaker after the session

How
1. Open the Cisco Events Mobile App
2. Find your desired session in the “Session Scheduler”
3. Click “Join the Discussion”
4. Install Webex Teams or go directly to the team space
5. Enter messages/questions in the team space
Introduction: Gurudatt pai

Undergrad : Computer Science Engineering
• Introduction
• Cisco’s QoS Strategy
• Application Classification Rules
• Tactical QoS Design
• WAN and Branch QoS
• MPLS VPN QoS
• LAN QoS
• WLAN QoS
• Policy Overview
• Customisations and Operations
• Policy interop with SDA
• Demo – Application Policy Live!
• Cisco DNA Application Assurance
• What’s Next
• Summary
Introduction
Challenge for Enterprise IT - Doing more with Less

An evolved world needs a network evolved.

Data growth
Connected devices
Threat surface areas

$60B
Spent of
Network Operations

3x more
Organisations intend to be digital-ready within 2 years

Resources

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public
Quality of Experience Challenges

Are your employees productive?

Are your customer getting a good experience?

Are your leaders able to communicate effectively?
Complexity in deploying consistent QoS policies
Lowering Operational Costs

• “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
The Need for a New Network

Constantly Learning
Support 100X new devices, apps, users

Constantly Adapting
Respond Instantly to business demands with limited staff and budget

Constantly Protecting
See and predict issues and threats and respond fast
The Network. Intuitive LEARNING

Cisco DNA Center
- Policy
- Automation
- Analytics

Informed by Context
Visibility into traffic and threat patterns
- Who, What, When, Where, How

Powered by Intent
Translate Business Intent to Network Policy
Automate the management and provisioning millions of devices instantly

Intent-based Network Infrastructure

SECURITY

INTENT

CONTEXT

LEARNING
Cisco DNA Automation with Cisco Validated Designs
Bridging the Gap to Increased Success in Network Deployment and Use

Any given “custom” configuration has a very high probability of not being tested exactly as deployed “individually—as a one off…” which introduces potential issues...

The automated configuration deployed by the controller will have gone through...

- Joint development by the Cisco Product Teams, the Architects developing Best Practices, and the Controller Team—“Blessed Configurations”
- Testing by Cisco’s Solution, System, and Devtest teams against the deployment use cases developed jointly, above
- And will be deployed by 1000’s, with any unforeseen situations addressed ASAP due to widespread and standardised deployment

Automation
Controller-Led Networking Deployment

Greatly increased probability of success
Cisco’s QoS Strategy
Objective: Closing the Application Experience Loop

Defining the Intent
Expressing Business-Level Intent

Validating the Outcome
Cisco DNA Assurance & Analytics
Quantitatively Correlating the Delivered Outcome with the Expressed Business-Intent

Delivering the Intent
Cisco DNA Automation
Translating Business Intent into Network Policies and Transport
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 (QoE) for video applications
- Improving user productivity by minimising network response times
- Managing business applications that are “bandwidth hogs”
- Identifying and de-prioritising 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)
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 marked 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
Application Classification Rules
**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 Behaviour</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, CS5 (Optional) PQ</td>
<td>Cisco IP Video Surveillance / Cisco Enterprise TV</td>
<td></td>
</tr>
<tr>
<td>Real-Time Interactive</td>
<td>CS4, CS4 (Optional) PQ</td>
<td>Cisco TelePresence</td>
<td></td>
</tr>
<tr>
<td>Multimedia Conferencing</td>
<td>AF4, AF4 BW Queue + DSCP WRED</td>
<td>Cisco Jabber, Cisco WebEx</td>
<td></td>
</tr>
<tr>
<td>Multimedia Streaming</td>
<td>AF3, 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</td>
<td>Default Queue + RED</td>
<td></td>
</tr>
</tbody>
</table>

- **Relevant**
- **Default**
- **Irrelevant**

Apply RFC 4594-based Marking / Queuing / Dropping Treatments
## What Do We Do Under-the-Hood?

Apply RFC 4594-based Marking / Queuing / Dropping Treatments

### Table

<table>
<thead>
<tr>
<th>Application Class</th>
<th>Per-Hop Behaviour</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 TelePresence</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>
Tactical QoS Design
Converting Business Intent into Tactical Policies

The principle goal of the tactical QoS policy is to express the strategic QoS policy with maximum fidelity.

- QoS design best practices will be used to generate platform-specific configurations.
- QoS features will be selectively enabled if they directly contribute to expressing the strategic policy on a given platform.

- Cisco DNA Center
  - Policy Automation
  - Analytics

- Catalyst 9300
  - Trust Boundary
  - PEP
  - 4Q (WMM)

- Catalyst 4500
  - 1P7Q1T

- Catalyst 6500
  - 1PQ4T
  - 1P7Q4T
  - 2P6Q4T

- Nexus 7700
  - F3: 1P7Q1T

- Wireless AP
  - Trust Boundary
  - PEP
  - 4Q (WMM)

- WLC
  - PEP

- ASR/ISRs
  - MQC

- Wireless AP
  - Trust Boundary
  - PEP
  - 4Q (WMM)

- Catalyst 2960-X
  - Trust Boundary
  - PEP
  - 1P3Q3T

The principle goal of the tactical QoS policy is to express the strategic QoS policy with maximum fidelity.

- QoS design best practices will be used to generate platform-specific configurations.
- QoS features will be selectively enabled if they directly contribute to expressing the strategic policy on a given platform.
Deploy End-to-End DSCP-Based Queuing Policies

Application Policy **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.

Cisco DNA Center

- Policy Automation
- Analytics

Cisco DNA Center Analytics Policy Automation

BRKRST-3685 © 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public 25
WAN & Branch QoS
WAN & Branch QoS

- Router LAN–Edge Policy–Enforcement Point
- Queuing Policies

Cisco DNA Center

Policy Automation
Analytics

Wireless AP
Trust Boundary
PEP
4Q (WMM)

Catalyst 2K/3K/9K
Trust Boundary
PEP
1P3Q3T

Catalyst 4500
1P7Q1T

Nexus 7700
F3: 1P7Q1T

WLC
PEP

ASR/ISRs
MQC

Catalyst 4500
1P7Q4T
1P7Q4T
2P6Q4T
...

Catalyst 6500
1P3Q4T

Catalyst 3850
Trust Boundary
PEP
2P6Q3T

Wireless AP
Trust Boundary
PEP
4Q (WMM)
WAN & Branch QoS: Protocol Pack 14+ LAN-Edge PEP
NBAR2 Application Library
Deployment Challenge

• NBAR2 library is very large (~1400 apps)
• While powerful this toolset is not simple to wield
NBAR2 Attributes
New QoS Attributes: Traffic-Class and Business-Relevance

show ip nbar protocol-attribute skype
# CLMEL

## NBAR2 Attributes

New QoS Attributes: Traffic-Class and Business-Relevance

<table>
<thead>
<tr>
<th>show ip nbar protocol-attribute skype</th>
<th></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>traffic-class</td>
<td>multimedia-conferencing</td>
</tr>
<tr>
<td>business-relevance</td>
<td>business-irrelevant</td>
</tr>
</tbody>
</table>
NBAR2 QoS Attributes
Changing Business-Relevancy

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

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

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**

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

Scenario 2: Making an Application **Default**

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

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

```plaintext
ip nbar attribute-map DNAC-ATTRIBUTE_MAP-SCAVENGED
  attribute business-relevance business-irrelevant
ip nbar attribute-set application-name DNAC-ATTRIBUTE_MAP-SCAVENGED
```
Holy Grail QoS Configuration: NBAR2 1400+ App / 12-Class Model

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-CONFERENCEING
  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

class-map match-all SCAVENGER
  match protocol attribute business-relevance business-irrelevant

policy-map MARKING
  class VOICE
    set dscp ef
  class BROADCAST-VIDEO
    set dscp cs5
  class REAL-TIME-INTERACTIVE
    set dscp cs4
  class MULTIMEDIA-CONFERENCEING
    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
WAN & Branch QoS: WAN-Edge Queuing
Application Policy Default

WAN BW Model

- Best Effort: 25%
- Voice: 10%
- Broadcast Video: 10%
- Real-Time Interactive: 13%
- Multimedia Conferencing: 10%
- Multimedia Streaming: 10%
- Network Control: 3%
- OAM: 2%
- Signaling: 2%
- Transactional Data: 10%
- Bulk Data: 4%
- Scavenger: 1%
Default Queuing Profile – Bandwidth Values

Ability to customize the bandwidth allocation for various traffic classes.

Configuration Snippet:

```
policy-map prm-dscp#QUEUING_OUT
  class prm-EZQOS_12C#VOICE
    police rate percent 10
    priority
  class prm-EZQOS_12C#BROADCAST
    police rate percent 10
    priority
  class prm-EZQOS_12C#REALTIME
    police rate percent 13
    priority
  class prm-EZQOS_12C#MM_CONF
    bandwidth remaining percent 15
    fair-queue
    random-detect dscp-based
  class prm-EZQOS_12C#MM_STREAM
    bandwidth remaining percent 15
    fair-queue
    random-detect dscp-based
  class prm-EZQOS_12C#CONTROL
    bandwidth remaining percent 4
  class prm-EZQOS_12C#SIGNALING
    bandwidth remaining percent 3
  class prm-EZQOS_12C#OAM
    bandwidth remaining percent 3
  class prm-EZQOS_12C#TRANS_DATA
    bandwidth remaining percent 15
    fair-queue
    random-detect dscp-based
  class prm-EZQOS_12C#BULK_DATA
    bandwidth remaining percent 6
    fair-queue
    random-detect dscp-based
  class prm-EZQOS_12C#SCAVENGER
    bandwidth remaining percent 1
  class class-default
    bandwidth remaining percent 38
    fair-queue
    random-detect dscp-based
```
Default Queuing Profile – DSCP Values

Ability to customize the DSCP value for each of the various traffic-classes.
MPLS VPN QoS
MPLS VPN QoS

- Router LAN–Edge Policy–Enforcement Point
- Sub-Line–Rate Shaping (as needed)
- Enterprise–to–SP Mapping (as needed)
- Queuing Policies

Catalyst 2k/3k/9k Trust Boundary PEP 1P3Q3T

Catalyst 4500 1P7Q1T

Nexus 7700 F3: 1P7Q1T

WLC PEP

ASR/ISRs MQC

MPLS VPN

Cisco DNA Center

Policy Automation Analytics

Wireless AP

Trust Boundary

PEP 4Q (WMM)

Catalyst 3850 Trust Boundary PEP 2P6Q3T

Wireless AP

Trust Boundary

PEP 4Q (WMM)

Catalyst 3k/9k Trust Boundary PEP 1P3Q4T 1P7Q4T 2P6Q4T

…

• Router LAN–Edge Policy–Enforcement Point
• Sub-Line–Rate Shaping (as needed)
• Enterprise–to–SP Mapping (as needed)
• Queuing Policies

Cisco live!

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public
High Level Workflow

**Step 1** Design
Create SP Profiles

**Policy**
Identify WAN interfaces on each Border Router

**Step 2**

**Policy**
Specify sub-line rate for each WAN interface

**Step 3**

**Policy**
Specify the SP profile for each WAN interface

**Step 4**

**Policy**
Customise SP Profile if needed (Optional)
# Create SP Profile

![Cisco DNA Center screenshot](image)

- **Network Hierarchy**: Find Hierarchy
  - Global
    - NYC
    - PDX
    - SJC
    - SP
    - USA

- **Network Settings**: SP Profiles
  - **QoS**
    - Profile Name: Demo-SP-Profile
    - WAN Provider: Demo-WAN-Provider
    - Model:
      - 4 Class
      - 5 Class
      - 6 Class
      - 8 Class

---

---
Assign SP Profile to WAN Interface

Router → WAN Interface → SP Profile → Upstream Bandwidth
What Changes for QoS on Sub-Line-Rate Interfaces?

Queuing policies *will not* engage unless the interface is congested

- A shaper will guarantee that traffic will not exceed the contracted rate
- A nested queuing policy will force queuing to engage at the contracted sub-line-rate to prioritise packets prior to shaping

### Queuing Policies

- **REALTIME**
  - Priority: 1000

- **SIGNALING**
  - Bandwidth: $x$

- **TRANSACTIONAL**
  - Bandwidth: $y$

### Service Shaper

- Default Queue
  - 1 Mbps

- **CBWFQ Scheduler**
  - Signaling
  - Transactional

### Traffic Shaping

- Class-based shaper

### GE Interface

- With a sub-line-rate access service (e.g., 50 Mbps)
SP Profile HQoS Policy

HQoS Parent Shaping policy (with nested queuing policy) is applied to the sub-line-rate interface

```plaintext
interface GigabitEthernet0/0/1
  ip address 10.1.3.2 255.255.255.248
  negotiation auto
  service-policy input prm-MARKING_IN
  service-policy output prm-dscp#EQ_Demo-SPProfile2#shape#200.0

policy-map prm-dscp#EQ_Demo-SP-Profile2
  class prm-EZQOS_12C#VOICE
    police rate percent 10
    priority
    set dscp ef
  class prm-EZQOS_12C#BROADCAST
    bandwidth remaining percent 10
    set dscp af31
  class prm-EZQOS_12C#REALTIME
    bandwidth remaining percent 14
    set dscp af31
  class prm-EZQOS_12C#MM_CONF
    bandwidth remaining percent 10
    fair-queue
    set dscp af31
    random-detect dscp-based
  class prm-EZQOS_12C#MM_STREAM
    bandwidth remaining percent 10
    fair-queue
    set dscp af31
    random-detect dscp-based
  class prm-EZQOS_12C#CONTROL
    bandwidth remaining percent 3
    set dscp default
```

```plaintext
policy-map prm-dscp#EQ_Demo-SP-Profile2
  class class-default
    shape average 200000000
    service-policy prm-dscp#EQ_Demo-SP-Profile2
```

Cisco Live! #CLMEL
MPLS VPN QoS: 4-Class Service Provider Model
## 4 Class Service Provider Profile

### Service Provider Profiles

<table>
<thead>
<tr>
<th>Class Name</th>
<th>DSCP</th>
<th>SP Bandwidth %</th>
<th>Queuing Bandwidth %</th>
<th>Admitted Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice(Priority)</td>
<td>46 (EF)</td>
<td>10 %</td>
<td>10 %</td>
<td>voip_telephony</td>
</tr>
<tr>
<td>CLASS1 DATA</td>
<td>26 (AF31)</td>
<td>44 %</td>
<td>14 %</td>
<td>multimedia_conferencing</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>real_time_interactive</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>multimedia_streaming</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>broadcast_video</td>
</tr>
<tr>
<td>CLASS2 DATA</td>
<td>18 (AF21)</td>
<td>25 %</td>
<td>3 %</td>
<td>signaling</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>14 %</td>
<td>transactional_data</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 %</td>
<td>ops_admin_mgmt</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5 %</td>
<td>bulk_data</td>
</tr>
<tr>
<td>Default</td>
<td>0 (Best Effort)</td>
<td>31 %</td>
<td>1 %</td>
<td>scavenger</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 %</td>
<td>network_control</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>27 %</td>
<td>best_effort</td>
</tr>
</tbody>
</table>

### Bandwidth % usage

- Priority(10%)+100%
- Priority(10%)+100%

---

**Ability to customise the DSCP values, SP Bandwidth% and Queuing BW for each class**
Application Policy Marking Mappings into 4-Class SPP

<table>
<thead>
<tr>
<th>Application</th>
<th>DSCP</th>
<th>CS6 Sent Unchanged</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internetwork Control</td>
<td>CS6</td>
<td></td>
</tr>
<tr>
<td>VoIP</td>
<td>EF</td>
<td></td>
</tr>
<tr>
<td>Broadcast Video</td>
<td>CS5 → AF31</td>
<td></td>
</tr>
<tr>
<td>Multimedia Conferencing</td>
<td>AF41 → AF31</td>
<td></td>
</tr>
<tr>
<td>Real-Time Interactive</td>
<td>CS4 → AF31</td>
<td></td>
</tr>
<tr>
<td>Multimedia Streaming</td>
<td>AF31</td>
<td></td>
</tr>
<tr>
<td>Signalling</td>
<td>CS3 → AF21</td>
<td></td>
</tr>
<tr>
<td>Transactional Data</td>
<td>AF21</td>
<td></td>
</tr>
<tr>
<td>Network Management</td>
<td>CS2 → AF21</td>
<td></td>
</tr>
<tr>
<td>Bulk Data</td>
<td>AF11 → AF21</td>
<td></td>
</tr>
<tr>
<td>Scavenger</td>
<td>CS1</td>
<td></td>
</tr>
<tr>
<td>Best Effort</td>
<td>DF</td>
<td></td>
</tr>
</tbody>
</table>

SPP1 (4-Class Model)

- SP-VOICE
  - PQ-10% BW
- SP-CLASS1DATA
  - (UDP)
  - 44% BWR
- SP-CLASS2DATA
  - (TCP)
  - 25% BWR
- SP-DEFAULT
  - 31% BWR

BWR = Bandwidth Remaining
MPLS VPN QoS:
5-Class Service Provider Model
## 5 Class Service Provider Profile

### Service Provider Profiles

<table>
<thead>
<tr>
<th>Class Name</th>
<th>DSCP</th>
<th>SP Bandwidth %</th>
<th>Queuing Bandwidth %</th>
<th>Admitted Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice(Priority)</td>
<td>46 (EF)</td>
<td>10 %</td>
<td>10 %</td>
<td>voip_telephony</td>
</tr>
<tr>
<td>CLASS1 DATA</td>
<td>26 (AF31)</td>
<td>44 %</td>
<td>10 %</td>
<td>broadcast_video</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>multimedia_conferencing</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>real_time_interactive</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>multimedia_streaming</td>
</tr>
<tr>
<td>CLASS2 DATA</td>
<td>18 (AF21)</td>
<td>25 %</td>
<td>3 %</td>
<td>signaling</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>14 %</td>
<td>transactional_data</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 %</td>
<td>ops_admin_mgmt</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5 %</td>
<td>bulk_data</td>
</tr>
<tr>
<td>CLASS3 DATA</td>
<td>10 (AF11)</td>
<td>1 %</td>
<td>1 %</td>
<td>scavenger</td>
</tr>
<tr>
<td>Default</td>
<td>0 (Best Effort)</td>
<td>30 %</td>
<td>3 %</td>
<td>network_control</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>27 %</td>
<td>best_effort</td>
</tr>
</tbody>
</table>

**Bandwidth % usage**: Priority(10%) + 100%
Application Policy Marking Mappings into 5-Class SPP

<table>
<thead>
<tr>
<th>Application</th>
<th>DSCP</th>
<th>SPP2 (5-Class Model)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internetwork Control</td>
<td>CS6</td>
<td>EF</td>
</tr>
<tr>
<td>VoIP</td>
<td>EF</td>
<td>SP-VOICE PQ=10% BW</td>
</tr>
<tr>
<td>Broadcast Video</td>
<td>CS5 → AF31</td>
<td>AF31</td>
</tr>
<tr>
<td>Multimedia Conferencing</td>
<td>CS4 → AF31</td>
<td>SF-CLASS1DATA (UDP) 44% BWR</td>
</tr>
<tr>
<td>Real-Time Interactive</td>
<td>AF31</td>
<td>AF31</td>
</tr>
<tr>
<td>Multimedia Streaming</td>
<td>CS3 → AF21</td>
<td>AF21</td>
</tr>
<tr>
<td>Signalling</td>
<td>AF21</td>
<td>AF21</td>
</tr>
<tr>
<td>Transactional Data</td>
<td>CS2 → AF21</td>
<td>AF11</td>
</tr>
<tr>
<td>Network Management</td>
<td>AF11 → AF21</td>
<td>AF11</td>
</tr>
<tr>
<td>Bulk Data</td>
<td>CS1 → AF11</td>
<td>CS1</td>
</tr>
<tr>
<td>Scavenger</td>
<td>DF</td>
<td>DF</td>
</tr>
<tr>
<td>Best Effort</td>
<td>DF</td>
<td>DF</td>
</tr>
</tbody>
</table>

AF31 → SF-CLASS2DATA (TCP) 25% BWR

Egress: CS6 Sent Unchanged

DSCP

AF11 → SF-CLASS3DATA–1% BWR

AF21

AF31

EF

SP-VOICE PQ=10% BW

SP-CLASS1DATA (UDP) 44% BWR

SP-CLASS2DATA (TCP) 25% BWR

SP-CLASS3DATA–1% BWR

SP-DEFAULT 30% BWR

BRKRST-3685 © 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public
MPLS VPN QoS: 6-Class Service Provider Model
6 Class Service Provider Profile

### Service Provider Profiles

<table>
<thead>
<tr>
<th>Class Name</th>
<th>DSCP</th>
<th>SP Bandwidth %</th>
<th>Queuing Bandwidth %</th>
<th>Admitted Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice (Priority)</td>
<td>46 (EF)</td>
<td>10 %</td>
<td>10 %</td>
<td>voip_telephony</td>
</tr>
<tr>
<td>CLASS1 DATA</td>
<td>26 (AF31)</td>
<td>10 %</td>
<td>10 %</td>
<td>multimedia_streaming</td>
</tr>
<tr>
<td>CLASS2 DATA</td>
<td>18 (AF21)</td>
<td>25 %</td>
<td>3 %</td>
<td>signaling</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>14 %</td>
<td>transactional_data</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 %</td>
<td>ops_admin_mgmt</td>
</tr>
<tr>
<td>CLASS3 DATA</td>
<td>10 (AF11)</td>
<td>1 %</td>
<td>5 %</td>
<td>bulk_data</td>
</tr>
<tr>
<td>Video</td>
<td>34 (AF41)</td>
<td>34 %</td>
<td>14 %</td>
<td>scavenger</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>10 %</td>
<td>real_time_interactive</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>10 %</td>
<td>broadcast_video</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>multimedia_conferencing</td>
</tr>
<tr>
<td>Default</td>
<td>0 (Best Effort)</td>
<td>30 %</td>
<td>3 %</td>
<td>network_control</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>27 %</td>
<td>best_effort</td>
</tr>
</tbody>
</table>

**Bandwidth % usage**: Priority(10%) + 100%

- Ability to customise the DSCP values, SP Bandwidth% and Queuing BW for each class.
Application Policy Marking Mappings into 6-Class SPP

<table>
<thead>
<tr>
<th>Application</th>
<th>DSCP</th>
<th>SPP3 (6-Class Model)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internetwork Control</td>
<td>CS6</td>
<td>EF</td>
</tr>
<tr>
<td>VoIP</td>
<td>EF</td>
<td>SP-VOICE PQ=10% BWR</td>
</tr>
<tr>
<td>Broadcast Video</td>
<td>CS5→AF41</td>
<td>AF41</td>
</tr>
<tr>
<td>Multimedia Conferencing</td>
<td>AF41</td>
<td>SP-VIDEO 34% BWR</td>
</tr>
<tr>
<td>Real-Time Interactive</td>
<td>CS4→AF41</td>
<td>AF31</td>
</tr>
<tr>
<td>Multimedia Streaming</td>
<td>AF31</td>
<td>SP-CLASS1DATA (UDP) 10% BWR</td>
</tr>
<tr>
<td>Signaling</td>
<td>CS3→AF21</td>
<td>AF21</td>
</tr>
<tr>
<td>Transactional Data</td>
<td>AF21</td>
<td>SP-CLASS2DATA (TCP) 25% BWR</td>
</tr>
<tr>
<td>Network Management</td>
<td>CS2→AF21</td>
<td>AF11</td>
</tr>
<tr>
<td>Bulk Data</td>
<td>AF11→AF21</td>
<td>AF11</td>
</tr>
<tr>
<td>Scavenger</td>
<td>CS1→AF11</td>
<td>AF11</td>
</tr>
<tr>
<td>Best Effort</td>
<td>DF</td>
<td>SP-DEFAULT 30% BWR</td>
</tr>
</tbody>
</table>

CS6 Sent Unchanged

Network Management
- Real-Time Interactive
- Multimedia Streaming
- Multimedia Conferencing

VoIP
- Internetwork Control

Broadcast Video
- Signaling

Transactional Data
- Bulk Data

Best Effort
- Scavenger

Application Policy Marking Mappings into 6-Class SPP

#CLMEL
MPLS VPN QoS: 8-Class Service Provider Model
### Service Provider Profiles

<table>
<thead>
<tr>
<th>Class Name</th>
<th>DSCP</th>
<th>SP Bandwidth %</th>
<th>Queuing Bandwidth %</th>
<th>Admitted Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>VOICE(Priority)</td>
<td>46 (EF)</td>
<td>10 %</td>
<td>10 %</td>
<td>voip_telephony</td>
</tr>
<tr>
<td>CALL-SIGNALING</td>
<td>24 (CS3)</td>
<td>4 %</td>
<td>4 %</td>
<td>signaling</td>
</tr>
<tr>
<td>CRITICAL-DATA</td>
<td>18 (AF21)</td>
<td>25 %</td>
<td>16 %</td>
<td>transactional_data</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ops_admin_mgmt</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>bulk_data</td>
</tr>
<tr>
<td>INTERACTIVE-VIDEO</td>
<td>34 (AF41)</td>
<td>30 %</td>
<td>17 %</td>
<td>real_time_interactive</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>multimedia_conferencing</td>
</tr>
<tr>
<td>NET CTRL-MGMT</td>
<td>48 (CS6)</td>
<td>5 %</td>
<td>5 %</td>
<td>network_control</td>
</tr>
<tr>
<td>SCAVENGER</td>
<td>8 (CS1)</td>
<td>1 %</td>
<td>1 %</td>
<td>scavenger</td>
</tr>
<tr>
<td>STREAMING-VIDEO</td>
<td>26 (AF31)</td>
<td>10 %</td>
<td>5 %</td>
<td>broadcast_video</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>multimedia_streaming</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>0 (Best Effort)</td>
<td>25 %</td>
<td>25 %</td>
<td>best_effort</td>
</tr>
</tbody>
</table>

**Bandwidth % usage**

- Priority(10%) + 100%
- Priority(10%) + 100%

---

**Ability to customise the DSCP values, SP Bandwidth% and Queuing BW for each class.**
## Application Policy Marking Mappings into 8-Class SPP

### Application Policy Marking Mappings

<table>
<thead>
<tr>
<th>Application</th>
<th>DSCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internetwork Control</td>
<td>CS6</td>
</tr>
<tr>
<td>VolP</td>
<td>EF</td>
</tr>
<tr>
<td>Broadcast Video</td>
<td>CS5 → AF31</td>
</tr>
<tr>
<td>Multimedia Conferencing</td>
<td>AF41</td>
</tr>
<tr>
<td>Real-Time Interactive</td>
<td>CS4 → AF41</td>
</tr>
<tr>
<td>Multimedia Streaming</td>
<td>AF31</td>
</tr>
<tr>
<td>Signaling</td>
<td>CS3</td>
</tr>
<tr>
<td>Transactional Data</td>
<td>AF21</td>
</tr>
<tr>
<td>Network Management</td>
<td>CS2 → AF21</td>
</tr>
<tr>
<td>Bulk Data</td>
<td>AF11 → AF21</td>
</tr>
<tr>
<td>Scavenger</td>
<td>CS1</td>
</tr>
<tr>
<td>Best Effort</td>
<td>DF</td>
</tr>
</tbody>
</table>

### SPP4 (8-Class Model)

- **EF**: SP-VOICE PQ-10% BWR
- **CS6**: SP-NET-CTRL-MGMT 5% BWR
- **AF41**: SP-INTERACTIVE-VIDEO 30% BWR
- **AF31**: SP-STREAMING-VIDEO 10% BWR
- **CS3**: SP-CALL-SIGNALING 4% BWR
- **AF21**: SP-CRITICAL-DATA 25% BWR
- **CS1**: SP-SCAVENGER-1% BWR
- **DF**: SP-DEFAULT 25% BWR

**Legend**:
- Green: Best Effort
- Red: Critical Data
- Blue: Video
- Yellow: Scavenger
- Orange: Critical
- Gray: Default
- White: Other
MPLS VPN QoS: DSCP-Marking Restoration
NBAR-Based Marking/Remarking Policies

Cisco DNA Center

Wireless AP
Trust Boundary
PEP
4Q (WMM)

Catalyst 4500
1P7Q1T

Catalyst 6500
1P3Q4T
1P7Q4T
2P6Q4T
...

Nexus 7700
F3: 1P7Q1T

ASR/ISRs
MQC

Wireless AP
Trust Boundary
PEP
4Q (WMM)

Catalyst 2k/3k/9k
Trust Boundary
PEP
1P3Q3T

Catalyst 3850
Trust Boundary
PEP
2P6Q3T

NBAR LAN-Edge (Ingress) Marking Policy

NBAR WAN-Edge (Ingress) Re-Marking (Restoration) Policy
SP-WAN Remarkering (Restoration) Configuration

LAN Edges

interface GigabitEthernet0/0/2
ip address 10.5.1.1 255.255.255.0
service-policy input prm-MARKING_IN
service-policy output prm-dscp#QUEUING_OUT

WAN Edges with SP Profiles

interface GigabitEthernet0/0/1
ip address 10.1.3.2 255.255.255.248
service-policy input prm-MARKING_IN
service-policy output prm-dscp#EQ_Demo-SP-Profile2#shape#200.0

Same NBAR marking config are used to restore DSCP markings on INGRESS from SP-WAN
LAN QoS
LAN QoS

- LAN access-edge trust boundaries
- LAN Policy-Enforcement Points (PEPs)
- Queuing Policies

LAN QoS components include:

- Catalyst 3650
  - Trust Boundary PEP
  - 1P7Q1T
- Catalyst 4500
  - 1P7Q1T
- Nexus 7700
  - 4Q (WMM)
  - F3: 1P7Q1T
- Catalyst 6500
  - 1P3Q4T
  - 1P7Q4T
  - 2P6Q4T
  - ...
- WLC
- Cisco DNA Center
  - Policy Automation
  - Analytics
- ASR/ISRs
  - PEP
  - MQC LLQ/CBWFQ

Additional components:

- Catalyst 2960-X
  - Trust Boundary PEP
  - 1P3Q3T
- Catalyst 2650
  - Trust Boundary PEP
  - 2P6Q3T
- Cisco DNA Center
  - LAN access-edge trust boundaries
  - LAN Policy-Enforcement Points (PEPs)
  - Queuing Policies
LAN QoS Design: Trust Boundaries and Policy Enforcement Points
Cisco Campus Switches Default Trust States

- Catalyst 2960x series switches
  - MLS QoS Default trust state: untrusted (with QoS enabled)
- Catalyst 3650/3850/9300/9400/9500 series switches
  - MQC Default trust state: trusted
- Catalyst 4500 series switches
  - MQC Default trust state: trusted
- Catalyst 6500/6800 series switches
  - C3PL default trust state: trusted
- Nexus 7000/7700 series switches
  - NX-OS default trust state: trusted
How Can Apps Be Classified at Campus LAN PEPs?

NBAR2 Protocol Library

Downloading NBAR2 Protocol Packs
NBAR Protocol Packs are available for download on the Cisco.com software download page, here:
http://www.cisco.com/cisco/software/nbar.html

On the download page, specify a platform model to display software available for download. One software for:
Protocol Packs.

Example:
To display protocol packs available for the Cisco ASR 1001 platform, open the link provided above and navigate:
Products > Routers > Service Provider Edge Routers > ASR 1000 Series Aggregation Services Routers > ASR

NBAR2 Protocol Packs for Cisco IOS and IOS-XE Releases

<table>
<thead>
<tr>
<th>Protocol Pack</th>
<th>Supported Releases</th>
<th>Supported From...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol Pack 35.0.0</td>
<td>Releases supported by Protocol Pack upgrade: IOS-XE Denali 16.3.2</td>
<td>2019-01-02</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2018-01-02</td>
</tr>
<tr>
<td>Protocol Pack 34.0.0</td>
<td>Releases supported by Protocol Pack upgrade: IOS-XE Denali 16.3.2</td>
<td>2017-11-15</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2017-11-15</td>
</tr>
<tr>
<td>Protocol Pack 33.0.0</td>
<td>Built into: IOS-XE Denali 16.6.2</td>
<td>2017-11-05</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2017-11-05</td>
</tr>
<tr>
<td>Protocol Pack 32.1.0</td>
<td>Releases supported by Protocol Pack upgrade: IOS-XE Denali 16.3.2</td>
<td>2017-09-26</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2017-09-26</td>
</tr>
<tr>
<td>Protocol Pack 32.0.0</td>
<td>Releases supported by Protocol Pack upgrade: IOS-XE Denali 16.3.2</td>
<td>2017-08-10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2017-08-10</td>
</tr>
</tbody>
</table>

Global ID: L4:1604
ID: 1433

Known Mappings
UDP Port: 1604, 2512, 2513
TCP Port: 1494, 1604, 2512, 2513, 2598
IP Protocol: -
IP Version: IPv4
IPv6 Support: Yes
IPv6 Support: Yes
Application Group: other
Business Relevance: business-relevant. From Cisco IOS-XE 3.165 and IOS-XE 3.5(3)M only.


Google Search: NBAR Protocol Pack


#CLMEL
How are Apps be Classified in the Campus LAN?

<protocol>
<attributes>
<application-group>other</application-group>
<business-relevance>business-relevant</business-relevance>
<category>business-and-productivity-tools</category>
<encrypted>false</encrypted>
<p2p-technology>false</p2p-technology>
<traffi-class>multimedia-streaming</traffic-class>
<tunnel>false</tunnel>
</attributes>
<common-name>Citrix Static</common-name>
<enabled>true</enabled>
<engine-id>3</engine-id>
<global-id>L4:1604</global-id>
<help-string>Citrix Static</help-string>
{id>1433</id>
<ipv4>true</ipv4>
<ipv6>true</ipv6>
</ip-version>
<long-description>Citrix is an application that mediates users remotely to their corporate applications. ICA: Independed Computing Architecture is a designated protocol for application server system; it is used for transferring data between clients and servers…

Note: Application Policy maintains an ACE Count by App e.g. citrix-static: 6 ACEs (TCAMs)
Switch LAN-Edge PEP Policy Workflow

Start Deployment

TCAMs Available for QoS?

Have All Custom Apps Been Processed?

Deploy ACE(s) For Next L4-App From Custom Apps

Note: Per-Platform TCAM Limits for QoS Pre-Programmed into Application Policy + Confirmed before Deployment

Note: Remaining Apps to be Pre-Sorted by:
1) Popularity Attribute
2) Alphabetically

ID App as L4-App + Construct ACE(s)

TCAMs Available for QoS?

Have All Favorite Apps Been Processed?

Is the App Voice or Video?

Any (More) TCP or UDP Ports?

TCP Port 80, 443, 8080, etc.?

ID App as L4-App + Construct ACE(s)

Redistribute remaining TCAMs Across Traffic-Classes and Process Each Traffic Class

Continue to Next App

Have All Remaining Apps Been Processed?

Is the App Voice or Video?

Any (More) TCP or UDP Ports?

TCP Port 80, 443, 8080, etc.?

ID App as L4-App + Construct ACE(s)

Have All Remaining Apps Been Processed?

Continue to Next App

TCAMs Available for Traffic-Class?

Have All Remaining Apps Been Processed?

Is the App Voice or Video?

Any (More) TCP or UDP Ports?

TCP Port 80, 443, 8080, etc.?

ID App as L4-App + Construct ACE(s)

Stop

Note: “Video” in this context includes: realtime-interactive, broadcast-video, multimedia-conferencing traffic-classes.
## Catalyst Switch Access-Layer PEP - Static Endpoint ACLs

<table>
<thead>
<tr>
<th>Wired Endpoint Device Type</th>
<th>Allowed DSCP Value</th>
<th>Traffic Class for ACE Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IP Phone</td>
<td>EF</td>
<td>VOIP</td>
</tr>
<tr>
<td></td>
<td>AF41</td>
<td>MULTIMEDIA CONFERENCING</td>
</tr>
<tr>
<td>Cisco Video Conferencing Endpoint</td>
<td>EF</td>
<td>VOIP</td>
</tr>
<tr>
<td></td>
<td>AF41</td>
<td>MULTIMEDIA CONFERENCING</td>
</tr>
<tr>
<td>Cisco Telepresence Device</td>
<td>CS4</td>
<td>REALTIME INTERACTIVE</td>
</tr>
<tr>
<td></td>
<td>EF</td>
<td>VOIP</td>
</tr>
<tr>
<td>Cisco Video Surveillance Camera</td>
<td>CS5</td>
<td>BROADCAST VIDEO</td>
</tr>
</tbody>
</table>
Catalyst Switch Access-Layer PEP ACL Example

! ip access-list extended prm-APIC_QOS_IN#VOICE__acl
   permit ip host 10.4.81.21 any DSCP ef
!
! ip access-list extended prm-APIC_QOS_IN#MM-CONF__acl
   permit ip host 10.4.81.21 any DSCP af41
!
! ip access-list extended prm-APIC_QOS_IN#MM_STREAM__acl
   remark citrix - Citrix
   permit tcp any eq 1494
   permit udp any eq 1494
   permit tcp any eq 2598
   permit udp any eq 2598
   remark citrix-static - Citrix-Static
   permit tcp any eq 1604
   permit udp any eq 1604
   permit tcp any range 2512 2513
   permit udp any any range 2512 2513
</snip>
exit

ip access-list extended prm-APIC_QOS_IN#SIGNAGING__acl
   remark h323 - H.323
   permit tcp any eq 1300
   permit udp any any eq 1300
   permit tcp any eq 1718 1720
   permit udp any eq 1718 1720
   permit tcp any eq 11720
   permit udp any eq 11720
   remark mgcp - Media Gateway Control Protocol
   permit tcp any range 2427 2428

! ip access-list extended prm-APIC_QOS_IN#TUNNELED__acl
   remark CAPWAP Control Traffic
   permit udp any eq 5246
   remark CAPWAP Data Traffic
   permit udp any eq 5247
exit
LAN QoS Design: LAN Queuing
**Catalyst 2960-X / 3560-X / 3750-X**

1P3Q3T Egress Queuing Model

<table>
<thead>
<tr>
<th>Application</th>
<th>DSCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Control</td>
<td>(CS7)</td>
</tr>
<tr>
<td>Internetwork Control</td>
<td>CS6</td>
</tr>
<tr>
<td>VoIP</td>
<td>EF</td>
</tr>
<tr>
<td>Broadcast Video</td>
<td>CS5</td>
</tr>
<tr>
<td>Multimedia Conferencing</td>
<td>AF4</td>
</tr>
<tr>
<td>Realtime Interactive</td>
<td>CS4</td>
</tr>
<tr>
<td>Multimedia Streaming</td>
<td>AF3</td>
</tr>
<tr>
<td>Signaling</td>
<td>CS3</td>
</tr>
<tr>
<td>Transactional Data</td>
<td>AF2</td>
</tr>
<tr>
<td>Bulk Data</td>
<td>CS2</td>
</tr>
<tr>
<td>Scavenger</td>
<td>CS1</td>
</tr>
<tr>
<td>Best Effort</td>
<td>DF</td>
</tr>
</tbody>
</table>

**1P3Q3T**

- **Queue 4** (5%)
  - AF1
  - CS1
- **Default Queue**
  - DF
  - CS7
  - CS6
  - CS3
  - CS5
  - CS2
- **Queue 3** (35%)
  - AF4
  - AF3
  - AF2
  - CS2
- **Queue 2** (30%)
  - EF
  - CS5
  - CS4
  - Q1

- **Priority Queue**
Catalyst 2960-X
1P3Q3T Egress Queuing—Part 1

! This section configures egress buffers and thresholds
mls qos queue-set output 1 buffers 15 30 35 20
mls qos queue-set output 1 threshold 1 100 100 100 100
mls qos queue-set output 1 threshold 2 80 90 100 400
mls qos queue-set output 1 threshold 3 100 100 100 400
mls qos queue-set output 1 threshold 4 60 80 100 400

! This section configures egress CoS-to-Queue mappings
mls qos srr-queue output cos-map queue 1 threshold 3 4 5
mls qos srr-queue output cos-map queue 2 threshold 1 2
mls qos srr-queue output cos-map queue 2 threshold 2 3
mls qos srr-queue output cos-map queue 2 threshold 3 6 7
mls qos srr-queue output cos-map queue 4 threshold 3 1
This section configures egress DSCP-to-Queue mappings

```plaintext
mls qos srr-queue output dscp-map queue 1 threshold 3 32 40 44 46
mls qos srr-queue output dscp-map queue 2 threshold 1 16 18 20 22
mls qos srr-queue output dscp-map queue 2 threshold 1 26 28 30 34 36 38
mls qos srr-queue output dscp-map queue 2 threshold 2 24
mls qos srr-queue output dscp-map queue 2 threshold 3 48 56
mls qos srr-queue output dscp-map queue 3 threshold 3 0 1 2 3 4 5 6 7
mls qos srr-queue output dscp-map queue 3 threshold 3 9 11 13 15
mls qos srr-queue output dscp-map queue 3 threshold 3 17 19 21 23
mls qos srr-queue output dscp-map queue 3 threshold 3 25 27 29 31
mls qos srr-queue output dscp-map queue 3 threshold 3 33 35 37 39
mls qos srr-queue output dscp-map queue 3 threshold 3 41 42 43 44 45 47
mls qos srr-queue output dscp-map queue 3 threshold 3 49 50 51 52 53 54 55
mls qos srr-queue output dscp-map queue 3 threshold 3 57 58 59 60 61 62 63
mls qos srr-queue output dscp-map queue 4 threshold 1 8 14
mls qos srr-queue output dscp-map queue 4 threshold 2 12
mls qos srr-queue output dscp-map queue 4 threshold 3 10
```
This section configures interface parameters for **ACCESS INTERFACES** (10/100/1000)

```plaintext
no mls qos trust
queue-set 1
srr-queue bandwidth share 1 30 35 5
priority-queue out
```

This section configures interface parameters for **UPLINK INTERFACES** (10/100/1000)

```plaintext
mls qos trust
queue-set 1
srr-queue bandwidth share 1 30 35 5
priority-queue out
```
Catalyst 3650/3850/9300/9500
2P6Q3T with Weighted Tail Drop (WTD) Egress Queuing Model

<table>
<thead>
<tr>
<th>Application</th>
<th>DSCP</th>
<th>2P6Q3T</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Control</td>
<td>(CS7)</td>
<td>EF PQ Level 1 (10%)</td>
</tr>
<tr>
<td>Internetwork Control</td>
<td>CS6</td>
<td>CS5 PQ Level 2 (20%)</td>
</tr>
<tr>
<td>VoIP</td>
<td>EF</td>
<td>CS4</td>
</tr>
<tr>
<td>Broadcast Video</td>
<td>CS5</td>
<td>CS7 &amp; CS6 (BWR 10%)</td>
</tr>
<tr>
<td>Multimedia Conferencing</td>
<td>AF4</td>
<td>CS3 &amp; CS2 (BWR 10% + WTD)</td>
</tr>
<tr>
<td>Realtime Interactive</td>
<td>CS4</td>
<td>Q6 (BWR 10%)</td>
</tr>
<tr>
<td>Multimedia Streaming</td>
<td>AF3</td>
<td>EF (BWR 10% + DSCP-Based WTD)</td>
</tr>
<tr>
<td>Signaling</td>
<td>CS3</td>
<td>AF4 Q5 (BWR 10% + WTD)</td>
</tr>
<tr>
<td>Transactional Data</td>
<td>AF2</td>
<td>AF3 (BWR 10% + DSCP-Based WTD)</td>
</tr>
<tr>
<td>Network Management</td>
<td>CS2</td>
<td>AF2 Q4 (BWR 10% + DSCP-Based WTD)</td>
</tr>
<tr>
<td>Bulk Data</td>
<td>AF1</td>
<td>AF1 Q3 (BWR 10% + DSCP-Based WTD)</td>
</tr>
<tr>
<td>Scavenger</td>
<td>CS1</td>
<td>AF1 Q3 (BWR 10% + DSCP-Based WTD)</td>
</tr>
<tr>
<td>Best Effort</td>
<td>DF</td>
<td>DF Q2 (BWR 5% + DSCP-Based WTD)</td>
</tr>
</tbody>
</table>

BWR = Bandwidth Remaining
WTD = Weighted Tail Drop

Network Management
- Internetwork Control
- VoIP
- Broadcast Video
- Multimedia Conferencing
- Realtime Interactive
- Multimedia Streaming
- Signaling
- Transactional Data
- Network Management
- Bulk Data
- Scavenger
- Best Effort

Application DSCP 2P6Q3T
- Network Control (CS7) EF PQ Level 1 (10%)
- Internetwork Control CS6 CS5 PQ Level 2 (20%)
- VoIP EF CS4
- Broadcast Video CS5 CS7 & CS6 (BWR 10%)
- Multimedia Conferencing AF4 CS3 & CS2 (BWR 10% + WTD)
- Realtime Interactive CS4 Q6 (BWR 10%)
- Multimedia Streaming AF3 EF (BWR 10% + DSCP-Based WTD)
- Signaling CS3 AF4 Q5 (BWR 10% + WTD)
- Transactional Data AF2 AF3 (BWR 10% + DSCP-Based WTD)
- Network Management CS2 AF2 Q4 (BWR 10% + DSCP-Based WTD)
- Bulk Data AF1 AF1 Q3 (BWR 10% + DSCP-Based WTD)
- Scavenger CS1 AF1 Q3 (BWR 10% + DSCP-Based WTD)
- Best Effort DF DF Q2 (BWR 5% + DSCP-Based WTD)
Catalyst 3850 / 3650 / 9300/ 9500 Egress Queueing

2P6Q3T Queuing

class-map match-any APIC_EM-VOICE-PQ1
  match dscp ef
class-map match-any APIC_EM-VIDEO-PQ2
  match dscp cs4
  match dscp af41
  match dscp af42
  match dscp af43
  match dscp cs5
class-map match-any APIC_EM-CONTROL-QUEUE
  match dscp cs2
  match dscp cs3
  match dscp cs6
  match dscp cs7
class-map match-any APIC_EM-MM_STREAM-QUEUE
  match dscp af31
  match dscp af32
  match dscp af33
class-map match-any APIC_EM-TRANS_DATA-QUEUE
  match dscp af21
  match dscp af22
  match dscp af23
class-map match-any APIC_EM-BULK_DATA-QUEUE
  match dscp af11
  match dscp af12
  match dscp af13
class-map match-any APIC_EM-SCAVENGER-QUEUE
  match dscp cs1
Cisco DNA Center 1.2.8 Queuing policy Changes

- As per CVD recommendations, queuing policy maps were adjusted for 3650/3850/CAT9K

- The changes:
  - DCSP values AF41/AF42/AF43 (Multimedia Conferencing) should be removed from VIDEO-PQ2 and moved to a new dedicated non-priority queue
  - Scavenger & Bulk Data traffic should unite to a single queue (BULK_DATA queue).
  - Maximum bandwidth of 33% should be allocated to PQ traffic (rather than 43%)
  - Priority & police should be enforced on PQs
  - Transactional Data, the new Bulk Data + Scavenger and Class-default queues should have WRED enabled on the CAT9K platform

- Upon upgrading to DNA Center release 1.2.8:
  - All wired application policies will be marked as stale.
  - User is advised to redeploy the stale policies to update the devices with the recommended CVD.
Example CLIs for CAT9K

class-map match-any DNA-EQQOS_2P6Q3T_9K#BULK-DATA
  match dscp cs1
  match dscp af12
  match dscp af13
  match dscp af11

class-map match-any DNA-EQQOS_2P6Q3T_9K#CONTROL-PLANE
  match dscp cs3
  match dscp cs2
  match dscp cs7
  match dscp cs6

class-map match-any DNA-EQQOS_2P6Q3T_9K#MULTIMEDIA-CONFERENCING
  match dscp af43
  match dscp af41
  match dscp af42

class-map match-any DNA-EQQOS_2P6Q3T_9K#VIDEO-PQ2
  match dscp cs5
  match dscp cs4

class-map match-any DNA-EQQOS_2P6Q3T_9K#VOICE-PQ1
  match dscp ef

class-map match-any DNA-EQQOS_2P6Q3T_9K#TRANSACTIONAL-DATA
  match dscp af23
  match dscp af21
  match dscp af22

class-map match-any DNA-EQQOS_2P6Q3T_9K#MULTIMEDIA-STREAMING
  match dscp af32
  match dscp af33
  match dscp af31

policy-map DNA-dscp#APIC_QOS_Q_OUT
  class DNA-EQQOS_2P6Q3T_9K#VOICE-PQ1
    priority level 1
    police rate percent 10
    queue-buffers ratio 5
  class DNA-EQQOS_2P6Q3T_9K#VIDEO-PQ2
    priority level 2
    police rate percent 23
    queue-buffers ratio 5

\[ \sum = 33\% \]

class DNA-EQQOS_2P6Q3T_9K#CONTROL-PLANE
  bandwidth remaining percent 10
  queue-buffers ratio 5

class DNA-EQQOS_2P6Q3T_9K#MULTIMEDIA-CONFERENCING
  bandwidth remaining percent 15
  queue-buffers ratio 10
  queue-limit dscp af41 percent 100
  queue-limit dscp af42 percent 90
  queue-limit dscp af43 percent 80

class DNA-EQQOS_2P6Q3T_9K#MULTIMEDIA-STREAMING
  bandwidth remaining percent 15
  queue-buffers ratio 10
  queue-limit dscp af32 percent 90
  queue-limit dscp af33 percent 80

class DNA-EQQOS_2P6Q3T_9K#TRANSACTIONAL-DATA
  bandwidth remaining percent 15
  queue-buffers ratio 10
  random-detect dscp-based
  random-detect dscp 18 percent 80 100
  random-detect dscp 20 percent 70 100
  random-detect dscp 22 percent 60 100

class DNA-EQQOS_2P6Q3T_9K#BULK-DATA
  bandwidth remaining percent 7
  queue-buffers ratio 10
  random-detect dscp-based
  random-detect dscp 8 percent 60 100
  random-detect dscp 10 percent 80 100
  random-detect dscp 12 percent 70 100
  random-detect dscp 14 percent 60 100

class class-default
  bandwidth remaining percent 38
  queue-buffers ratio 25
  random-detect dscp-based
  random-detect dscp 0 percent 80 100

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

DSCP based WRED
NBAR based Classification for Catalyst 9k switches

• Before this feature was introduced, upon application policy deployment on Catalyst 9300, 9400 & 9500 (but not 9500H) series platforms:
  • IP/Port (ACL) based policy was pushed on the devices.

• Starting from DNAC 1.2.8, upon application policy deployment on Catalyst 9300 & 9400 & 9400 series platform NBAR based policy will be pushed on the device when the following requirements are met:
  • Switch is running Cisco IOS-XE 16.9.1 or higher
  • Switch is in the Access role
  • The switch has Advanced licensing installed
  • Cisco Encrypted Traffic Analytics (ETA) is not configured on the switch

Otherwise, IP/Port based policy will be pushed on the device.
NBAR on switch Configuration example:

**NBAR Based**

```
class-map match-any DNA-MARKING_IN_TUNNELED-NBAR
  class-map match-any DNA-MARKING_IN_VOICE_CUSTOM
  class-map match-any DNA-MARKING_IN_BROADCAST_CUSTOM
  class-map match-any DNA-MARKING_IN_REALTIME_CUSTOM
  class-map match-any DNA-MARKING_IN_CONF
  class-map match-any DNA-MARKING_IN_M珩_STREAM_CUSTOM
  class-map match-any DNA-MARKING_IN_CONTROL_CUSTOM
  class-map match-any DNA-MARKING_IN_SIGNALINGCUSTOM
  class-map match-any DNA-MARKING_IN_OAM_CUSTOM
  match access-group name DNA-MARKING_IN_OAM_CUSTOM_acl
  class-map match-any DNA-MARKING_IN_TRANSDATA_CUSTOM
  match protocol attribute traffic-class voip-telephony
  match protocol attribute business-relevance business-relevant
  class-map match-all DNA-MARKING_IN_REALTIME
  match protocol attribute traffic-class real-time-interactive
  match protocol attribute business-relevance business-relevant
  class-map match-all DNA-MARKING_IN_CONF
  match protocol attribute traffic-class multimedia-conferencing
  match protocol attribute business-relevance business-relevant
  class-map match-all DNA-MARKING_IN_M珩
  match protocol attribute traffic-class multimedia-streaming
  match protocol attribute business-relevance business-relevant
  class-map match-all DNA-MARKING_IN_CONTROL
  match protocol attribute traffic-class network-control
  match protocol attribute business-relevance business-relevant
  class-map match-all DNA-MARKING_IN_SIGNALING
  match protocol attribute traffic-class signaling
  match protocol attribute business-relevance business-relevant
  class-map match-all DNA-MARKING_IN_OAM
  match protocol attribute traffic-class cpe-admin-vmgmt
  match protocol attribute business-relevance business-relevant
  class-map match-all DNA-MARKING_IN_TRANSDATA
  match protocol attribute traffic-class transactional-data
  match protocol attribute business-relevance business-relevant
  class-map match-all DNA-MARKING_IN_BULK_DATA
  match protocol attribute traffic-class bulk-data
  match protocol attribute business-relevance business-relevant
  class-map match-all DNA-MARKING_IN_SCAVENGER
  match protocol attribute business-relevance business-irrelevant
```

**ACL Based**

```
class-map match-any DNA-APIC_QOS_IN#VOICE
  class-map match-any DNA-APIC_QOS_IN#BROADCAST
  match access-group name DNA-APIC_QOS_IN#BROADCAST_acl
  class-map match-any DNA-APIC_QOS_IN#REALTIME
  class-map match-any DNA-APIC_QOS_IN#CONF
  match access-group name DNA-APIC_QOS_IN#CONF_acl
  class-map match-any DNA-APIC_QOS_IN#M珩
  match access-group name DNA-APIC_QOS_IN#M珩 STREAM_acl
  class-map match-any DNA-APIC_QOS_IN#M珩 STREAM
  match access-group name DNA-APIC_QOS_IN#M珩 STREAM_acl
class-map match-any DNA-APIC_QOS_IN#SIGNALING
  match access-group name DNA-APIC_QOS_IN#SIGNALING_ACL
  class-map match-any DNA-APIC_QOS_IN#OAM
  match access-group name DNA-APIC_QOS_IN#OAM acl
  class-map match-any DNA-APIC_QOS_IN#TRANSDATA
  match access-group name DNA-APIC_QOS_IN#TRANSDATA acl
  class-map match-any DNA-APIC_QOS_IN#BULK_DATA
  match access-group name DNA-APIC_QOS_IN#BULK_DATA acl
  class-map match-any DNA-APIC_QOS_IN#SCAVENGER
  match access-group name DNA-APIC_QOS_IN#SCAVENGER_acl
  class-map match-any DNA-APIC_QOS_IN#TUNNELED
  match access-group name DNA-APIC_QOS_IN#TUNNELED_acl
```

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
WLAN QoS
WLAN QoS

- WLAN access-edge trust boundaries
- WLAN Policy-Enforcement Points (PEPs)
- WMM Policies

Cisco DNA Center

Policy Automation

Analytics

WLAN access
- edge trust boundaries

WLAN Policy
- Enforcement Points (PEPs)

WMM Policies
AireOS QoS Policy Deployment

List of Steps

1) Disable Radios and WLANs
2) Tune EDCA and CAC
3) Tune QoS Profile
4) Create AVC Profile
5) Attach QoS and AVC Profiles to WLAN and Enable AVC
6) Configure Downstream DSCP-to-UP Mapping and Enable Upstream DSCP-Trust
7) Re-enable WLANs and radios
AireOS QoS Policy Deployment

Step 1) Disable Radios and WLANs

(Cisco Controller) > config 802.11a disable network
(Cisco Controller) > config 802.11b disable network
! Must disable 802.11a/b networks to make changes to QoS

(Cisco Controller) > config wlan disable all
! Must disable all WLANs to make changes to QoS
AireOS QoS Policy Deployment

Step 2) Tune EDCA and CAC

(Cisco Controller) > config 802.11a Qos Mode 7
(Cisco Controller) > config 802.11b Qos Mode 7
! Apply FL EDCA profile (best of current EDCA profiles) for 802.11a/b

(Cisco Controller) > config 802.11a cac voice acm enable
(Cisco Controller) > config 802.11b cac voice acm enable
! Enable ACM for 802.11a/b

(Cisco Controller) > config 802.11a cac voice max-bandwidth 50
(Cisco Controller) > config 802.11b cac voice max-bandwidth 50
! Limit voice traffic to 50% of total bandwidth for 802.11a/b

(Cisco Controller) > config 802.11a cac voice roam-bandwidth 6
(Cisco Controller) > config 802.11b cac voice roam-bandwidth 6
! Keep 6% bandwidth for roaming users for 802.11a/b

(Cisco Controller) > config 802.11a exp-bwreq enable
(Cisco Controller) > config 802.11b exp-bwreq enable
! Enable Expedited Bandwidth for 802.11a/b
AireOS QoS Policy Deployment

Step 3) Tune Platinum QoS Profile

(Cisco Controller) > config qos priority platinum voice besteffort besteffort
! Set QoS Profile to Platinum
! Set default marking to unmarked unicast and multicast traffic to best effort

(Cisco Controller) > config qos protocol-type platinum none
! Disables 802.1p marking (all wired marking is DSCP-based)

(Cisco Controller) > config qos burst-realtime-rate platinum per-ssid downstream 0
! Do not restrict profile bandwidth for UDP traffic

(Cisco Controller) > config qos average-realtime-rate platinum per-ssid downstream 0
! Do not restrict profile bandwidth for TCP traffic
### AireOS QoS Policy Deployment

**Step 4) Create an AVC Profile—Example (Part 1 of 2)**

<table>
<thead>
<tr>
<th>(Cisco WLC) &gt; config avc profile AVC-STATIC-PROFILE create</th>
</tr>
</thead>
<tbody>
<tr>
<td>! Creates the AVC Profile</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(Cisco WLC) &gt; config avc profile AVC-STATIC-PROFILE rule add application cisco-phone-audio mark 46</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Cisco WLC) &gt; config avc profile AVC-STATIC-PROFILE rule add application cisco-jabber-audio mark 46</td>
</tr>
<tr>
<td>(Cisco WLC) &gt; config avc profile AVC-STATIC-PROFILE rule add application ms-lync-audio mark 46</td>
</tr>
<tr>
<td>(Cisco WLC) &gt; config avc profile AVC-STATIC-PROFILE rule add application citrix-audio mark 46</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(Cisco WLC) &gt; config avc profile AVC-STATIC-PROFILE rule add application cisco-phone-video mark 34</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Cisco WLC) &gt; config avc profile AVC-STATIC-PROFILE rule add application cisco-jabber-video mark 34</td>
</tr>
<tr>
<td>(Cisco WLC) &gt; config avc profile AVC-STATIC-PROFILE rule add application ms-lync-video mark 34</td>
</tr>
<tr>
<td>(Cisco WLC) &gt; config avc profile AVC-STATIC-PROFILE rule add application webex-media mark 34</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(Cisco WLC) &gt; config avc profile AVC-STATIC-PROFILE rule add application citrix mark 26</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Cisco WLC) &gt; config avc profile AVC-STATIC-PROFILE rule add application pcoip mark 26</td>
</tr>
<tr>
<td>(Cisco WLC) &gt; config avc profile AVC-STATIC-PROFILE rule add application vnc mark 26</td>
</tr>
<tr>
<td>(Cisco WLC) &gt; config avc profile AVC-STATIC-PROFILE rule add application vnc-http mark 26</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(Cisco WLC) &gt; config avc profile AVC-STATIC-PROFILE rule add application skinny mark 24</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Cisco WLC) &gt; config avc profile AVC-STATIC-PROFILE rule add application cisco-jabber-control mark 24</td>
</tr>
<tr>
<td>(Cisco WLC) &gt; config avc profile AVC-STATIC-PROFILE rule add application sip mark 24</td>
</tr>
<tr>
<td>(Cisco WLC) &gt; config avc profile AVC-STATIC-PROFILE rule add application sip-tls mark 24</td>
</tr>
</tbody>
</table>
#CLMEL

AireOS QoS Policy Deployment

Step 4) Create an AVC Profile—Example (Part 2 of 2)

! This section configures AVC to mark Transactional Data applications to AF21 (DSCP 18)
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application cisco-jabber-im mark 18
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application ms-office-web-apps mark 18
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application salesforce mark 18
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application sap mark 18

! This section configures AVC to mark OAM applications to CS2 (DSCP 16)
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application dhcp mark 16
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application dns mark 16
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application ntp mark 16
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application snmp mark 16

! This section configures AVC to mark Bulk Data applications marking to AF11 (DSCP 10)
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application ftp mark 10
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application ftp-data mark 10
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application ftfps-data mark 10
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application cifs mark 10

! This section configures AVC to mark Scavenger applications to CS1 (DSCP 8)
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application netflix mark 8
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application youtube mark 8
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application skype mark 8
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application bittorrent mark 8
AireOS QoS Policy Deployment
Step 5) Attach QoS and AVC Profiles to WLAN and Enable AVC

(Cisco WLC) > config wlan qos 10 platinum
! Applies the Platinum QoS profile to the WLAN

(Cisco WLC) > config wlan avc 10 visibility enable
! Enables AVC Visibility on WLAN 10

(Cisco WLC) > config wlan avc 10 profile AVC-APPS enable
! This command applies the AVC profile AVC-APPS to WLAN ID 10
AireOS QoS Policy Deployment
Step 6) Configure Downstream DSCP-to-UP Mapping and Enable Upstream DSCP-Trust

<table>
<thead>
<tr>
<th>RFC 4594-Based Model</th>
<th>DSCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Control</td>
<td>(CS7)</td>
</tr>
<tr>
<td>Internetwork Control</td>
<td>CS6</td>
</tr>
<tr>
<td>Voice + Voice-ADMIT</td>
<td>EF + 44</td>
</tr>
<tr>
<td>Broadcast Video</td>
<td>CS5</td>
</tr>
<tr>
<td>Multimedia Conferencing</td>
<td>AF4</td>
</tr>
<tr>
<td>Real-Time Interactive</td>
<td>CS4</td>
</tr>
<tr>
<td>Multimedia Streaming</td>
<td>AF3</td>
</tr>
<tr>
<td>Signaling</td>
<td>CS3</td>
</tr>
<tr>
<td>Transactional Data</td>
<td>AF2</td>
</tr>
<tr>
<td>QoS</td>
<td>CS2</td>
</tr>
<tr>
<td>Bulk Data</td>
<td>AF1</td>
</tr>
<tr>
<td>Scavenger</td>
<td>CS1</td>
</tr>
<tr>
<td>Best Effort</td>
<td>DF</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IEEE 802.11e Model</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>UP 7</td>
<td>Voice</td>
</tr>
<tr>
<td>UP 6</td>
<td>Access</td>
</tr>
<tr>
<td>UP 5</td>
<td>Video</td>
</tr>
<tr>
<td>UP 4</td>
<td>Access</td>
</tr>
<tr>
<td>UP 3</td>
<td>Best Effort</td>
</tr>
<tr>
<td>UP 0</td>
<td>Access</td>
</tr>
<tr>
<td>UP 2</td>
<td>Background</td>
</tr>
<tr>
<td>UP 1</td>
<td>Access</td>
</tr>
</tbody>
</table>
AireOS QoS Policy Deployment
Step 6) Configure Downstream DSCP-to-UP Mapping and Enable Upstream DSCP-Trust—Configuration (Part 1 of 2)

Step 1: Disable the Current QoS Map
(Cisco WLC) > config qos qosmap disable

Step 2: Configure the UP-to-DSCP Maps
(Cisco WLC) > config qos qosmap up-to-dscp-map 0 0 0 7
(Cisco WLC) > config qos qosmap up-to-dscp-map 1 8 8 15
(Cisco WLC) > config qos qosmap up-to-dscp-map 2 16 16 23
(Cisco WLC) > config qos qosmap up-to-dscp-map 3 24 24 31
(Cisco WLC) > config qos qosmap up-to-dscp-map 4 32 32 39
(Cisco WLC) > config qos qosmap up-to-dscp-map 5 40 40 47
(Cisco WLC) > config qos qosmap up-to-dscp-map 6 48 48 63
(Cisco WLC) > config qos qosmap up-to-dscp-map 7 56 63 63
AireOS QoS Policy Deployment
Step 6) Configure Downstream DSCP-to-UP Mapping and Enable Upstream DSCP-Trust—Configuration (Part 2 of 3)

Step 3: Configure DSCP-to-UP Mapping Exceptions

(Cisco Controller) > config qos qosmap dscp-to-up-exception 56 0
(Cisco Controller) > config qos qosmap dscp-to-up-exception 48 0
(Cisco Controller) > config qos qosmap dscp-to-up-exception 46 6
(Cisco Controller) > config qos qosmap dscp-to-up-exception 44 6
(Cisco Controller) > config qos qosmap dscp-to-up-exception 40 5
(Cisco Controller) > config qos qosmap dscp-to-up-exception 38 4
(Cisco Controller) > config qos qosmap dscp-to-up-exception 36 4
(Cisco Controller) > config qos qosmap dscp-to-up-exception 34 4
(Cisco Controller) > config qos qosmap dscp-to-up-exception 32 5
(Cisco Controller) > config qos qosmap dscp-to-up-exception 30 4
(Cisco Controller) > config qos qosmap dscp-to-up-exception 28 4
(Cisco Controller) > config qos qosmap dscp-to-up-exception 26 4
(Cisco Controller) > config qos qosmap dscp-to-up-exception 24 4
(Cisco Controller) > config qos qosmap dscp-to-up-exception 22 3
(Cisco Controller) > config qos qosmap dscp-to-up-exception 20 3
(Cisco Controller) > config qos qosmap dscp-to-up-exception 18 3
(Cisco Controller) > config qos qosmap dscp-to-up-exception 16 0
(Cisco Controller) > config qos qosmap dscp-to-up-exception 14 2
(Cisco Controller) > config qos qosmap dscp-to-up-exception 12 2
(Cisco Controller) > config qos qosmap dscp-to-up-exception 10 2
(Cisco Controller) > config qos qosmap dscp-to-up-exception 8 1
AireOS QoS Policy Deployment

Step 6) Configure Downstream DSCP-to-UP Mapping and Enable Upstream DSCP-Trust—Configuration (Part 3 of 3)

Step 4: Enable DSCP-Trust, the New Qos Maps and the 802.11 Networks
(Cisco Controller) > config qos qosmap trust-dscp-upstream enable
(Cisco Controller) > config qos qosmap enable
AireOS QoS Policy Deployment

Step 6) Configure Downstream DSCP-to-UP Mapping and Enable Upstream DSCP-Trust—UI Zoom

Before AireOS 8.4

Note: this screen has been significantly updated in AireOS 8.4
AireOS Static QoS Policy Deployment

Step 7) Re-Enable Radios and WLANs

(Cisco Controller) > config 802.11a enable network
(Cisco Controller) > config 802.11b enable network
(Cisco Controller) > config wlan enable all
Policy Overview
Policy Overview for Device Role = Access

**Ingress Marking Policies**
- Applied on all interfaces which are not connected to another network device
- Decision is based on looking at the topology / link information in NIB

**Egress Queuing Policies**
- Applied on all interfaces
Ingress Marking Policies

- No Marking policies applied on any interface

Egress Queuing Policies

- Applied on all interfaces
Policy Overview for Device Role = Core

**Ingress Marking Policies**
- No Marking policies applied on any interface

**Egress Queuing Policies**
- Applied on all interfaces
Policy Overview Device Role = Border Router

Ingress Marking Policies

• Marking policies applied on all interfaces except in the case where no SP Profile is specified for WAN interfaces

Egress Queuing Policies

• For LAN interfaces – LAN egress queuing policies are attached
• For WAN interfaces – egress queuing policies corresponding to the SP profile is attached to the interface
Policy Overview Device Type = WLC

Upstream

- Trust DSCP at the Access Point
- DSCP re-marked as per the AVC policy on WLC

Downstream

- DSCP re-marked as per the AVC policy on WLC
- DSCP \rightarrow UP mapping at the Access Point
Customisations and Operations
Application Policy – Custom Applications

Ability to add Custom Application to the Application Registry
Application Policy – Exclude Interface / Device

Ability to add Exclude Interfaces and/or Devices from Policy Scope
Application Policy - Policy Preview

Configuration changes to CAMPUS-Router1.cisco.com

class-map match-any DNA-MARKING_INETUNET-BAR
match protocol capwap-data
class-map match-any DNA-MARKING_INIVOICE_CUSTOM
class-map match-any DNA-MARKING_INETBROADCAST_CUSTOM
class-map match-any DNA-MARKING_INIREALTIME_CUSTOM
class-map match-any DNA-MARKING_INETIMM_CONF_CUSTOM
class-map match-any DNA-MARKING_INETIMM_STREAM_CUSTOM
class-map match-any DNA-MARKING_INETCONTROL_CUSTOM
class-map match-any DNA-MARKING_INETREALTIME_CUSTOM
class-map match-any DNA-MARKING_INETOAM_CUSTOM
class-map match-any DNA-MARKING_INETTRANS_DATA_CUSTOM
class-map match-any DNA-MARKING_INETULK_DATA_CUSTOM
class-map match-any DNA-MARKING_INETSCAVENGER_CUSTOM
class-map match-any DNA-MARKING_INIVOICE
match protocol cisco-jabber-audio
match protocol ms-lync-audio
class-map match-any DNA-MARKING_INETBROADCAST
match protocol dmp
match protocol cisco-ip-camera
class-map match-any DNA-MARKING_INETREALTIME
match protocol presence-media
class-map match-any DNA-MARKING_INETIMM_CONF
match protocol adobe-connect
match protocol ms-lync
match protocol rtp
match protocol cisco-jabber-video
match protocol cisco-phone
match protocol ms-lync-video
match protocol webex-media
match protocol unifi-media

Preview the CLI configuration before deployment
Model-based policy validation prior to deploying a policy.
Ability to Save Policy draft and deploy it at a later time
Application Policy – History and Rollback

Policy History

Policy Name: Demo-QOS-Policy

<table>
<thead>
<tr>
<th>Version</th>
<th>Date / Time</th>
<th>View</th>
<th>Rollback</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Jun 12, 2018 17:32:56</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Jun 12, 2018 17:30:17</td>
<td>Difference</td>
<td>Rollback</td>
</tr>
</tbody>
</table>

Deployment Status:
- 4/7 Devices Pro

Policy Name:
- Demo-QOS-Policy
  - Version: 2
  - Policy Status: Deploying

- Demo-QOS-Policy (Draft)
  - Version: 3
  - Policy Status: Draft

Showing 2 of 2
Application Policy – Clone and Restore

Ability to Clone existing Policy to a different Site/Scope

Ability to Restore brownfield QoS configuration
Application Policy – Consumers and Bi-Directionality

- Adds a Consumer (source IP address/range and source port/range) to the application
- Creates reverse ACE entries within ACLs for the application (Default: Unidirectional)
Application Policy – QOS Deployment Workflow

Step 1: Discovery - Discover Network Devices

Step 2: Design - Create Sites

Step 3: Design - Create Service Provider Profiles

Step 4: Provision - Add Network Devices to Sites

Step 5: Policy - Review Apps; Create Custom Queuing & WAN QOS profiles

Step 6: Policy - Create Custom Queuing & WAN QOS profiles

Step 7: Policy - Create, Preview, Pre-Check and then Apply Policy

Step 8: Policy - Modify, Rollback and Delete Policies (Optional)
Demo - Application Policy Live!
Cisco DNA Application Assurance
Top Applications in Use by Business

- Collection of application performance metric from routers
- Application visibility and Throughput from WLCs in a wireless only environment
- Use of NBAR2 to identify over 1400 applications, including hundreds of encrypted applications (without decryption and while ensuring full privacy and message-integrity)
- Use of Flexible NetFlow with application-identification extensions to export flow telemetry from wired and wireless clients
Assurance of Business Critical Applications

Health of Business Relevant Apps overtime

Table with the top N (filterable) applications:
- Name
- Heath
- User count
- Business class / Traffic class
- Usage / Average Throughput
- Perf (Loss, Latency, App Delay)
Application health dashboard menu

Click to see Application dashboard
Application Health Dashboard

Application Health Summary: As of May 22, 2018 12:36 pm

Business Relevant Application Health:

100%
Healthy Business Relevant Applications

Applications with GOOD Health
Application Name
ssh
Healthscore 1

Applications
6

Application Usage:

Top 10 Applications by Usage
- ssh: 52.63%
- snmp: 28.27%
- espn-browsing: 18.21%
- http: 5.0%
- ms-services: 0.7%
- apple-updates: 0.03%
- apple-services: 0.02%
- dns: 0.02%
- ntp: 0.1%
- ssl: 0.01%
# CLMEL

Application Health Dashboard – Applications

As of May 22, 2018 1:11 pm

Select applications by type and health

<table>
<thead>
<tr>
<th>Name</th>
<th>Health</th>
<th>Client Count</th>
<th>Business Class</th>
<th>Traffic Class</th>
<th>Usage</th>
<th>Average Throughput</th>
<th>Packet Loss (%)</th>
<th>Network Latency</th>
</tr>
</thead>
<tbody>
<tr>
<td>ssh</td>
<td>9</td>
<td>4</td>
<td>business-relevant</td>
<td>ops-admin-mgmt</td>
<td>2.79 GB</td>
<td>276.99 Kbps</td>
<td>2</td>
<td>5 ms</td>
</tr>
<tr>
<td>vnc</td>
<td>9</td>
<td>1</td>
<td>business-relevant</td>
<td>multimedia-streaming</td>
<td>15.76 MB</td>
<td>1.53 Kbps</td>
<td>12</td>
<td>22 ms</td>
</tr>
<tr>
<td>outlook-web-service</td>
<td>7</td>
<td>1</td>
<td>business-relevant</td>
<td>bulk-data</td>
<td>78.9 KB</td>
<td>7 bps</td>
<td>1</td>
<td>4 sec</td>
</tr>
<tr>
<td>ms-lync</td>
<td>10</td>
<td>5</td>
<td>business-relevant</td>
<td>multimedia-conferencing</td>
<td>73.09 MB</td>
<td>7.1 Kbps</td>
<td>0</td>
<td>3 ms</td>
</tr>
<tr>
<td>ms-office-web-apps</td>
<td>10</td>
<td>2</td>
<td>business-relevant</td>
<td>transactional-data</td>
<td>201.5 KB</td>
<td>19 bps</td>
<td>0</td>
<td>2 ms</td>
</tr>
<tr>
<td>ms-lync-control</td>
<td>10</td>
<td>1</td>
<td>business-relevant</td>
<td>signaling</td>
<td>1.37 KB</td>
<td>0 bps</td>
<td>0</td>
<td>0 ms</td>
</tr>
</tbody>
</table>
Application 360

Application health over time

Site application health details
Application experience in site

Application performance metrics

Select site to view application performance in site

Click to view clients using the application
Summary
Evolution of Application Policy

EasyQoS
First ever Policy manifestation
2nd most used application
Several 1000s of deployments
Several 100s of Make a Wish

Application Policy
Still the first manifestation of Policy
Same code, many improvements
Customers still loving it!
Application Policy Lifecycle

EasyQos

Design

Revise

Preview

Deploy

Design

Revise

Deploy

Preview

Save

Pre-check

Application Policy
Application Policy – What’s new in Cisco DNA Center v1.2.8

- Application Health Dashboard (Cisco DNA Assurance)
- Model-based policy validation prior to deploying a policy (Pre-check)
- Ability to save policy
- Device Exclusion from a scope
- New Device support (Cat6K Sup6T, ISR G2 w SM-ES2, SM-ES3, ISR 4351 & 4331, C9500H)
- DMVPN and GRE Interface support
- Skype 4 Business Integration with Cisco DNA App Assurance
Demo– Cisco DNA Center 1.2.8 Application Policy / Experience
What’s new in Cisco DNA Center 1.3
Application Visibility & Control in Cisco DNA-Center

- Application Policy
  Automating Deployment of QoS Policies Across the network

- Application Recognition Service
  Managing the registry of applications that the network can recognize, and how application recognition works throughout the network

- Application Assurance
  Monitoring the utilization and performance of individual applications, provides tools for isolating performance issues
Application Recognition Service – Cisco DNA-based Recognition Overview

- A new controller-based approach for ‘application-recognition’ in which the controller connects to any NBAR function in the network.
- Some of the classification work that a device has been doing is offloaded to the controller, this allows:
  - Better ‘first-packet-classification’
  - Improved classification in an asymmetrical routing environment.
- The “protocol pack” is managed by the controller, and can be dynamically augmented by connecting to external sources, this will:
  - Dynamically improve the signatures for applications (e.g. Microsoft-office-365-connector)
  - Allow the user to discover and easily add applications that are not included in the pack (e.g. home grown apps) by connecting to external sources as your datacentre/VPC/DNS server/etc..
Application Recognition Service – Cisco DNA-based Recognition
How Does it work?

• **Step 1:**
  NBAR Engines running on the devices are constantly sending
  • classification rules (server-based mapping of IP/port to app-name) to the controller
  • Details about unclassified traffic (hosts/sockets)
  • Basic Application Visibility Details (App->BW)
  This is done with a proprietary JSON over UDP protocol.
Application Recognition Service – Cisco DNA-based Recognition
How Does it work?

Step 2:
The controller can connect to external authoritative sources that could either help classify the unclassified traffic, or help generate improved signatures.
Application Recognition Service – Cisco DNA-based Recognition

How Does it work?

Step 3:
The controller resolves conflicts between engines, imports new data from external sources and generates a new dedicated signature file (Protocol Pack) and an aggregated Classification Rules File (App Rules), that gets periodically loaded by the devices (via FTP) to improves the functionality of NBAR running on the device itself.
Application Recognition Service – Cisco DNA-based Recognition

What are the value propositions?

- Some of the classification work that a device has been doing is offloaded to the controller, this allows:
  - Better ‘first-packet-classification’
  - Improved classification in an asymmetrical routing environment.
- The “protocol pack” is managed by the controller, and can be dynamically augmented by connecting to external sources, this will:
  - Dynamically improve the signatures for applications (e.g. Microsoft-office-365-connector)
  - Allow the user to discover and easily add applications that are not included in the pack (e.g. home grown apps) by connecting to external sources as your datacentre/VPC/DNS server/etc..
Demo- Cisco DNA Center AVC
Summary

- Cisco DNA Center Application Policy is a simple, highly secure, and scalable automated network QoS policy deployment solution
- Cisco DNA Center Application Policy 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 DNA Center is a centralised operations console that dramatically simplifies the management and orchestration of the core networking infrastructure
- Application Policy deploys industry-standard best-practices via Cisco Validated Designs

Solution Summary

- Provides end-to-end orchestration of QoS
- Simple and easy to deploy
- Works for and 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
- Support wireless & BYOD devices without client software upgrades

Benefits
Cisco DNA Center Platform Support (Release 1.2)
Wide Support for Brownfield & Greenfield Devices

Keep talking with us

We take your feedback very seriously

So please let us know how can we improve the product
Your Choice
Continue your education

- Cisco Demos in the World of Solutions
- Labs
- Meet The Expert
- Related sessions

#CLMEL

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public 138
Complete Your Online Session Evaluation

• Give us your feedback and receive a complimentary Cisco Live 2019 Power Bank after completing the overall event evaluation and 5 session evaluations.

• All evaluations can be completed via the Cisco Live Melbourne Mobile App.

• Don’t forget: Cisco Live sessions will be available for viewing on demand after the event at:

  https://ciscolive.cisco.com/on-demand-library/
Thank you
IMAGINE

INTUITIVE