

Cisco *live!*

February 15 - 19, 2016 • Berlin, Germany

We're ready. Are you?

IWAN AVC/QoS Design

BRKRST-2043

Kelly Fleshner, Communications Architect

CCIE #1852 – 20 years

Housekeeping

- Who am I? (kfleshne@cisco.com)
- “Advanced” Class
 - ✓ This is not an ‘Introduction to IWAN’ session
 - ✓ This is not an ‘IWAN Design’ session (Some design aspects will be discussed)
 - ✓ This is not a QoS deep dive session
 - ✓ This session is about how to configure AVC/QoS with your Cisco Intelligent WAN

Session Abstract:

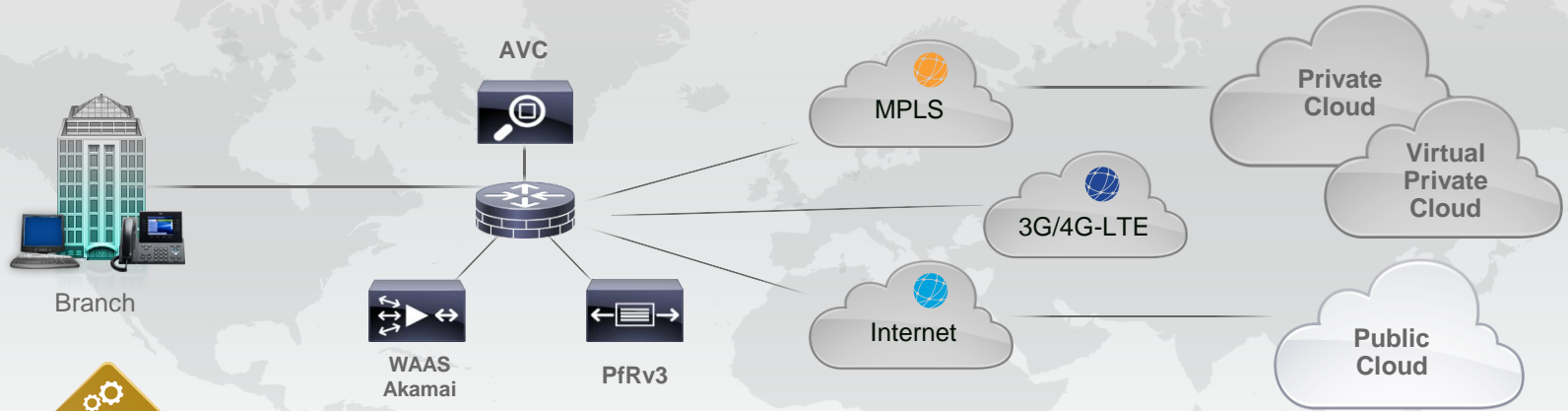
The most expensive bandwidth in the enterprise is in the WAN; as such, it should be fully optimized to deliver maximum ROI. This session focuses on how to deliver such optimization by deploying **Application Visibility and Control (AVC)** and **Quality of Service (QoS)** over the **Intelligent WAN (IWAN)**. Cisco’s QoS paradigm will be reviewed and applied to the IWAN, along with best practice QoS design recommendations. Practical and detailed design configurations will be presented for hierarchical QoS policies for sub-line rate Ethernet handoffs, MPLS VPN Class-of-Service mapping and DMVPN per-tunnel QoS. Additionally, new AVC/QoS technologies, such as **NBAR2 QoS** attributes will be introduced and applied to the IWAN. Cisco Prime Infrastructure templates for deploying and managing the IWAN will be reviewed, as will Cisco’s SD-WAN solution, the **APIC-EM IWAN** application, to show how the IWAN QoS and PfR can be centrally controlled.

Agenda

- Introduction and Overview
- Cisco's Approach to AVC/QoS
- Ingress LAN AVC/QoS Design
- Egress WAN AVC/QoS Design
 - WAN Queuing
 - Sub-line Rate Interfaces
 - DMVPN Per Tunnel QoS
 - Enterprise-to-SP Mapping
 - IWAN-Specific Considerations
 - PfR and QoS Interactions
- SD-WAN QoS (APIC-EM IWAN App)
- Summary and References

Introduction and Overview

Intelligent WAN (IWAN) Solution Components



Management & Orchestration



Cisco Prime



Transport Independence

- ▶ IPsec WAN Overlay
- ▶ Consistent Operational Model

DMVPN, PSK, PKI



Intelligent Path Control

- ▶ Optimal application routing
- ▶ Efficient use of bandwidth

Performance Routing (PfR)
QoS



Application Optimization

- ▶ Performance monitoring
- ▶ Optimization and Caching

AVC, WAAS, Akamai



Secure Connectivity

- ▶ NG Strong Encryption
- ▶ Threat Defense

Suite-B, CWS, ZBFW

The Why of AVC/QoS

AVC & QoS

Transform your business through
powerful yet simple networks
that are **customized** and **optimized** Why
to meet your needs

Cisco's Approach to AVC/QoS

Levels of QoS Policy Abstraction

Strategic vs. Tactical

- Strategic QoS Policy (**WHY** you want QoS)
 - reflects business *intent*
 - *is not constrained* by any technical or administrative limitation
 - is end-to-end
- Tactical QoS Policy (**HOW** you are going to do it / **WHAT** you configure)
 - adapts the strategic business intent to the maximum of platform's capabilities
 - *is limited* by various *tactical constraints*, including:
 - **Media constraints** (e.g. the WLAN has only 4 levels of service [access categories])
 - **Platform constraints** (e.g. a Catalyst 3750 has only 4 hardware queues)
 - **Interface constraints** (e.g. a T1 WAN link has limited bandwidth)
 - **Role constraints** (e.g. a CE may need to map into a reduced set of SP Classes-of-Service)

Strategic QoS Design

- 1) Define the business goals
- 2) Assign business-relevance to applications
- 3) Apply standards-based recommendations
- 4) Target bandwidth allocations per traffic-class



Strategic QoS Design

Part 1 of 4: Always, Always, Always Start with Defining the Business **Goals** of QoS

- *Guaranteeing voice quality*
- Delivering *Quality of Experience for video*
- *Improving user productivity*
- *Managing* business applications that are “*bandwidth hogs*”
- *De-prioritizing non-business applications*
- *Protecting the control planes*
- *Hardening the network*

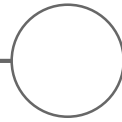
Strategic QoS Design

Part 2 of 4: Assign Business-Relevance to Applications



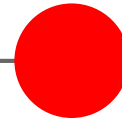
Relevant

- These applications directly supports business objectives
- Applications should be classified and marked according to **RFC 4594**-based rules



Default

- These applications may/may not support business objectives
 - E.g. HTTP/HTTPS
- Alternatively, administrator may not know the application (or how its being used in the org)
- Applications in this class should be marked DF and provisioned with a **default** best-effort service (**RFC 2474**)

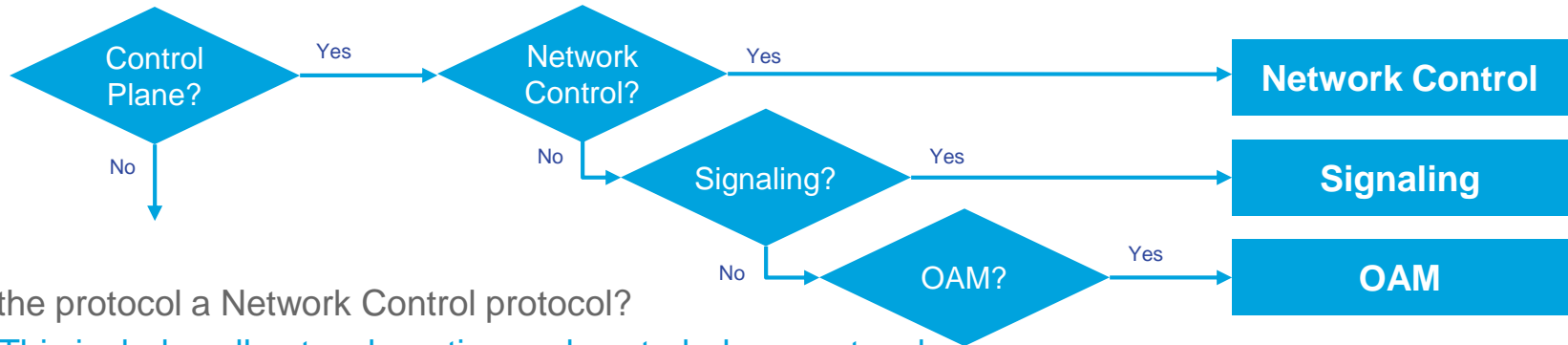


Irrelevant

- These applications are known and do not directly support any business objectives; this class includes ***all personal/consumer applications***
- Applications in this class should be marked CS1 and provisioned with a **“less-than-best-effort”** service , per (**RFC 3662**)

Strategic QoS Design

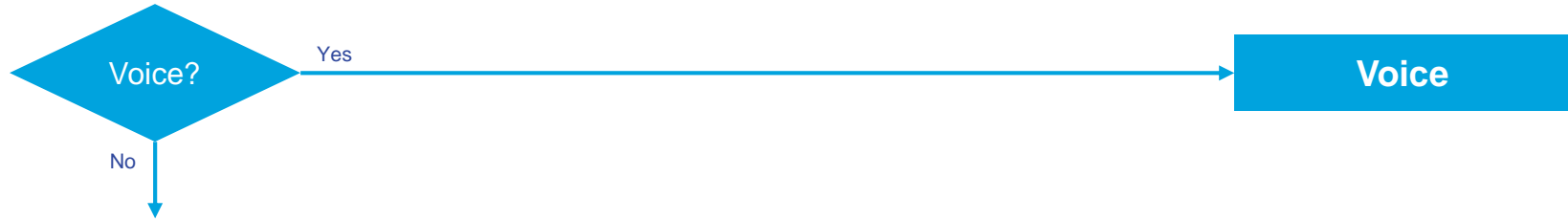
Part 3a of 4: Assign **Control Plane** to traffic-classes



- Is the protocol a Network Control protocol?
 - This includes all network routing and control-plane protocols
 - E.g. BGP, OSPF, EIGRP, HSRP, IKE, etc.
- Is the protocol a Signaling protocol?
 - This includes all call signaling / bandwidth reservation protocols
 - E.g. SIP, Skinny, H.323, RSVP etc.
- Is the protocol an Operations / Administration / Management protocol?
 - This includes all network management protocols (e.g. SNMP, Telnet, SSH, Syslog, NetFlow, etc.)

Strategic QoS Design

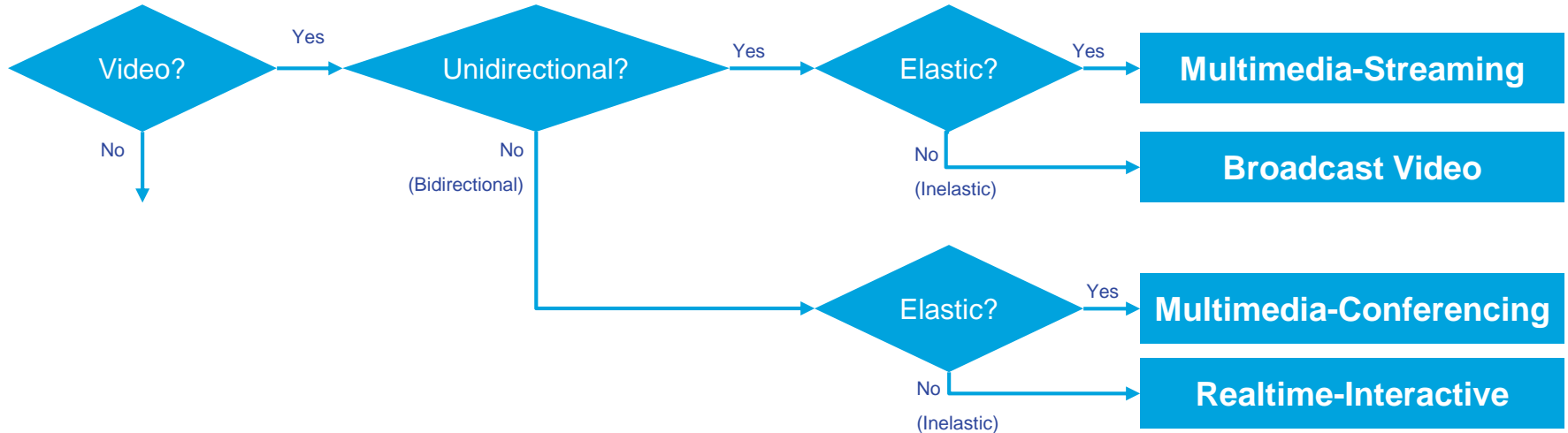
Part 3b of 4: Assign **Voice** applications / sub-components to voice traffic-class



- Is the application 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 Microsoft Lync; however, this option should **ONLY** be considered if this causes no conflict with your overall Call Admission Control strategy and voice-queue provisioning

Strategic QoS Design

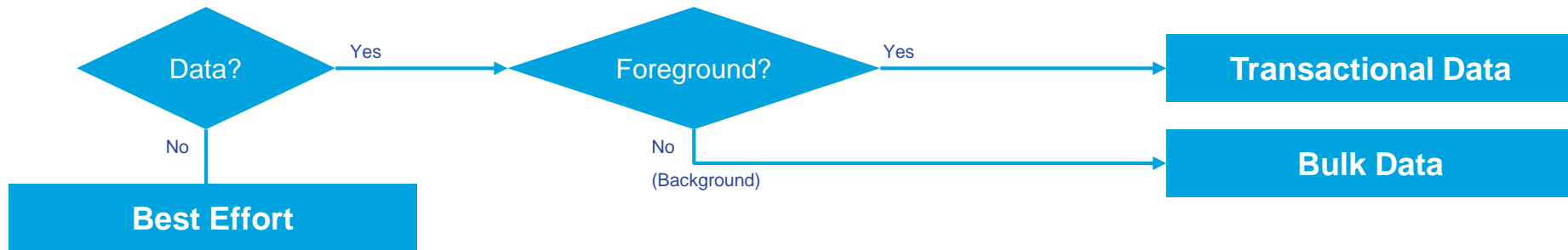
Part 3c of 4: Assign **Video** applications / sub-components to traffic-classes



- If the application is video?
 - If yes: determine if the application is unidirectional or bidirectional?
 - Then determine if the application is elastic (i.e. adaptive to congestion/drops) or inelastic?

Strategic QoS Design

Part 3d of 4: Assigning **Data** applications to traffic-classes



- Is the application Data?
 - Then determine: 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)

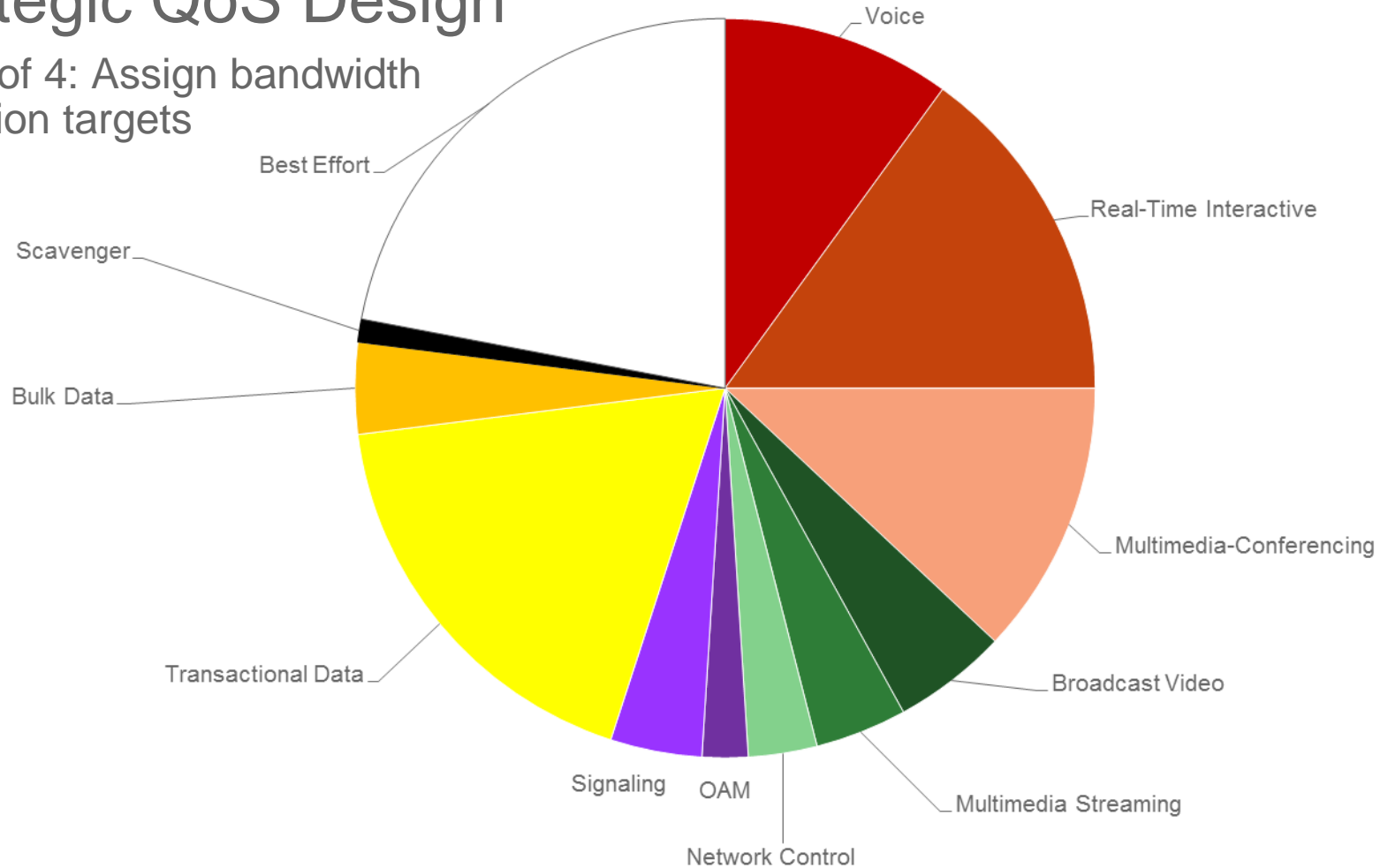
Strategic QoS Design

Part 3e of 4: Apply RFC 4594-based Marking / Queuing / Dropping Treatments

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

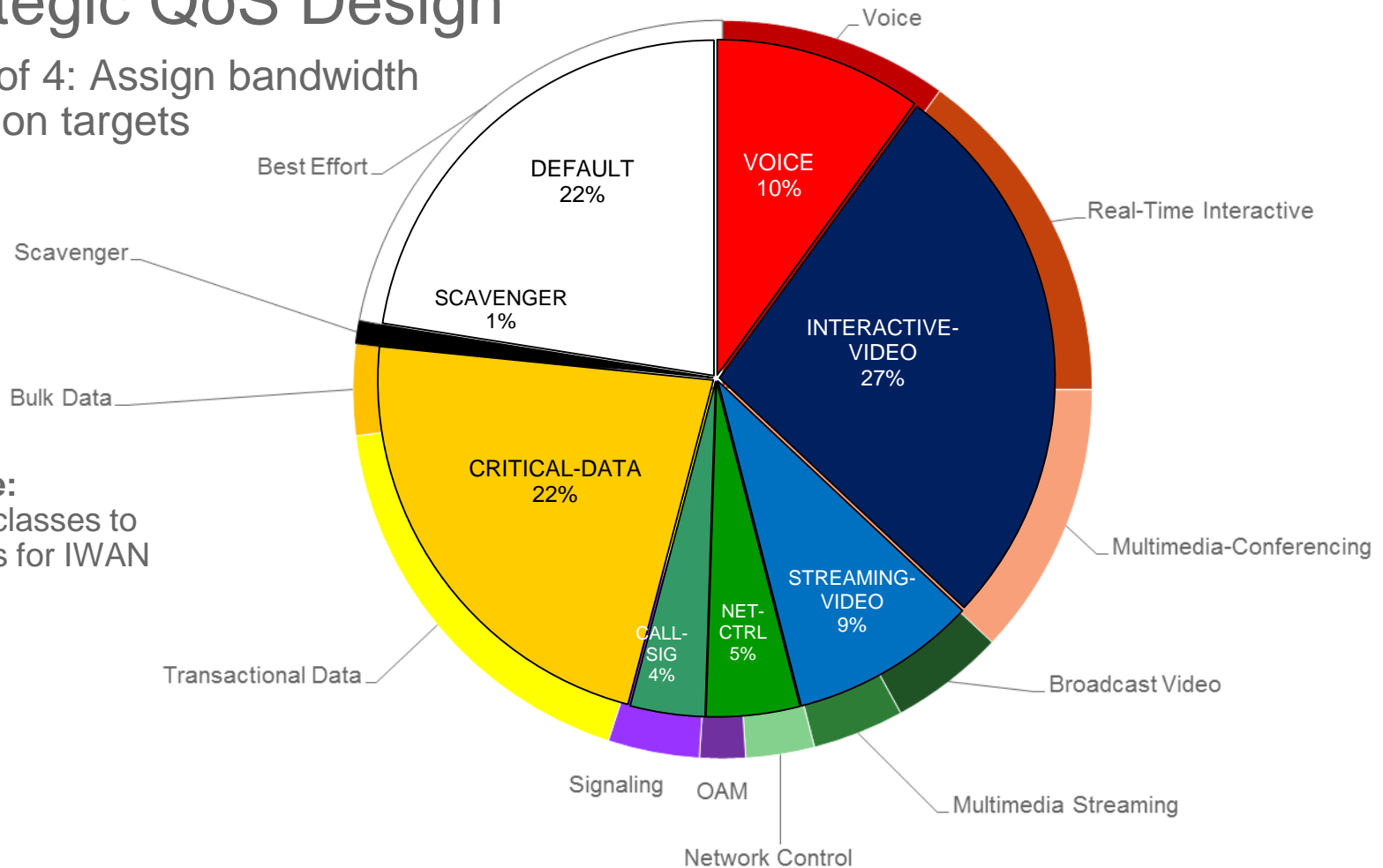
Strategic QoS Design

Part 4 of 4: Assign bandwidth allocation targets

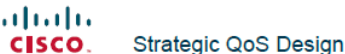


Strategic QoS Design

Part 4 of 4: Assign bandwidth allocation targets



Strategic QoS Design: At-A-Glance



The Quality of Service Challenge

Today there is a virtual explosion of rich media applications on the IP network. This explosion of content and media types, both managed and un-managed, requires network architects to take a new look at their Quality of Service (QoS) designs.

Step 1: Articulate Business Intent and Application Relevance

The first step may seem obvious and superfluous, but in actuality it is crucial: clearly define the business objectives that your QoS policies are to enable. These may include any/all of the following:

- Guaranteeing voice quality meets enterprise standards
- Ensuring a high Quality of Experience (QoE) for video
- Increasing user productivity by increasing network response times for interactive applications
- Managing applications that are "bandwidth hogs"
- Identifying and de-prioritizing consumer applications
- Improving network availability
- Hardening the network infrastructure

With these goals in mind, network architects can clearly identify which applications are relevant to their business. Conversely, this exercise will also make it apparent which applications are not relevant towards achieving business objectives. Such applications may include consumer-oriented and/or entertainment-oriented applications.

Finally, there may be applications/protocols that can fall into either category of business relevance. For example, HTTP/HTTPS may carry business-relevant traffic or consumer-oriented traffic, and as such cannot be clearly classified in either category. Note: in such cases, deep packet inspection technologies may be able to discreetly identify the applications being transported, allowing these to be properly classified in line with business objectives.

Figure 1 Determining Application Business Relevance



Step 2: Define an End-to-End QoS Design Strategy

Once applications have been defined as business-relevant (or otherwise), then the network architect must decide how to mark and treat these applications over the IP infrastructure.

To this end, Cisco advocates following relevant industry standards and guidelines, as this extends the effectiveness of your QoS policies beyond your direct administrative control. That being said, it may be helpful to overview a relevant RFC for QoS marking and provisioning: RFC 4594, "Configuration Guidelines for DiffServ Service Classes."

These guidelines are to be viewed as industry best-practice recommendations. As such, enterprises and service providers are encouraged to adopt these marking and provisioning recommendations with the aim of improving QoS consistency, compatibility, and interoperability. However, it should be noted that these guidelines are not standards; as such, modifications can be made to these recommendations as specific needs or constraints require.

Thus, to meet specific business requirements, Cisco has made a minor modification to its adoption of RFC 4594: specifically the swapping of Call-Signaling and Broadcast Video markings to CS3 and CS2, respectively. A summary of Cisco's implementation of RFC 4594 is presented in Figure 2.

Figure 2 Cisco (RFC 4594-Based) QoS Recommendations

Application Class	DSCP	Queueing and Scheduling
Voice	CS6	Priority Queue PSQ
Broadcast Video	CS2	Extended FQ
Real Time Interactive	CS4	Extended FQ
Multimedia Conferencing	AH2	DM Queue / DSCP WRED
Multimedia Streaming	AH3	DM Queue / DSCP WRED
CS	CS6	DM Queue
Live Signaling	CS3	DM Queue
Administrative/Control	CS2	DM Queue
Transactional Data	AH2	DM Queue / DSCP WRED
Bulk Data	AH1	DM Queue / DSCP WRED
Best Effort	EF	Default Queue / FQ
Scavenger	CS1	DM Queue

RFC 4594 also provides some application classification rules to help network architects to assign applications to the optimal traffic classes; these are summarized in the following sections:

Business relevant application can be grouped into one of four main categories:

- control plane protocols
- voice applications
- video applications
- data applications

Beginning with the control plane protocols, these may be sub-divided further, as shown in Figure 3.

Figure 3 Control Plane Traffic Classes



• **Network Control**—This traffic class is intended for network control plane traffic, which is required for reliable operation of the enterprise network. Traffic in this class should be marked CS6 and provisioned with a (moderate, but dedicated) guaranteed bandwidth queue. WRED should not be enabled on this class, as network control traffic should not be dropped. Example traffic includes EIGRP, OSPF, BGP, HSRP, IKE, etc.

• **Signaling**—This traffic class is intended for signaling traffic that supports IP voice and video telephony. Traffic in this class should be marked CS3 and provisioned with a (moderate, but dedicated) guaranteed bandwidth queue. WRED should not be enabled on this class, as signaling traffic should not be dropped. Example traffic includes SCCP, SIP, H.323, etc.

• **Operations/Administration/Management (OAM)**—This traffic class is intended for network operations, administration, and management traffic. This class is critical to the ongoing maintenance and support of the network. Traffic in this class should be marked CS2 and provisioned with a (moderate, but dedicated) guaranteed bandwidth queue. WRED should not be enabled on this class, as OAM traffic should not be dropped. Example traffic includes SSH, SNMP, Syslog, etc.

Cisco Strategic QoS Design

Provisioning for voice is relatively straightforward:

- **Voice**—This traffic class is intended for voice/audio traffic (VoIP signaling traffic is assigned to the "Call-Signaling" class). Traffic assigned to this class should be marked EF. This class is provisioned with an Expedited Forwarding (EF) Per-Hop Behavior (PHB). The EF PHB defined in RFC 3246 is a strict-priority queuing service and, as such, admission to this class should be controlled. Example traffic includes G.711 and G.729a, as well as the audio components of multimedia conferencing applications, like Cisco Jabber, WebEx and Spark.

Video—on the other hand—may have unique QoS requirements depending on the type, as illustrated in Figure 4.

Figure 4 Video Traffic Classes



Two key questions need to be answered to determine the optimal traffic classification for a video application:

- is the video unidirectional or bidirectional?
- is the video elastic or inelastic?

"Elastic" flows are able to adapt to network congestion and/or drops (by reducing frame rates, bit rates, compression rates, etc.); "inelastic" flows either do not have such capabilities or—in order to meet specific business configured not to utilize these.

With these two questions answered, video applications may be assigned to their respective traffic classes, including:

- **Broadcast Video**—This traffic class is intended for broadcast TV, live events, video surveillance flows, and similar "inelastic" streaming video flows. Traffic in this class should be marked Class Selector 5 (CS5) and may be provisioned with an EF PHB; as such, admission to this class should be controlled. Example traffic includes live Cisco Enterprise TV (ETV) streams, and Cisco IP Video Surveillance.

- **Real-Time Interactive**—This traffic class is intended for inelastic interactive video applications. Whenever possible, signaling and data sub-components of this class should be separated out and assigned to their respective traffic classes. Traffic in this class should be marked CS4 and may be provisioned with an EF PHB; as such, admission to this class should be controlled. An example application is Cisco TelePresence.

- **Multimedia Conferencing**—This traffic class is intended for elastic interactive multimedia collaboration applications. Whenever possible, signaling and data sub-components of this class should be separated out and assigned to their respective traffic classes. Traffic in this class should be marked Assured Forwarding (AF) Class 4 (AF4) and should be provisioned with a guaranteed bandwidth queue with DSCP-based Weighted-Random Early Detect (DSCP-WRED) enabled. Traffic in this class may be subject to policing and re-marking. Example applications include Cisco Jabber, WebEx and Spark.

- **Multimedia Streaming**—This traffic class is intended for elastic streaming video applications, such as Video-on-Demand (VoD). Traffic in this class should be marked AF Class 3 (AF3) and should be provisioned with a guaranteed bandwidth queue with DSCP-based WRED enabled. Example applications include Cisco Digital Media System Video-on-Demand (VoD) streams, E-Learning videos, etc.

Figure 5 Data Traffic Classes



When it comes to data applications, there is really only one key question to answer (as illustrated in Figure 5):

- Is the data application "foreground" or "background"?

"Foreground" refers to applications from which users expect a response—via the network—in order to continue with their tasks; excessive latency to such applications will directly impact user productivity.

Conversely, "background" applications—while business relevant—do not directly impact user productivity and typically consist of machine-to-machine flows.

- **Transactional Data**—This traffic class is intended for interactive, "foreground" data applications. Traffic in this class should be marked AF Class 2 (AF2) and should be provisioned with a dedicated bandwidth queue with DSCP-WRED enabled. This traffic class may be subject to policing and re-marking. Example applications include data components of multimedia collaboration applications, Enterprise Resource Planning (ERP) applications, Customer Relationship Management (CRM) applications, database applications, etc.

- **Bulk Data**—This traffic class is intended for non-interactive "background" data applications. Traffic in this class should be marked AF Class 1 (AF1) and should be provisioned with a dedicated bandwidth queue with DSCP-WRED enabled. This traffic class may be subject to policing and re-marking. Example applications include E-mail, backup operations, FTP/SFTP transfers, video and content distribution, etc.

With all business-relevant applications assigned to their respective traffic classes, then only two types of traffic classes are left to be provisioned:

- **Best Effort (the Default Class)**—This traffic class is the default class. The vast majority of applications will continue to default to this Best-Effort service class; as such, this default class should be adequately provisioned. Traffic in this class is marked Default Forwarding (DF or DSCP 0) and should be provisioned with a dedicated queue. WRED is recommended to be enabled on this class.

- **Scavenger**—This traffic class is intended for all applications that have been previously identified as business-relevant. These may include video applications that are consumer and/or entertainment-oriented. The approach of a "less-than-Best-Effort" service class for non-business applications (as opposed to shutting these down entirely) has proven to be a popular, political compromise. These applications are permitted on business networks when bandwidth is available; however, as soon as the network experiences congestion, this class is the most aggressively dropped. Traffic in this class should be marked CS1 and should be provisioned with a minimal bandwidth queue that is the first to starve should network congestion occur. Example traffic includes Netflix, YouTube, Xbox Live/360 Movies, iTunes, BitTorrent, etc.

For more details, see http://www.cisco.com/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSIntro_40.html And the Cisco Press Book: **End-to-End QoS Network Design** (Second Edition) Chapter 10



<http://tinyurl.com/hw4sbj6>

Ingress LAN AVC/QoS Design

NBAR QoS Attributes

- NBAR2 library is very large (~1400 apps)
- While **powerful** this toolset is not **simple** to wield



NBAR2 Overview

- Cisco Network Based Application Recognition (NBAR) can identify ~1400 applications/protocols via deep-packet inspection (DPI)
- To assist in policy-definition and in browsing, the extensive application library is grouped by various attributes, such as categories and sub-categories

Category	First level grouping of applications with similar functionalities
Sub-category	Second level grouping of applications with similar functionalities
Application-group	Grouping of applications based on brand or application suite
P2P-technology?	Indicates application is peer-to-peer
Encrypted?	Indicates application is encrypted
Tunneled?	Indicates application uses tunneling technique

New NBAR2 Attribute: Traffic-Class

Name	Description
voip-telephony	VoIP telephony (bearer-only) traffic
broadcast-video	Broadcast TV, live events, video surveillance
real-time-interactive	High-definition interactive video applications
multimedia-conferencing	Desktop software multimedia collaboration applications
multimedia-streaming	Video-on-Demand (VoD) streaming video
network-control	Network control plane traffic
signaling	Signaling traffic that supports IP voice and video telephony
ops-admin-mgmt	Network operations, administration, and management traffic
transactional-data	Interactive data applications
bulk-data	Non-interactive data applications

Introduced in IOS XE 3.16S and IOS 15.5(3)M

New NBAR2 Attribute: Business-Relevance

Name	Description
business-relevant	Business critical applications
default	Related business applications
business-irrelevant	Non business applications

Introduced in IOS XE 3.16S and IOS 15.5(3)M

New NBAR2 QoS Attributes

Business Relevance Attribute and Traffic-Class Attribute

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

Changing Business-Relevancy

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

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



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

```
ip nbar attribute-set skype ATTRIBUTE_MAP-RELEVANT
```

Changing Application Business-Relevance

Protocol Pack 14+ (All Options)

Scenario 1: Making an Application Business-Relevant

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

Scenario 2: Making an Application Best-Effort/Default

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

Scenario 3: Making an Application Business-Irrelevant

```
ip nbar attribute-map ATTRIBUTE_MAP-SCAVENGER attribute business-relevance business-irrelevant
ip nbar attribute-set application-name ATTRIBUTE_MAP-SCAVENGER
```

LAN Edge AVC/QoS Config for 1400+ Applications

```
class-map match-all VOICE-NBAR
  match protocol attribute traffic-class voip-telephony
  match protocol attribute business-relevance business-relevant
class-map match-all BROADCAST_VIDEO-NBAR
  match protocol attribute traffic-class broadcast-video
  match protocol attribute business-relevance business-relevant
class-map match-all REAL_TIME_INTERACTIVE-NBAR
  match protocol attribute traffic-class real-time-interactive
  match protocol attribute business-relevance business-relevant
class-map match-all MULTIMEDIA_CONFERENCING-NBAR
  match protocol attribute traffic-class multimedia-conferencing
  match protocol attribute business-relevance business-relevant
class-map match-all MULTIMEDIA_STREAMING-NBAR
  match protocol attribute traffic-class multimedia-streaming
  match protocol attribute business-relevance business-relevant
class-map match-all SIGNALING-NBAR
  match protocol attribute traffic-class signaling
  match protocol attribute business-relevance business-relevant
class-map match-all NETWORK_CONTROL-NBAR
  match protocol attribute traffic-class network-control
  match protocol attribute business-relevance business-relevant
class-map match-all NETWORK_MANAGEMENT-NBAR
  match protocol attribute traffic-class ops-admin-mgmt
  match protocol attribute business-relevance business-relevant
class-map match-all TRANSACTIONAL_DATA-NBAR
  match protocol attribute traffic-class transactional-data
  match protocol attribute business-relevance business-relevant
class-map match-all BULK_DATA-NBAR
  match protocol attribute traffic-class bulk-data
  match protocol attribute business-relevance business-relevant
class-map match-all SCAVENGER-NBAR
  match protocol attribute business-relevance business-irrelevant
```

```
policy-map MARKING
  class VOICE-NBAR
    set dscp ef
  class BROADCAST_VIDEO-NBAR
    set dscp cs5
  class REAL_TIME_INTERACTIVE-NBAR
    set dscp cs4
  class MULTIMEDIA_CONFERENCING-NBAR
    set dscp af41
  class MULTIMEDIA_STREAMING-NBAR
    set dscp af31
  class SIGNALING-NBAR
    set dscp cs3
  class NETWORK_CONTROL-NBAR
    set dscp cs6
  class NETWORK_MANAGEMENT-NBAR
    set dscp cs2
  class TRANSACTIONAL_DATA-NBAR
    set dscp af21
  class BULK_DATA-NBAR
    set dscp af11
  class SCAVENGER-NBAR
    set dscp cs1
  class class-default
    set dscp default
```

NBAR QoS Attributes: At-A-Glance



Cisco NBAR2 Business-Relevance and Traffic-Class Attributes

At-A-Glance

Role in Network

Cisco Network Based Application Recognition (NBAR) technology (now in its second generation) boasts an application library of over 1300 applications, many with media sub-component signatures also available, for an approximate total of 1400 distinct applications/sub-applications.

While this richness provides network administrators great flexibility and power in their policy-definitions, it is cumbersome to specify each application/sub-application by name within a QoS policy.

To assist in policy-definition and in browsing the application library, applications are grouped into categories and sub-categories. For example, NBAR application categories include:

- browsing
- business-and-productivity-tools
- email
- file-sharing
- gaming
- industrial-protocols
- instant-messaging
- internet-privacy
- layer3-over-ip
- location-based-services
- net-admin
- news-group
- social-networking
- streaming
- voice-and-video

Thus, for example if an administrator wanted to classify all email applications, they could use the `match protocol attribute category email` command within a class-map.

However, there may be cases where all applications within a given category may not be considered business-relevant, as shown in Figure 1.

Figure 1 Determining Application Business Relevance



For example, the voice-and-video category includes not only `cisco-phone` and `telepresence-media` voice and video flows, but also `skype` and `facetime`. But these consumer-oriented voice-and-video applications may be considered to be business-irrelevant, and so would need to be excluded from a business QoS policy.

Additionally, NBAR2 categories predate the industry-standard reference for configuring DiffServ QoS, namely RFC 4594. As such, these categories do not align with the traffic-class names used in this RFC.

Therefore, to simplify and expedite QoS configuration, NBAR2 has been enhanced in IOS XE 3.16 to support two new attributes:

- Business-Relevance
- Traffic-Class

Business-Relevance Attribute

The business-relevance attribute allows an administrator to classify a given application to one of three levels of business-relevance, as shown in Table 1.

Table 1 Business-Relevance NBAR2 Attribute

Name	Description
business-relevant	Business critical applications
default	Related business applications
business-irrelevant	Non business applications

All applications within the NBAR2 library has been pre-applied with the most common business-relevance attribute. For example, `youtube` by default is set as business-irrelevant, as most customers typically classify this application as such. However, this may not be the case across the board; for example, some businesses may be using YouTube for training purposes. In such cases, an administrator can change this business-relevancy setting to align with their objectives.

A business-irrelevant application is intended for a RFC 3662 "Scavenger" treatment. An application with a business-relevancy setting of default is intended for a RFC 2474 Default Forwarding treatment. In turn, business-relevant applications are intended to be serviced within their respective RFC 4594 traffic-class.

Traffic-Class Attribute

The traffic-class attribute aligns NBAR2 applications according to RFC 4594-based traffic-classes. For example, per RFC 4594 "Low Latency Data" applications (commonly referred to as "Bulk Data" applications) includes email, file-transfer and other "background" (i.e. non-user-interactive) applications. As such, rather than having to configure a class map along the lines of:

```
class-map match-any BULK-DATA
match protocol attribute category email
match protocol attribute category file-sharing
match protocol attribute sub-category backup-systems... etc.
```

An administrator can configure all relevant applications matching a specific RFC 4594 traffic-class with a single command (examples of which are shown on the reverse).

The ten RFC 4594 traffic classes for business-relevant applications are shown in Table 2.

Table 2 Traffic-Class NBAR2 Attribute

Name	Description
voip-telephony	VoIP telephony (bearer only) traffic
broadcast-video	Broadcast TV, live events, video surveillance
real-time-interactive	High-definition interactive video applications
multimedia-conferencing	Desktop software multimedia collaboration applications
multimedia-streaming	Video-on-Demand (VoD) streaming video
network-control	Network control plane traffic
signaling	Signaling traffic that supports IP voice and video telephony
ops-admin-mgmt	Network operators, administration, and management traffic
transactional-data	Interactive data applications
bulk-data	Non-interactive data applications

Thus, with these new attributes, all 1400 NBAR2 applications can be configured into a 12-class RFC 4594-based QoS model with a straightforward and user-intuitive syntax, as is shown on the reverse.

Cisco NBAR Business-Relevance and Traffic-Class Attributes

At-A-Glance

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

```
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 INTERACTIVE-VIDEO
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
class-map match-all SCAVENGER
match protocol attribute business-relevance business-irrelevant
```

Note: Highlighted commands are interface specific; otherwise these are global.

Step 2: Configure Marking Policy-Map

```
policy-map MARKING
class VOICE
set dscp ef
class BROADCAST-VIDEO
set dscp cs5
class INTERACTIVE-VIDEO
set dscp cs4
class MULTIMEDIA-CONFERENCING
set dscp af11
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
```

Step 3: Attach the Policy-Map to the Interface(s)
service-policy input MARKING

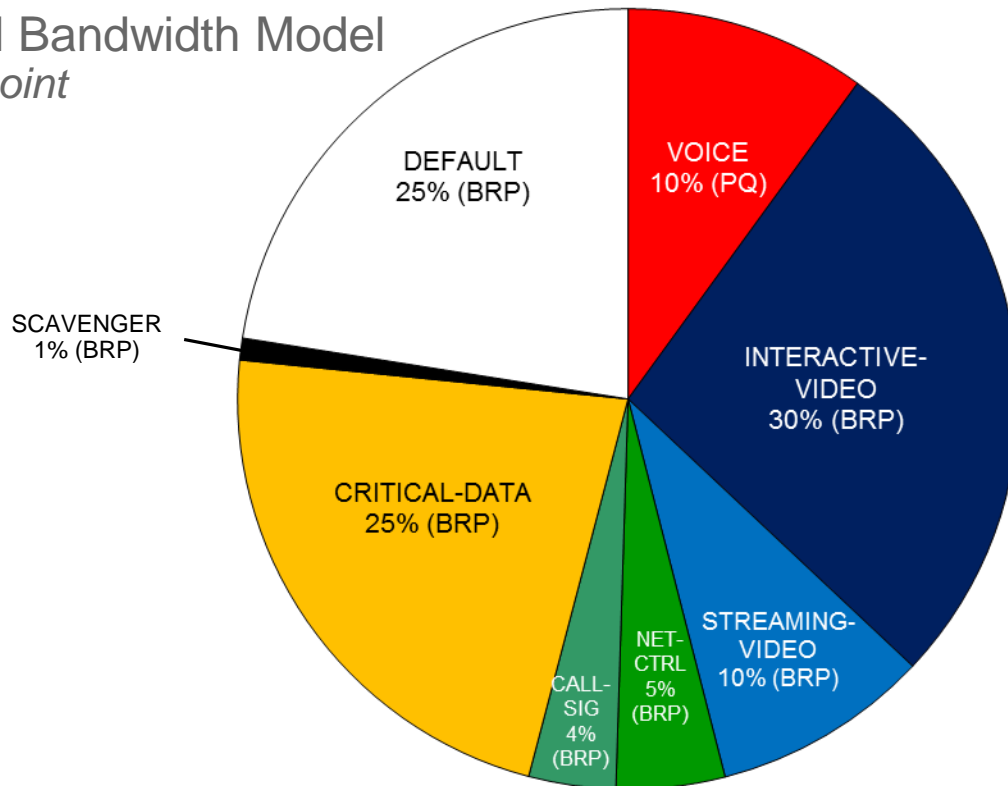
Egress WAN AVC/QoS Design

WAN Queueing

Example

8-Class IWAN Bandwidth Model

Good starting point

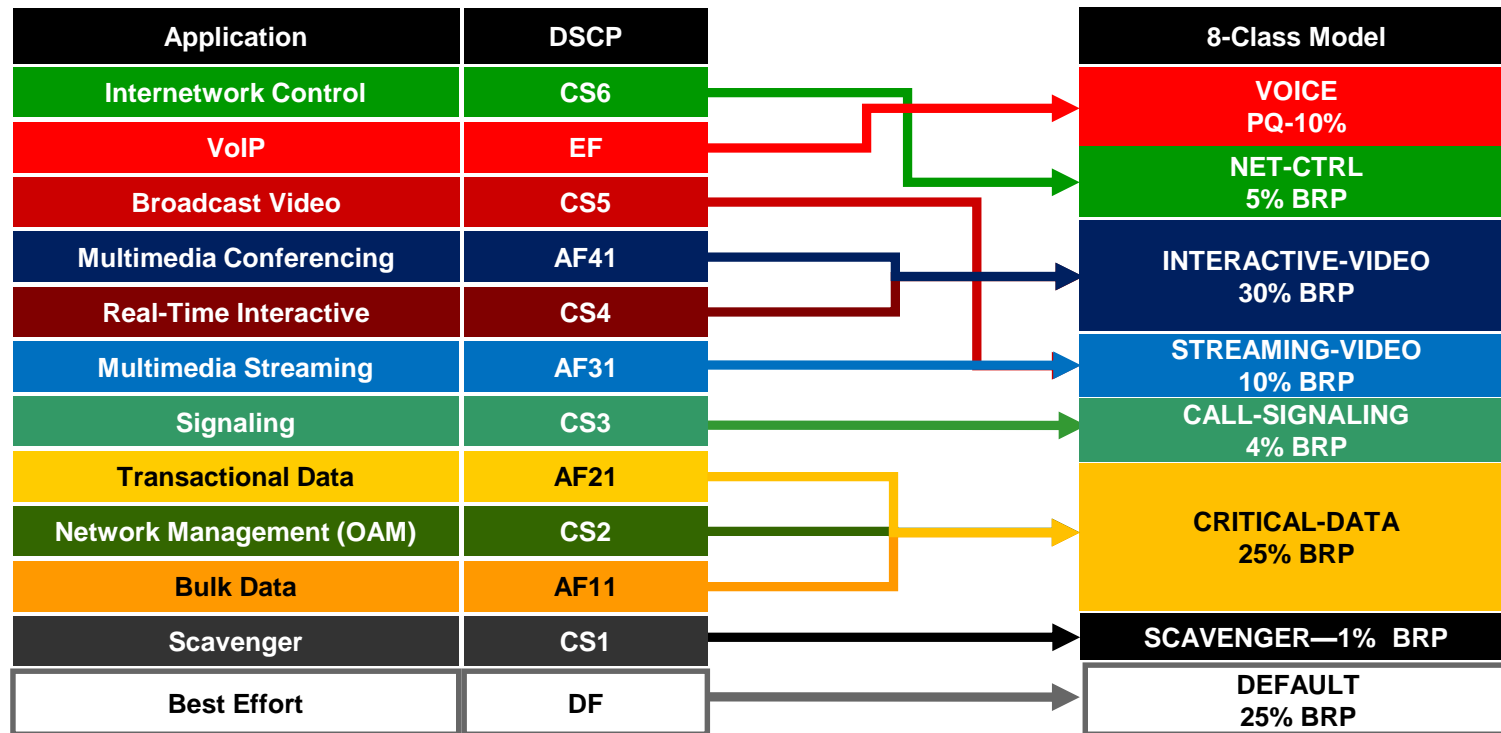


Note: Bandwidth Remaining Percentages must equal 100%

PQ = Priority Queue
BRP = Bandwidth Remaining Percent

QoS Mapping

Example: Combining 12 Classes into an 8-Class Model



8-Class QoS Model

IWAN 8-Class Class-Maps

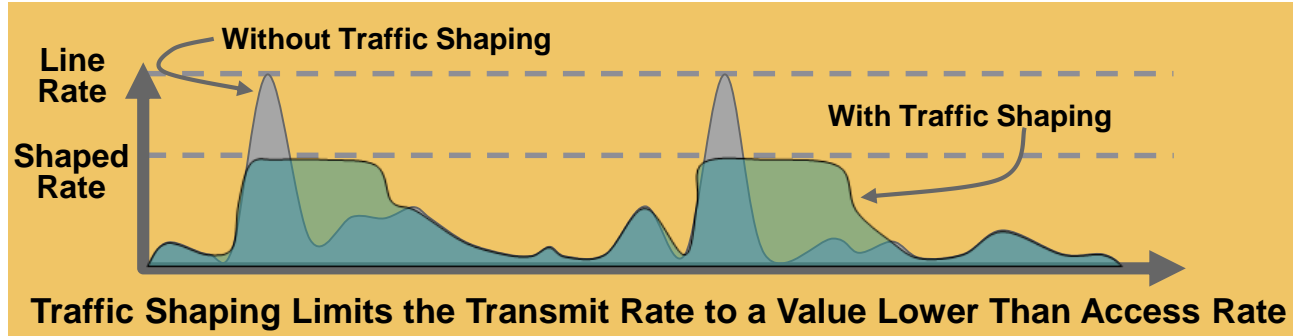
```
class-map match-any VOICE
  match dscp ef
class-map match-any INTERACTIVE-VIDEO
  match dscp cs4 af41 af42 af43
class-map match-any STREAMING-VIDEO
  match dscp cs5 af31 af32 af33
class-map match-any NET-CTRL
  match dscp cs6
class-map match-any CALL-SIGNALING
  match dscp cs3
class-map match-any CRITICAL-DATA
  match dscp cs2 af11 af12 af13 af21 af22 af23
class-map match-any SCAVENGER
  match dscp cs1
```

IWAN 8-Class Policy-Map

```
policy-map WAN
  class INTERACTIVE-VIDEO
    bandwidth remaining percent 30
    random-detect dscp-based
  class STREAMING-VIDEO
    bandwidth remaining percent 10
    random-detect dscp-based
  class NET-CTRL
    bandwidth remaining percent 5
  class CALL-SIGNALING
    bandwidth remaining percent 4
  class CRITICAL-DATA
    bandwidth remaining percent 25
    random-detect dscp-based
  class SCAVENGER
    bandwidth remaining percent 1
  class VOICE
    priority level 1
    police cir percent 10
  class class-default
    bandwidth remaining percent 25
    random-detect
```

Sub-Line Rate Interfaces

Traffic Shaping



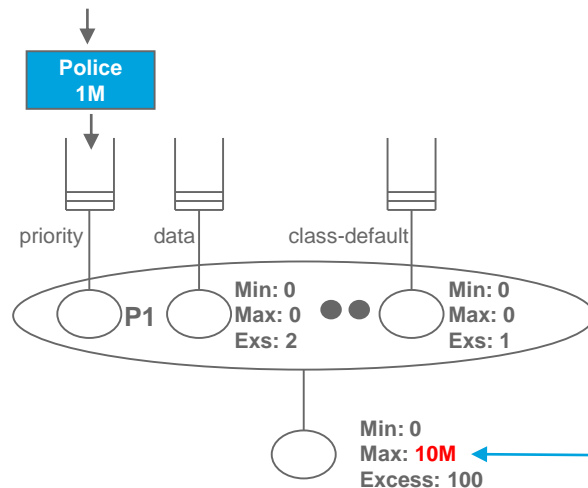
- Policers typically drop traffic
- Shapers typically delay excess traffic, smoothing bursts and preventing unnecessary drops
- Very common with Ethernet WAN, as well as Non-Broadcast Multiple-Access (NBMA) network topologies such as Frame-Relay and ATM

Access Rate Different from Service Rate

```
policy-map WAN
class INTERACTIVE-VIDEO
bandwidth remaining percent 30
random-detect dscp-based
class STREAMING-VIDEO
bandwidth remaining percent 10
random-detect dscp-based
class CALL-SIGNALING
bandwidth remaining percent 4
class NET-CTRL
bandwidth remaining percent 5
class CRITICAL-DATA
bandwidth remaining percent 25
random-detect dscp-based
class SCAVENGER
bandwidth remaining percent 1
class VOICE
priority level 1
police cir percent 10
class class-default
bandwidth remaining percent 25
random-detect
```

```
policy-map POLICY-TRANSPORT-1
class class-default
shape average 10000000
service-policy WAN
```

- 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 prioritize packets prior to shaping



GigE Interface
access service
with service rate of 10
(e.g. 10 Mbps)

Remote Site HQoS Policy Configuration

```
policy-map POLICY-TRANSPORT-1  
  class class-default  
    shape average 10000000  
    service-policy WAN
```

```
interface GigabitEthernet0/0  
  description Service Provider X  
  service-policy output POLICY-TRANSPORT-1
```

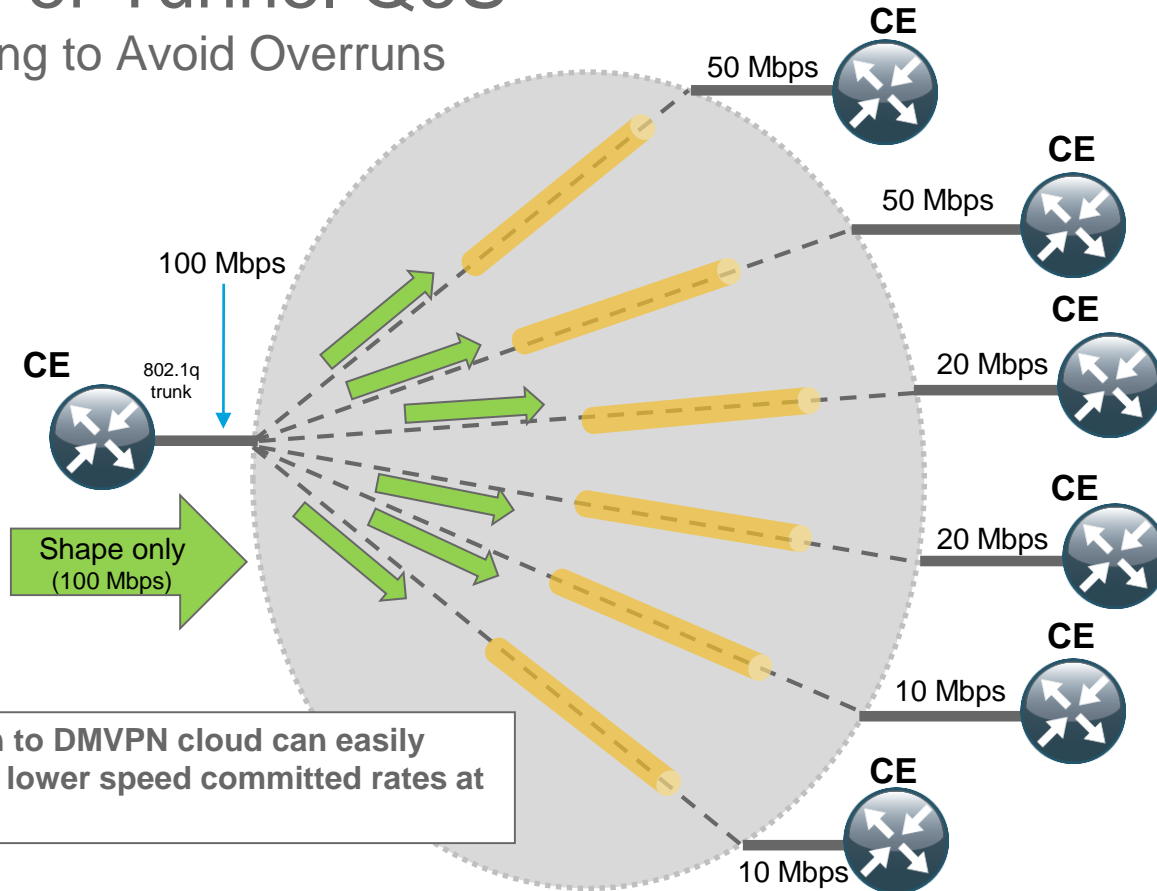
Sub-Line-Rate tag specifies the HQoS Parent Shaping policy that is required

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

DMVPN Per Tunnel QoS

DMVPN Per Tunnel QoS

Per-Site Shaping to Avoid Overruns



100 Mbps in to DMVPN cloud can easily overrun the lower speed committed rates at spoke sites



DMVPN Hub Per Tunnel QoS

Implementing Per-Site Traffic Shaping

```

policy-map RS-GROUP-50MBPS-POLICY
class class-default
shape average 50000000
service-policy WAN

policy-map RS-GROUP-20MBPS-POLICY
class class-default
shape average 20000000
service-policy WAN

policy-map RS-GROUP-10MBPS-POLICY
class class-default
shape average 10000000
service-policy WAN
    
```

Separate shaper policies for each remote-site bandwidth

```

policy-map POLICY-TRANSPORT-1-SHAPE-ONLY
class class-default
shape average 100000000
!
interface GigabitEthernet0/0/3
bandwidth 100000
service-policy output POLICY-TRANSPORT-1-SHAPE-ONLY

interface Tunnel10
nhrp map group RS-GROUP-10MBPS service-policy output RS-GROUP-10MBPS-POLICY
nhrp map group RS-GROUP-20MBPS service-policy output RS-GROUP-20MBPS-POLICY
nhrp map group RS-GROUP-50MBPS service-policy output RS-GROUP-50MBPS-POLICY
    
```

List all available policies as map groups on hub tunnel interface
 Add a class-default shape-only policy on the hub physical interface

Signal from the spoke to the hub to use the correct policy for each remote site

Spoke Tunnel Configurations

10 Mbps spoke

```

interface GigabitEthernet0/0
bandwidth 10000
service-policy output POLICY-TRANSPORT-1
!
interface Tunnel10
bandwidth 10000
nhrp group RS-GROUP-10MBPS
tunnel source GigabitEthernet0/0
tunnel vrf IWAN-TRANSPORT-1
    
```

20 Mbps spoke

```

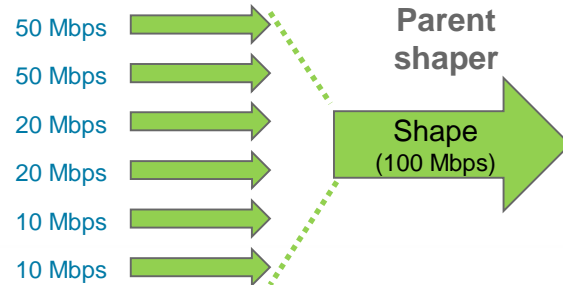
interface GigabitEthernet0/0
bandwidth 20000
service-policy output POLICY-TRANSPORT-1
!
interface Tunnel10
bandwidth 20000
nhrp group RS-GROUP-20MBPS
tunnel source GigabitEthernet0/0
tunnel vrf IWAN-TRANSPORT-1
    
```

50 Mbps spoke

```

interface GigabitEthernet0/0
bandwidth 50000
service-policy output POLICY-TRANSPORT-1
!
interface Tunnel10
bandwidth 50000
nhrp group RS-GROUP-50MBPS
tunnel source GigabitEthernet0/0
tunnel vrf IWAN-TRANSPORT-1
    
```

Per tunnel shapers



Enterprise-to-SP QoS Mapping

Enterprise to SP QoS Mapping



The **12 class** view is preserved across the enterprise even though we are treating it differently in the router and sending it to different channels within the SP network.

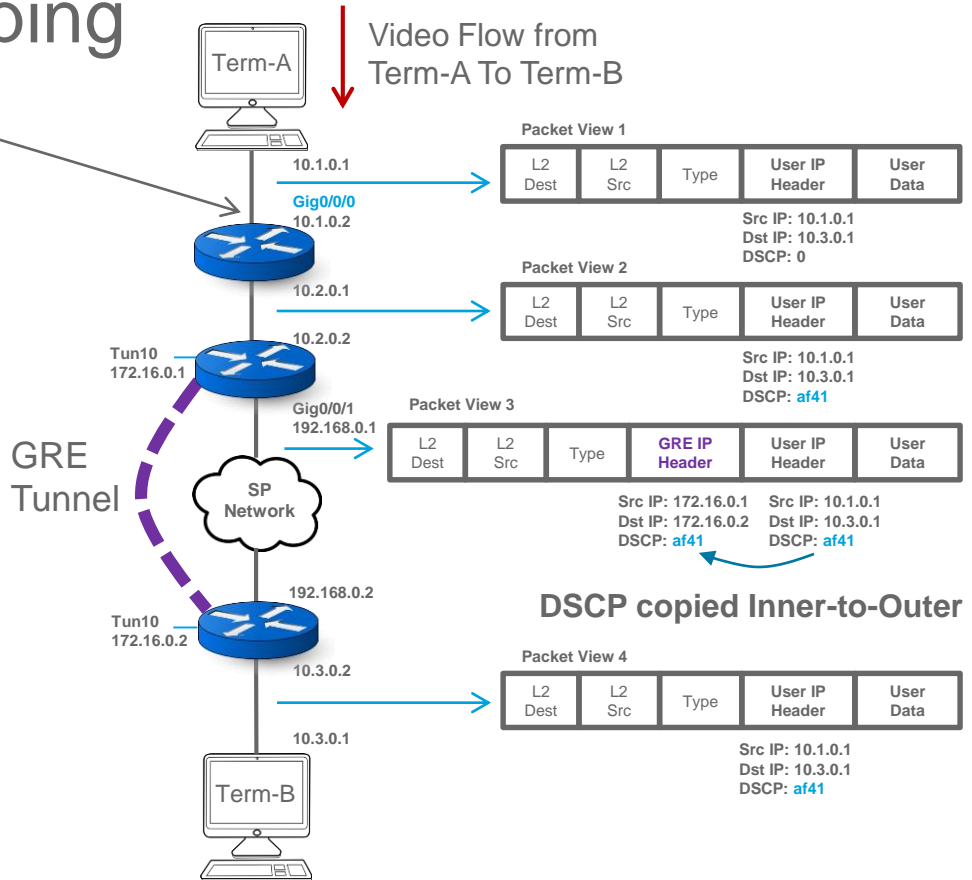
The **12 classes** remain intact on the inner header and the outer header is discarded after leaving the tunnel interface

Enterprise to SP Mapping

Default SP Marking

```

class-map match-all MULTIMEDIA_CONFERENCING-NBAR
match protocol attribute traffic-class multimedia-conferencing
match protocol attribute business-relevance business-relevant
!
policy-map traffic-marking
class MULTIMEDIA_CONFERENCING-NBAR
set dscp af41
!
int gig0/0/0
service-policy in traffic-marking
    
```



Enterprise to SP Mapping

Set dscp outbound on physical (Branch)

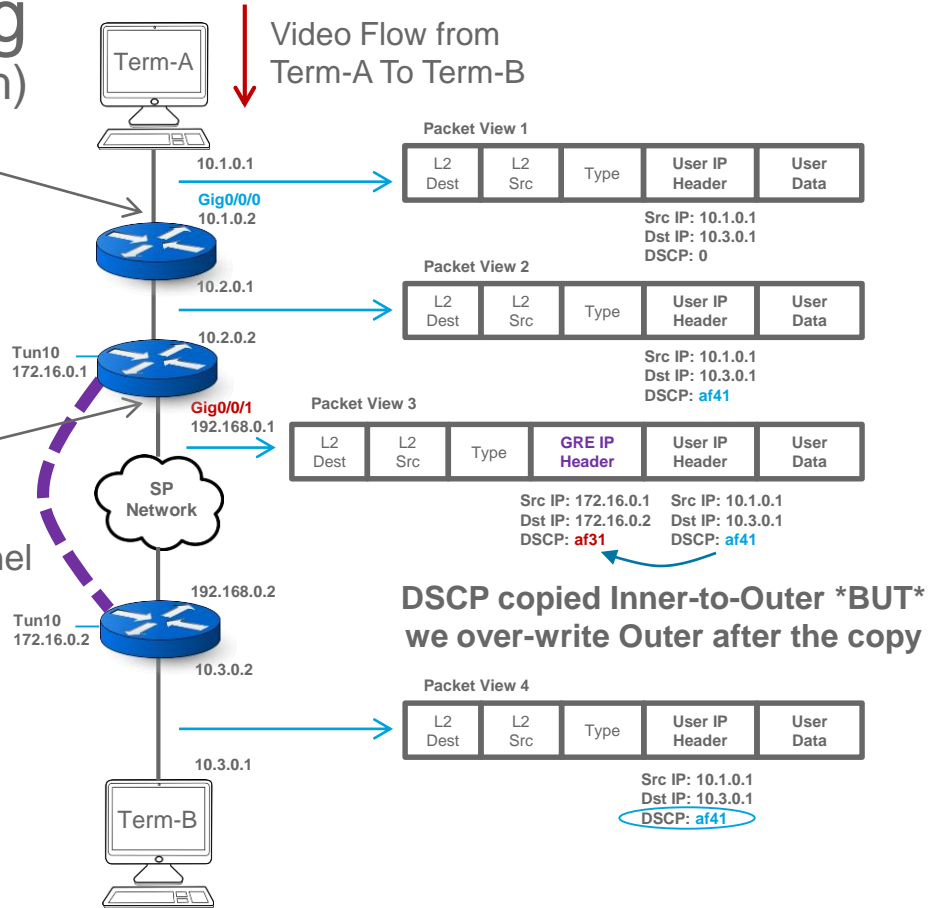
```

class-map match-all MULTIMEDIA_CONFERENCING-NBAR
match protocol attribute traffic-class multimedia-conferencing
match protocol attribute business-relevance business-relevant
!
policy-map traffic-marking
class MULTIMEDIA_CONFERENCING-NBAR
set dscp af41
!
int gig0/0/0
service-policy in traffic-marking
    
```

```

class-map INTERACTIVE-VIDEO
match dscp af41
!
policy-map egress-queuing
class INTERACTIVE-VIDEO
set dscp af31
!
int gig0/0/1
service-policy out egress-queuing
    
```

GRE Tunnel



Enterprise to SP Mapping

Set dscp tunnel outbound on tunnel (Hub)

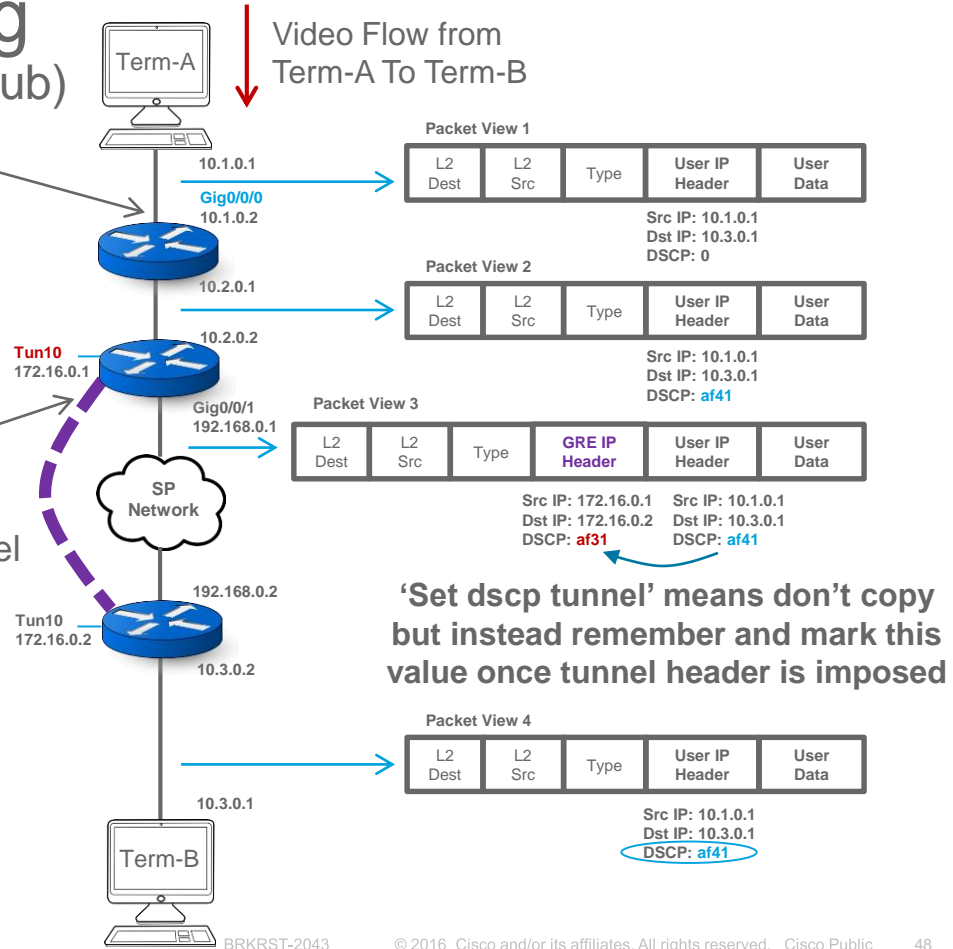
```

class-map match-all MULTIMEDIA_CONFERENCING-NBAR
match protocol attribute traffic-class multimedia-conferencing
match protocol attribute business-relevance business-relevant
!
policy-map traffic-marking
class MULTIMEDIA_CONFERENCING-NBAR
set dscp af41
!
int gig0/0/0
service-policy in traffic-marking
    
```

```

class-map INTERACTIVE-VIDEO
match dscp af41
!
policy-map egress-queuing
class INTERACTIVE-VIDEO
set dscp tunnel af31
!
int tun10
service-policy out egress-queuing
    
```

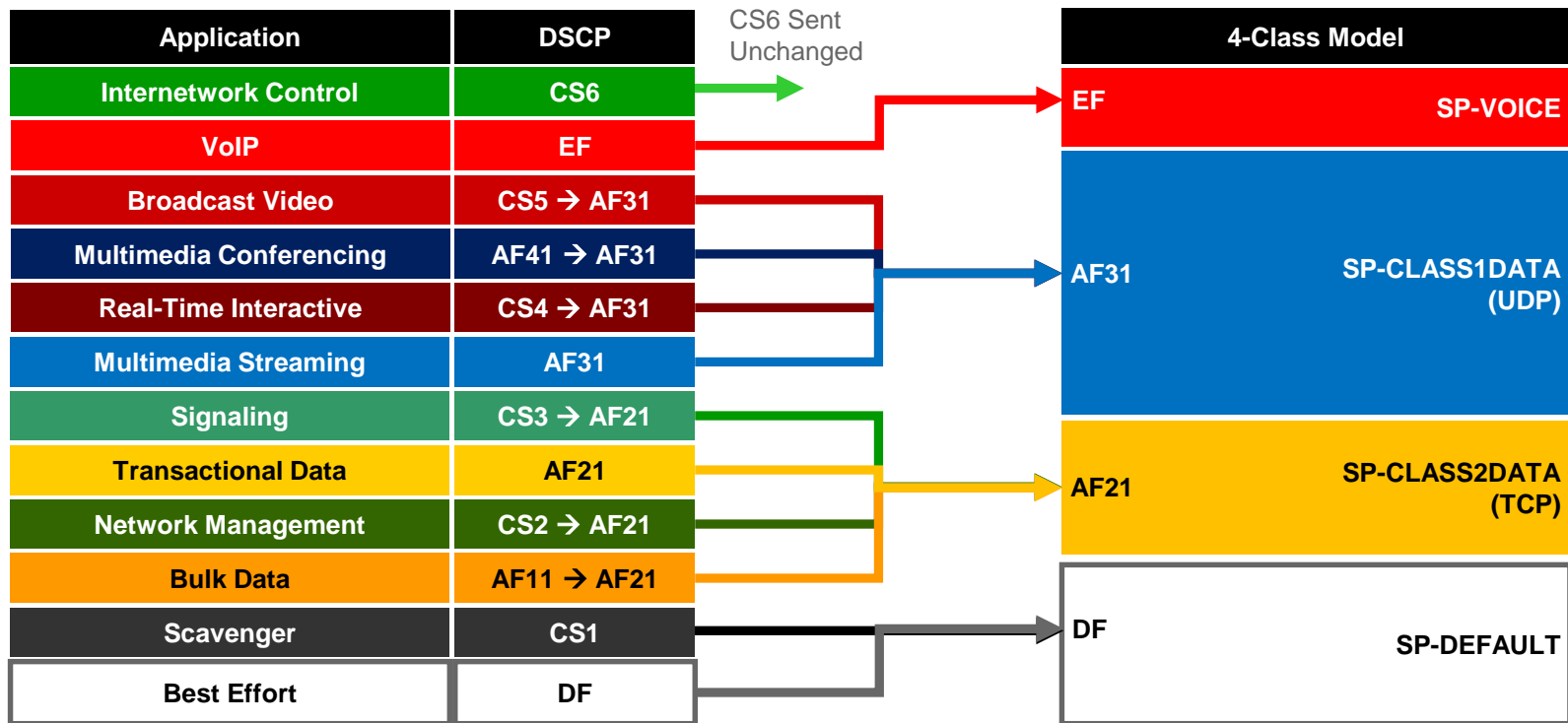
GRE Tunnel



'Set dscp tunnel' means don't copy but instead remember and mark this value once tunnel header is imposed

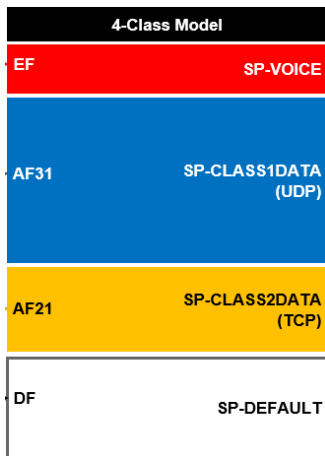
Enterprise to SP Mapping

Example: 4-Class SP Model



4-Class SP QoS Model Configuration

Tunnel Interface IWAN Hub BR



```
policy-map WAN
  class INTERACTIVE-VIDEO
    bandwidth remaining percent 30
    random-detect dscp-based
    set dscp tunnel af31
  class STREAMING-VIDEO
    bandwidth remaining percent 10
    random-detect dscp-based
    set dscp tunnel af31
  class NET-CTRL-MGMT
    bandwidth remaining percent 5
    set dscp tunnel cs6
  class CALL-SIGNALING
    bandwidth remaining percent 4
    set dscp tunnel af21
  class CRITICAL-DATA
    bandwidth remaining percent 25
    random-detect dscp-based
    set dscp tunnel af21
  class SCAVENGER
    bandwidth remaining percent 1
    set dscp tunnel default
  class VOICE
    priority level 1
    police cir percent 10
    set dscp tunnel ef
  class class-default
    bandwidth remaining percent 25
    random-detect
    set dscp tunnel default
```

Hub Router:

```
policy-map RS-GROUP-50MBPS-POLICY
  class class-default
    shape average 50000000
    bandwidth remaining ratio 50
    service-policy WAN
```

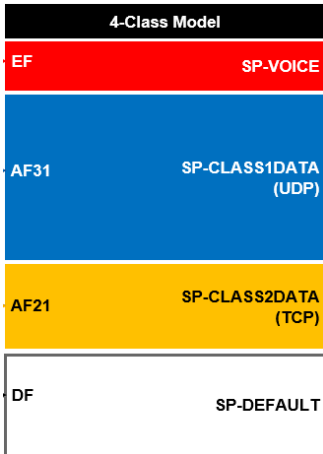
```
interface Tunnel10
  description Service Provider X
  nhrp map group RS-GROUP-50MBPS service-policy
  output RS-GROUP-50MBPS-POLICY
```

Branch Router:

```
interface GigabitEthernet0/0
  bandwidth 50000
  service-policy output POLICY-TRANSPORT-1
!
interface Tunnel10
  bandwidth 50000
  nhrp group RS-GROUP-50MBPS
  tunnel source GigabitEthernet0/0
  tunnel vrf IWAN-TRANSPORT-1
```

4-Class SP QoS Model Configuration

Physical Interface *IWAN Branch*



```
policy-map WAN
  class INTERACTIVE-VIDEO
    bandwidth remaining percent 30
    random-detect dscp-based
    set dscp af31
  class STREAMING-VIDEO
    bandwidth remaining percent 10
    random-detect dscp-based
    set dscp af31
  class NET-CTRL-MGMT
    bandwidth remaining percent 5
    set dscp cs6
  class CALL-SIGNALING
    bandwidth remaining percent 4
    set dscp af21
  class CRITICAL-DATA
    bandwidth remaining percent 25
    random-detect dscp-based
    set dscp af21
  class SCAVENGER
    bandwidth remaining percent 1
    set dscp default
  class VOICE
    priority level 1
    police cir percent 10
    set dscp ef
  class class-default
    bandwidth remaining percent 25
    random-detect
```

Branch Router:

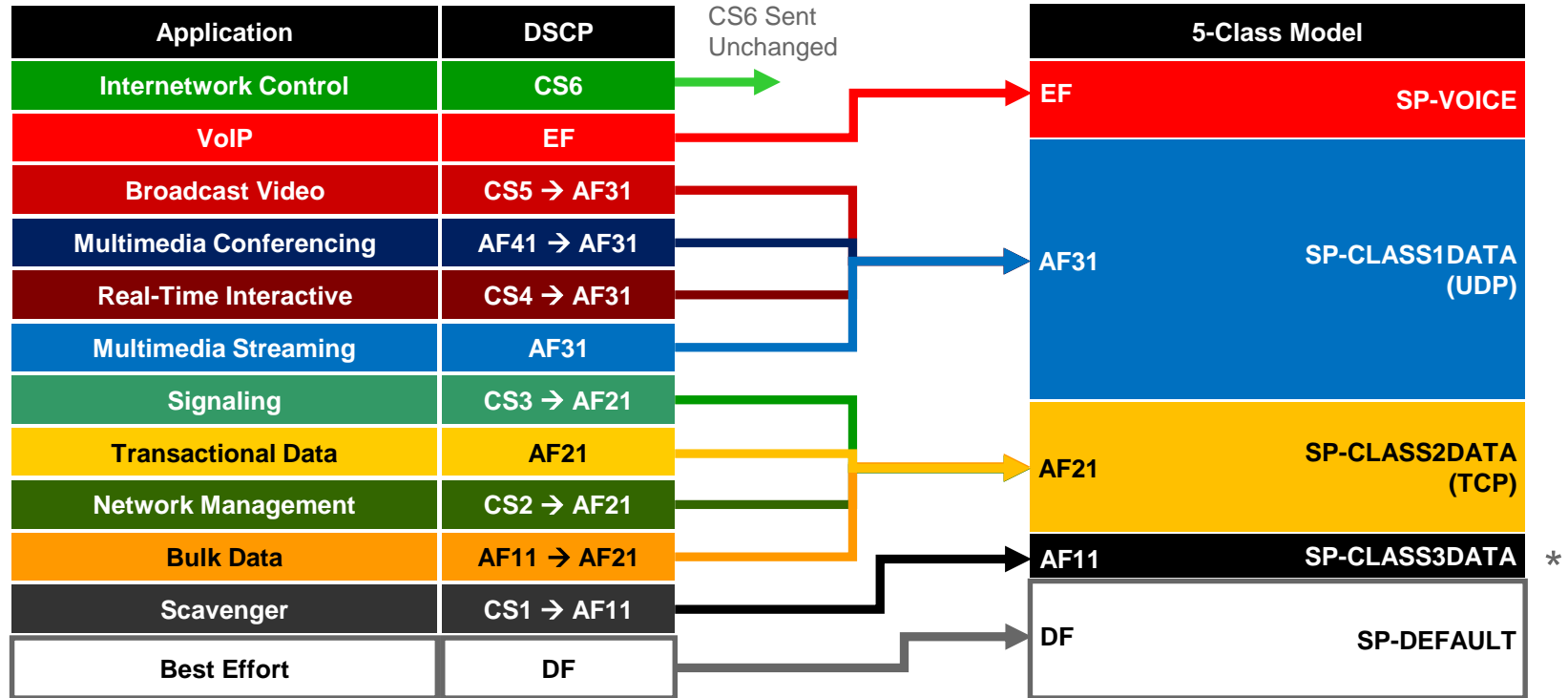
```
policy-map POLICY-TRANSPORT-1
  class class-default
    shape average 5000000
    service-policy WAN
```

```
interface GigabitEthernet0/0
  description Service Provider X
  service-policy output POLICY-TRANSPORT-1
```

QoS Mapping

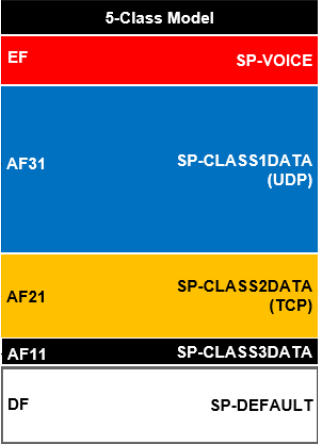
Example: 5-Class SP Model

Reference



5-Class QoS Model Configuration

Physical Interface *IWAN Branch*



```

policy-map WAN
  class INTERACTIVE-VIDEO
    bandwidth remaining percent 30
    random-detect dscp-based
    set dscp af31
  class STREAMING-VIDEO
    bandwidth remaining percent 10
    random-detect dscp-based
    set dscp af31
  class NET-CTRL-MGMT
    bandwidth remaining percent 5
    set dscp cs6
  class CALL-SIGNALING
    bandwidth remaining percent 4
    set dscp af21
  class CRITICAL-DATA
    bandwidth remaining percent 25
    random-detect dscp-based
    set dscp af21
  class SCAVENGER
    bandwidth remaining percent 1
    set dscp af11
  class VOICE
    priority level 1
    police cir percent 10
    set dscp tunnel ef
  class class-default
    bandwidth remaining percent 25
    random-detect
    set dscp tunnel default
  
```

Branch Router:

```

policy-map POLICY-TRANSPORT-1
  class class-default
    shape average 50000000
    service-policy WAN
  
```

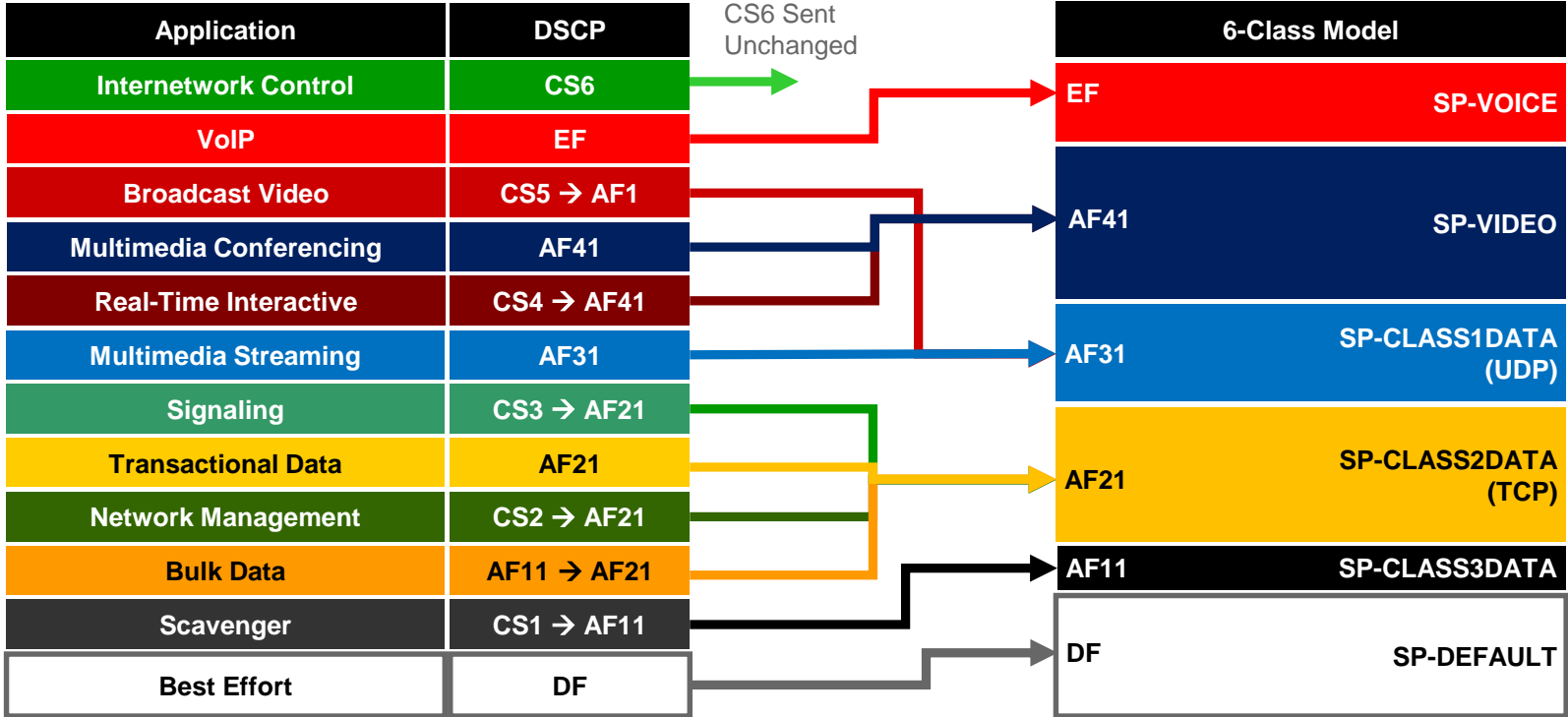
```

interface GigabitEthernet0/0
  description Service Provider
  service-policy output POLICY-TRANSPORT-1
  
```



Enterprise to SP Mapping

Example: 6-Class SP Model



* - Specified by ISP

6-Class QoS Model Configuration

Reference

Physical Interface *IWAN Branch*

6-Class Model	
EF	SP-VOICE
AF41	SP-VIDEO
AF31	SP-CLASS1DATA (UDP)
AF21	SP-CLASS2DATA (TCP)
AF11	SP-CLASS3DATA
DF	SP-DEFAULT

```
policy-map WAN
  class INTERACTIVE-VIDEO
    bandwidth remaining percent 30
    random-detect dscp-based
    set dscp af41
  class STREAMING-VIDEO
    bandwidth remaining percent 10
    random-detect dscp-based
    set dscp af31
  class NET-CTRL-MGMT
    bandwidth remaining percent 5
    set dscp cs6
  class CALL-SIGNALING
    bandwidth remaining percent 4
    set dscp af21
  class CRITICAL-DATA
    bandwidth remaining percent 25
    random-detect dscp-based
    set dscp af21
  class SCAVENGER
    bandwidth remaining percent 1
    set dscp af11
  class VOICE
    priority level 1
    police cir percent 10
    set dscp ef
  class class-default
    bandwidth remaining percent 25
    random-detect
```

Branch Router:

```
policy-map POLICY-TRANSPORT-1
  class class-default
    shape average 5000000
    service-policy WAN
```

```
interface GigabitEthernet0/0
  description Service Provider X
  service-policy output POLICY-TRANSPORT-1
```

CiscoLive!

Enterprise to SP Mapping: Summary

Application Class	Per-Hop Behavior	Queuing & Dropping	12-Class	8-Class For IWAN Router	6-Class For Tunnel	5-class For Tunnel	4-Class For Tunnel
Internetwork Control	CS6	BR Queue	Net-Ctrl	NET-CTRL	CS6	CS6	CS6
VoIP Telephony	EF	Priority Queue (PQ)	Voice	VOICE	EF	EF	EF
Multimedia Conferencing	AF4	BR Queue + DSCP WRED	Interactive-Video	INTERACTIVE-VIDEO	AF41	AF31	AF31
Real-Time Interactive	CS4	BR Queue + DSCP WRED	Real-Time	INTERACTIVE-VIDEO	AF41	AF31	AF31
Broadcast Video	CS5	BR Queue + DSCP WRED	Broadcast-Video	STREAMING-VIDEO	AF31	AF31	AF31
Multimedia Streaming	AF3	BR Queue + DSCP WRED	Streaming-Video	STREAMING-VIDEO	AF31	AF31	AF31
Signaling	CS3	BR Queue	Call-Signaling	CALL-SIGNALING	AF21	AF21	AF21
Ops / Admin / Mgmt	CS2	BR Queue + DSCP WRED	Net-Mgmt	CRITICAL-DATA	AF21	AF21	AF21
Transactional Data	AF2	BR Queue + DSCP WRED	Transactional-Data	CRITICAL-DATA	AF21	AF21	AF21
Bulk Data	AF1	BR Queue + DSCP WRED	Bulk-Data	CRITICAL-DATA	AF21	AF21	AF21
Best Effort	DF	BR Queue + RED	Default	DEFAULT	Default	Default	Default
Scavenger	CS1	Min BR Queue	Scavenger	SCAVENGER	AF11	AF11	Default

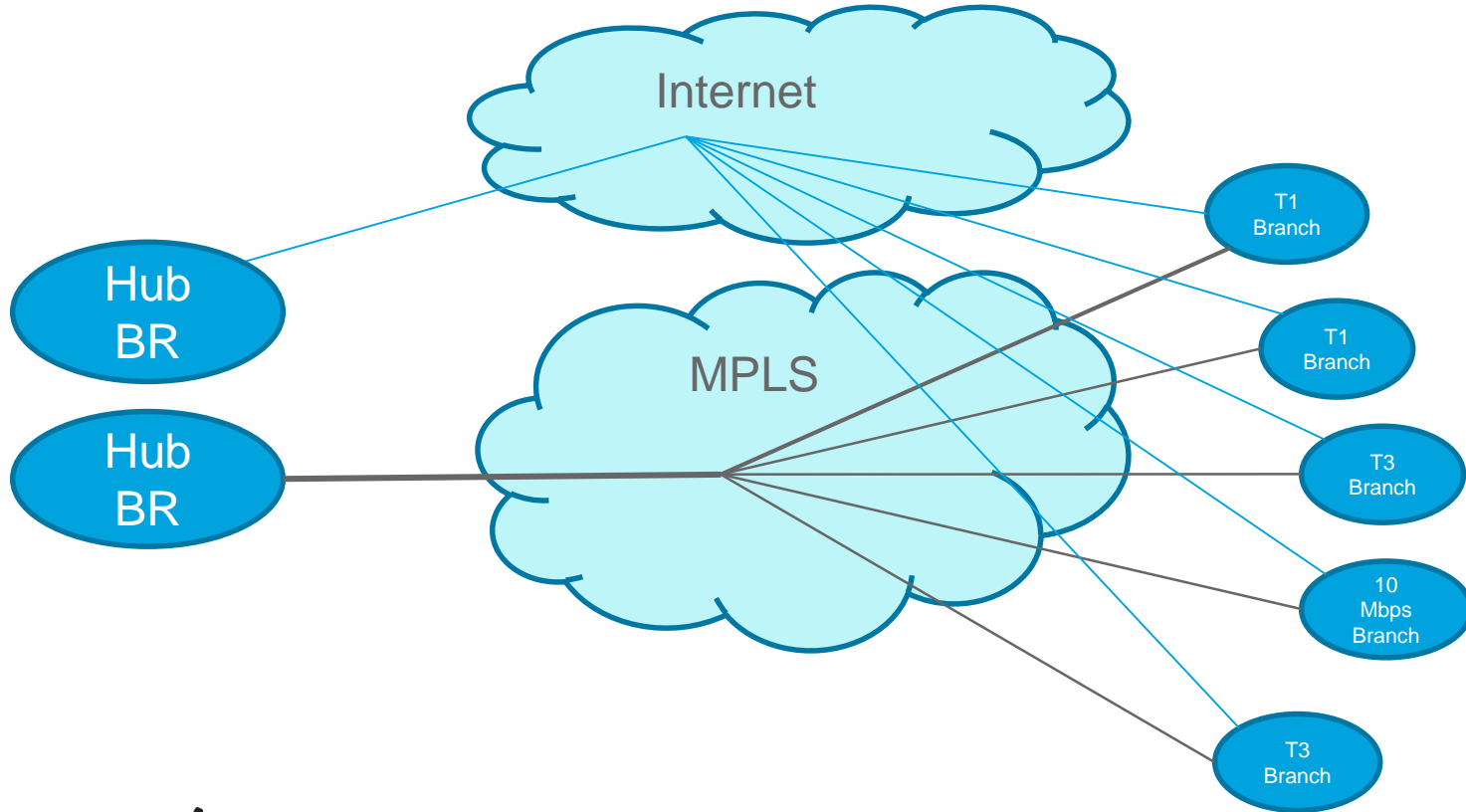
IWAN-Specific Considerations

What is IWAN from a QoS Perspective?

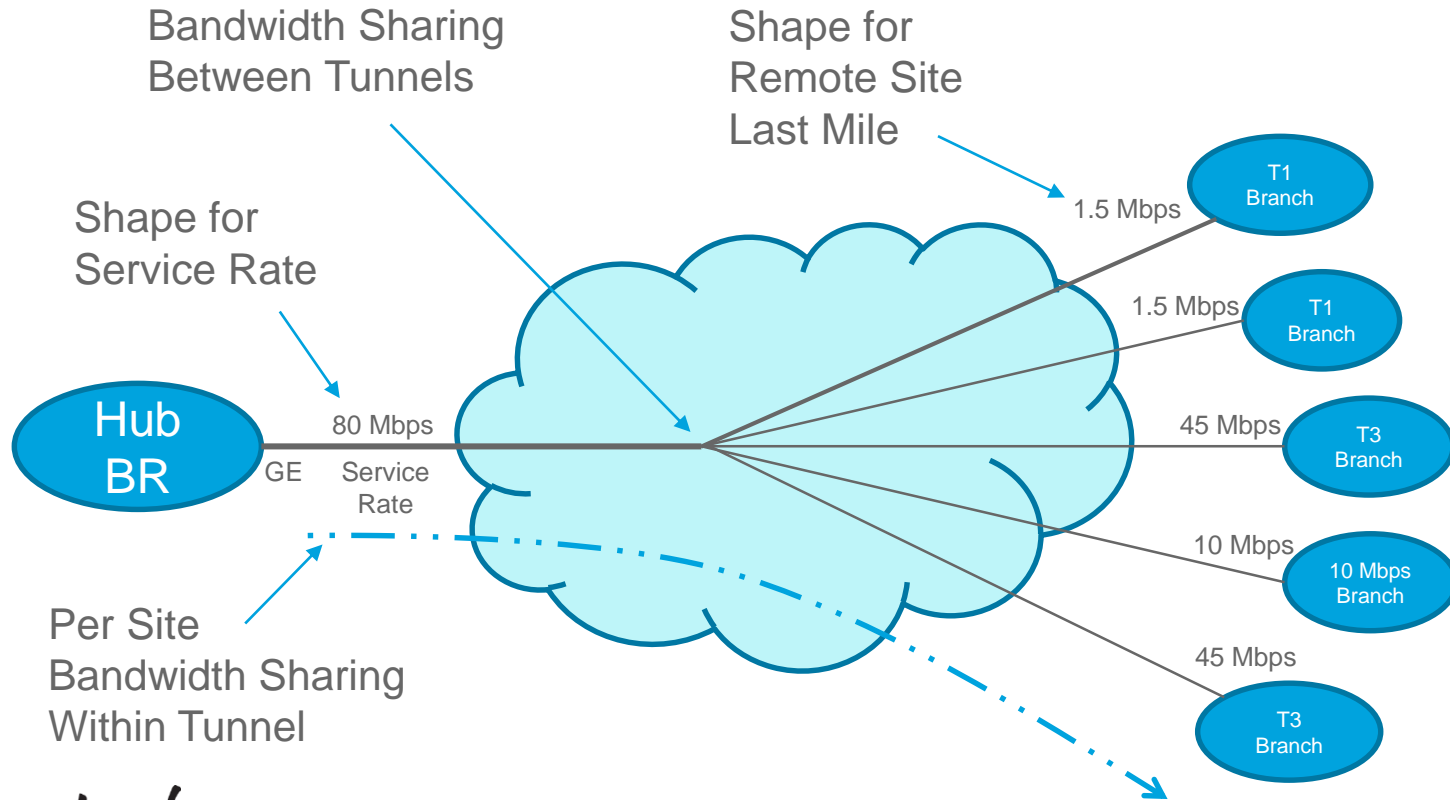
- Replacing expensive MPLS service with business class internet
- PfR to load balance / provide resiliency / best path
- DMVPN overlay on MPLS and Internet
- Up to 2,000 remote sites per hub router in a single domain
- MPLS will have SP QoS, but with Internet we assume none



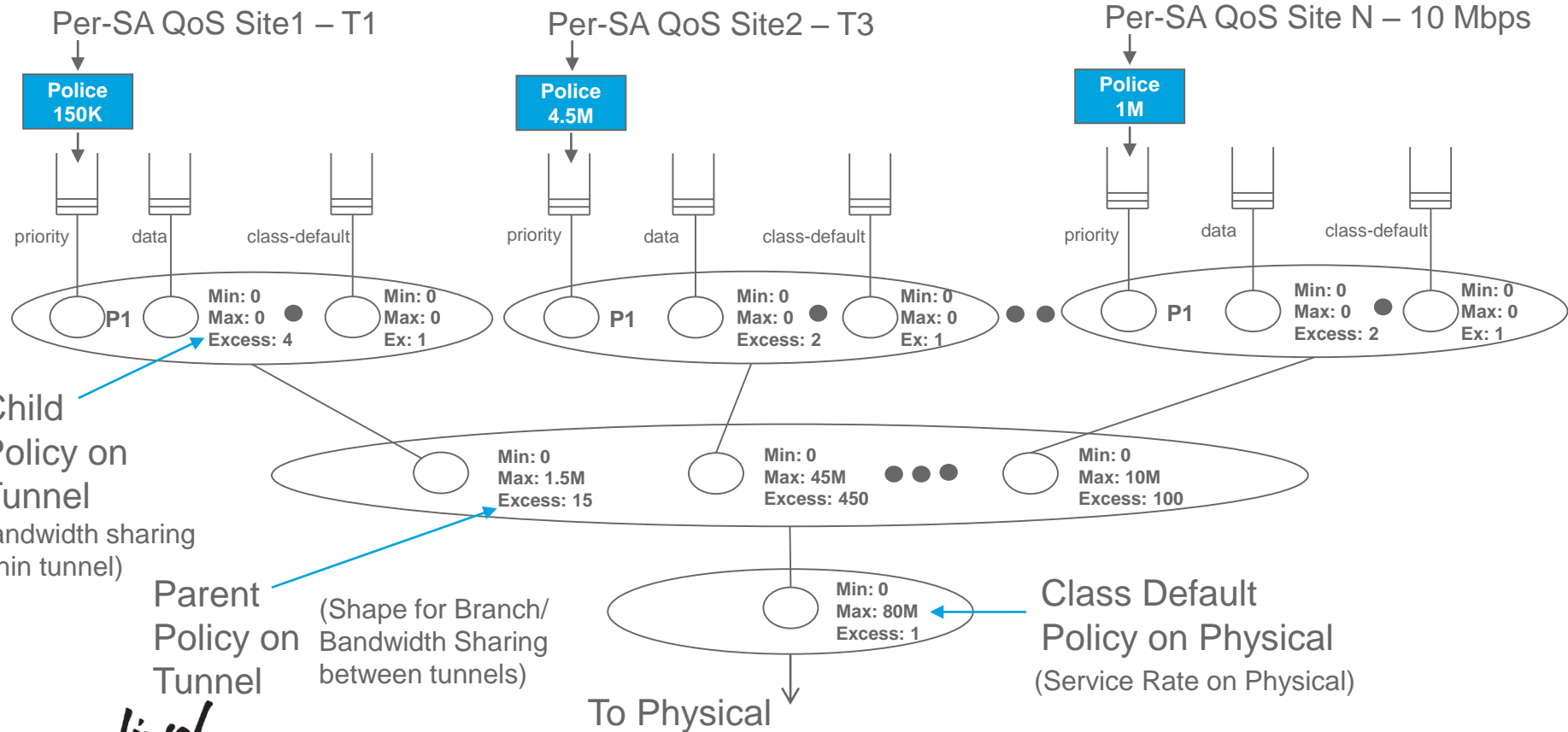
Hybrid Model – MPLS and Internet



Hub Site QoS Scheduling Requirements

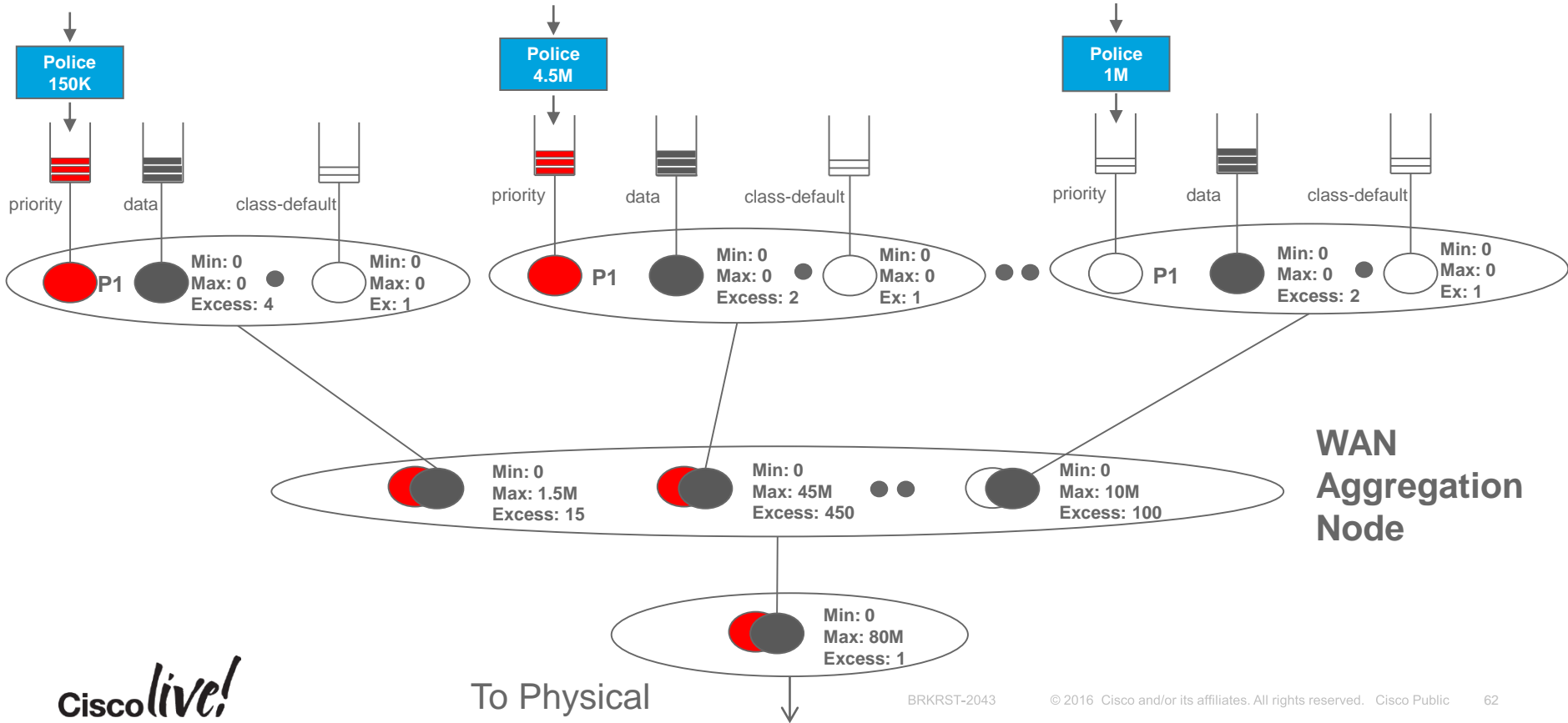


Hub Site QoS Scheduling Hierarchy We Have Today



Aggregate Priority Load

Priority Propagation / Passing Lanes



Aggregate Priority Load

IWAN Details

- IWAN supports 2,000 remote sites in a single domain
- Consider an average 2 Mbps access rate for remote sites – Aggregate: 4 Gbps
- On a GE connected Hub BR, we are already 4:1 oversubscribed
- If service-rate is less than GE (likely – say 500 Mbps) the oversubscription increases to 8:1

- An Aggregate Priority Load greater than Service Rate will starve non-Priority (including network control)

- Voice at 10% – Potential aggregate voice = 400 Mbps (10% of 4 Gbps sum of shapers)
- Always On Policer for Voice means we stay under the service rate
- Conditional Policer means individual sites could send more and over run the service rate

- Realtime Interactive – Another 27% of Priority queue ($30\% * .90$)
- Potential Aggregate Priority Load – 37% of 4 Gbps = 1.48 Gbps (Greater than access rate)
- If these are Cisco Adaptive Video codecs that ‘Like’ to grow => your risk is greater

Aggregate Priority Load

IWAN Conclusion

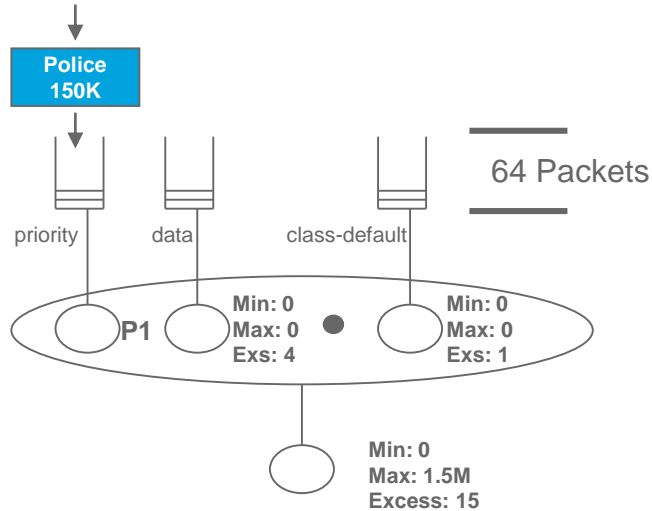
- For Voice, use an Always On policer, rather than a Conditional policer

```
class VOICE
  priority level 1
  police cir percent 10
```

- For Video, use a Bandwidth Remaining Percent queue, rather than a level 2 Priority queue

```
class INTERACTIVE-VIDEO
  bandwidth remaining percent 30
  random-detect dscp-based
```


Latency for 'Low Speed' Sites



- Bandwidth remaining percent means each queue gets a queue limit as if it had full bandwidth of parent (means high speed links will buffer 0.5 sec of data)
- Queue-Limit = $(\text{Intf Speed} * .05) / 8 / 1500$
- Anything less than 15M service rate gets 64 packets
- Aggregate T1: ~1.5 Sec of buffering IMIX
(12 queues * 64 packets * 8 bits * 350 bytes / 1.5M)

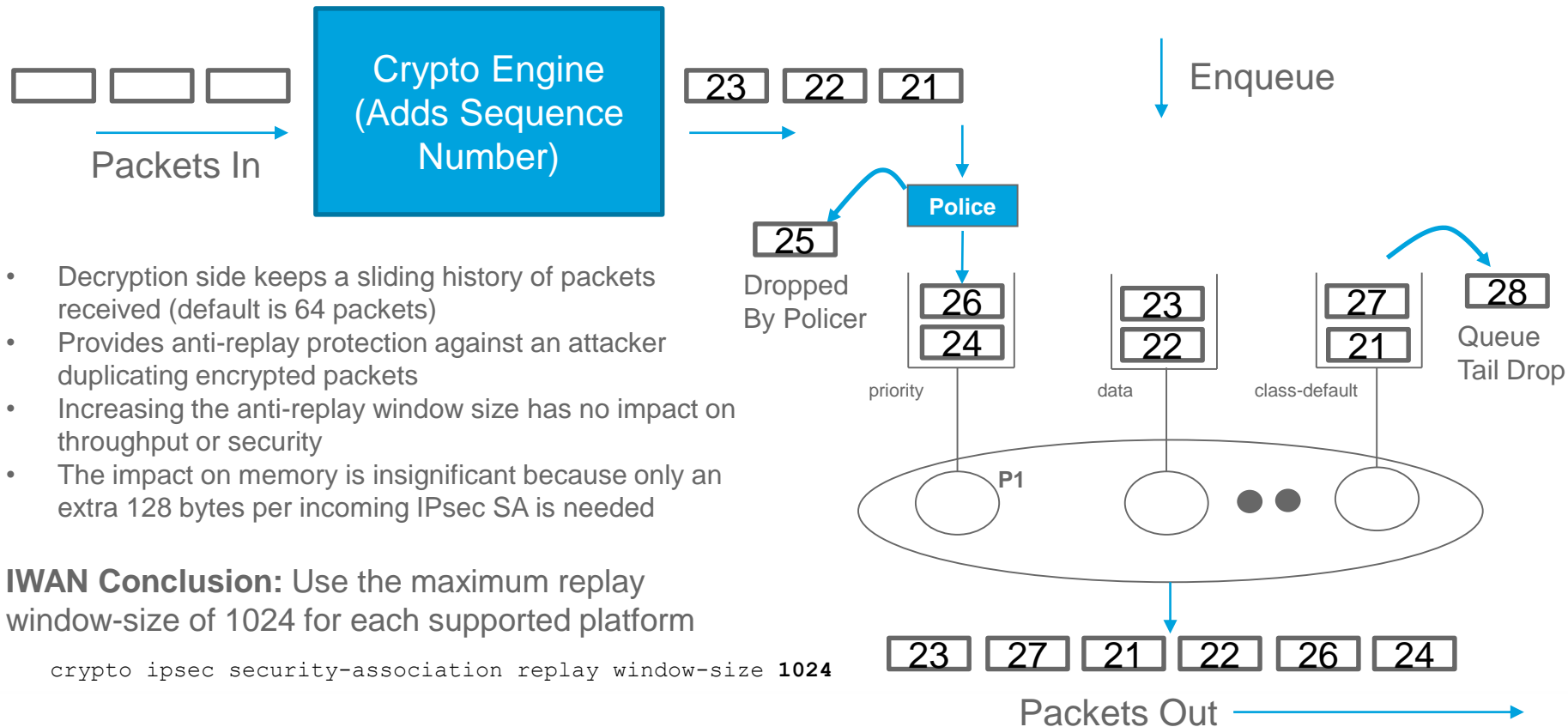
IWAN Conclusion: Use appropriate number of queues for the 12 classes on the WAN depending in your service rate

Example:

- 4 queues for service rate < 5 Mbps
- 8 queues for service rate => 5 Mbps and < 100 Mbps
- 12 queues for service rate => 100 Mbps

Traffic Type / Percentage	Service Rate	Drain 64 - 350 Byte Packets	Drain 64 - 1500 Byte Packets
Transactional Data / 10%	150K	1.2 secs	5 secs
Bulk Data / 4%	60K	3 secs	13 secs
Network Control / 2%	30K	6 secs	26 secs

IPSec Anti-Replay



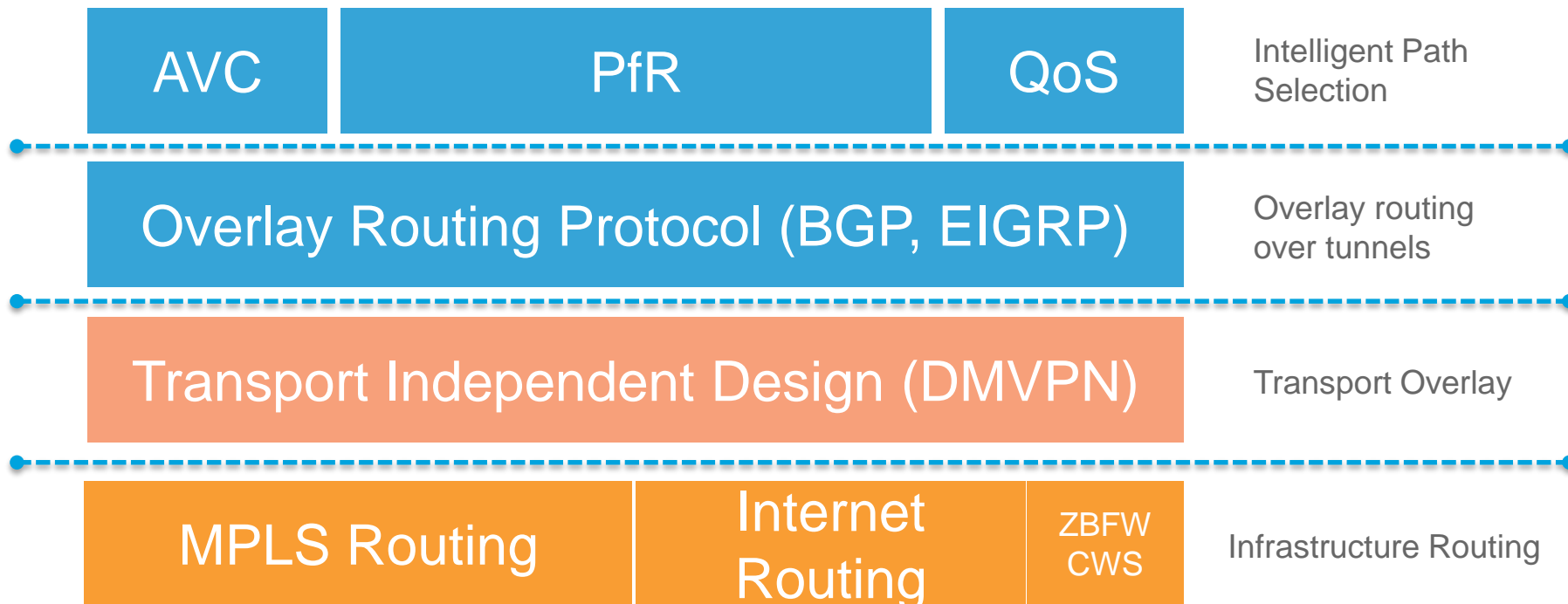
- Decryption side keeps a sliding history of packets received (default is 64 packets)
- Provides anti-replay protection against an attacker duplicating encrypted packets
- Increasing the anti-replay window size has no impact on throughput or security
- The impact on memory is insignificant because only an extra 128 bytes per incoming IPsec SA is needed

IWAN Conclusion: Use the maximum replay window-size of 1024 for each supported platform

```
crypto ipsec security-association replay window-size 1024
```

PfR and QoS Interaction

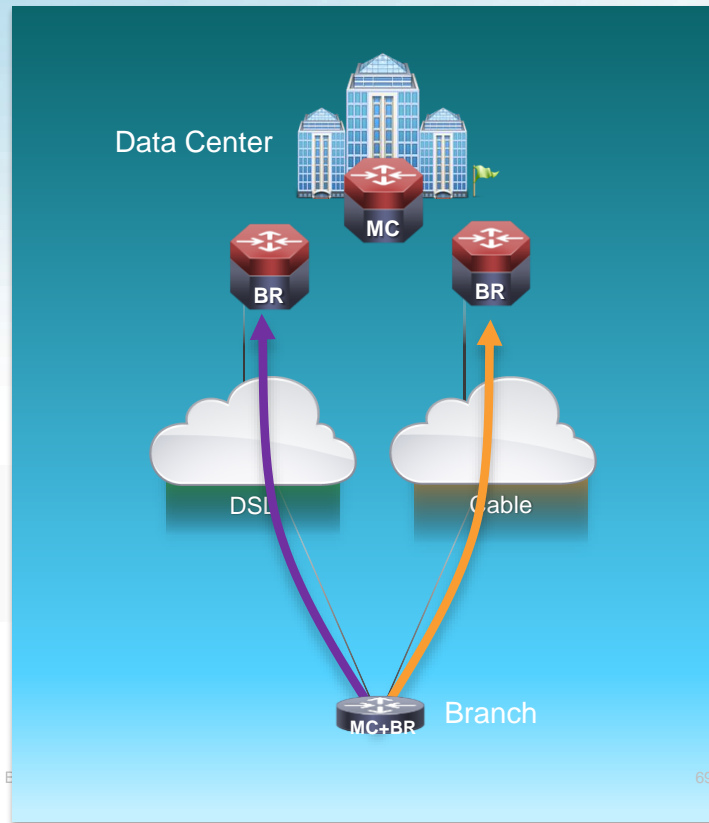
IWAN Layers



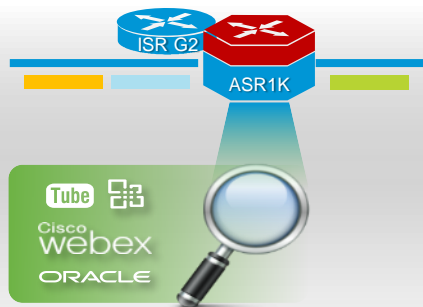
What is Performance Routing (PfR)?

“**Performance Routing (PfR)** provides additional intelligence to classic routing to track and verify the performance quality of a path between two devices over a Wide Area Networking (WAN) to determine the best path for application traffic....”

- Cisco IOS technology
- Two components: Master Controller , Border Router



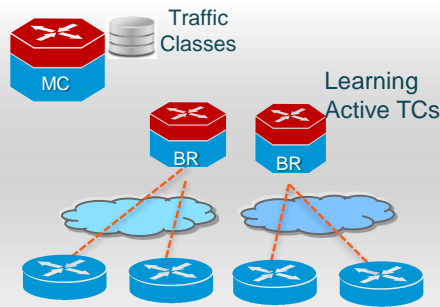
PfRv3 – How it Works



Define your Traffic Policy

Define path optimization policies on the Hub MC
load balancing,
path preference, application metrics

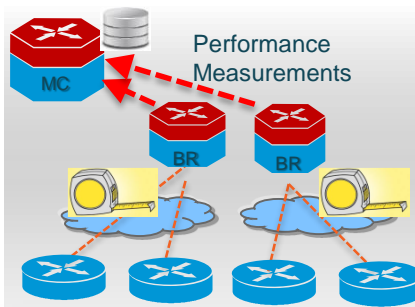
DSCP Based Policies
Application Based Policies



Learn the Traffic

Traffic flowing through the Border Routers (BRs) that match a policy are learned Traffic Classes

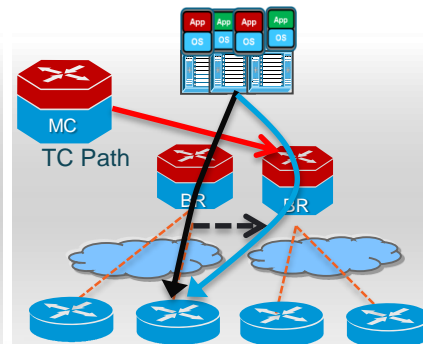
Unified Performance Monitor



Measurement

Report the measured TC performance metrics to the Master Controller for policy compliance

Unified Performance Monitor



Path Enforcement

Master Controller directs BR path changes to keep traffic within policy

Route Enforcement module in feature path



IWAN Design – PfR Policy

```
domain IWAN
vrf default
  master hub
  load-balance
  class VOICE sequence 10
    match dscp ef policy voice
    path-preference MPLS fallback INET
  class INTERACTIVE_VIDEO sequence 20
    match dscp cs4 policy real-time-video
    match dscp af41 policy real-time-video
    match dscp af42 policy real-time-video
    match dscp af43 policy real-time-video
    path-preference MPLS fallback INET
  class LOW_LATENCY_DATA sequence 30
    match dscp cs2 policy low-latency-data
    match dscp cs3 policy low-latency-data
    match dscp af21 policy low-latency-data
    match dscp af22 policy low-latency-data
    match dscp af23 policy low-latency-data
    path-preference MPLS fallback INET
```

```
class BULK_DATA sequence 40
  match dscp af11 policy bulk-data
  match dscp af12 policy bulk-data
  match dscp af13 policy bulk-data
  path-preference MPLS fallback INET
class SCAVENGER sequence 50
  match dscp cs1 policy scavenger
  path-preference INET fallback MPLS
class DEFAULT sequence 60
  match dscp default policy best-effort
  path-preference INET fallback MPLS
```

- Create the PfR classes with matching policy names and DSCP values to simplify the configuration
- Define the path preference for traffic
- Load balance non-priority traffic

Built-in Policy Templates

Pre-defined Template	Threshold Definition
Voice	priority 1 one-way-delay threshold 150 threshold 150 (msec) priority 2 packet-loss-rate threshold 1 (%) priority 2 byte-loss-rate threshold 1 (%) priority 3 jitter 30 (msec)
Real-time-video	priority 1 packet-loss-rate threshold 1 (%) priority 1 byte-loss-rate threshold 1 (%) priority 2 one-way-delay threshold 150 (msec) priority 3 jitter 20 (msec)
Low-latency-data	priority 1 one-way-delay threshold 100 (msec) priority 2 byte-loss-rate threshold 5 (%) priority 2 packet-loss-rate threshold 5 (%)

Pre-defined Template	Threshold Definition
Bulk-data	priority 1 one-way-delay threshold 300 (msec) priority 2 byte-loss-rate threshold 5 (%) priority 2 packet-loss-rate threshold 5 (%)
Best-effort	priority 1 one-way-delay threshold 500 (msec) priority 2 byte-loss-rate threshold 10 (%) priority 2 packet-loss-rate threshold 10 (%)
Scavenger	priority 1 one-way-delay threshold 500 (msec) priority 2 byte-loss-rate threshold 50 (%) priority 2 packet-loss-rate threshold 50 (%)

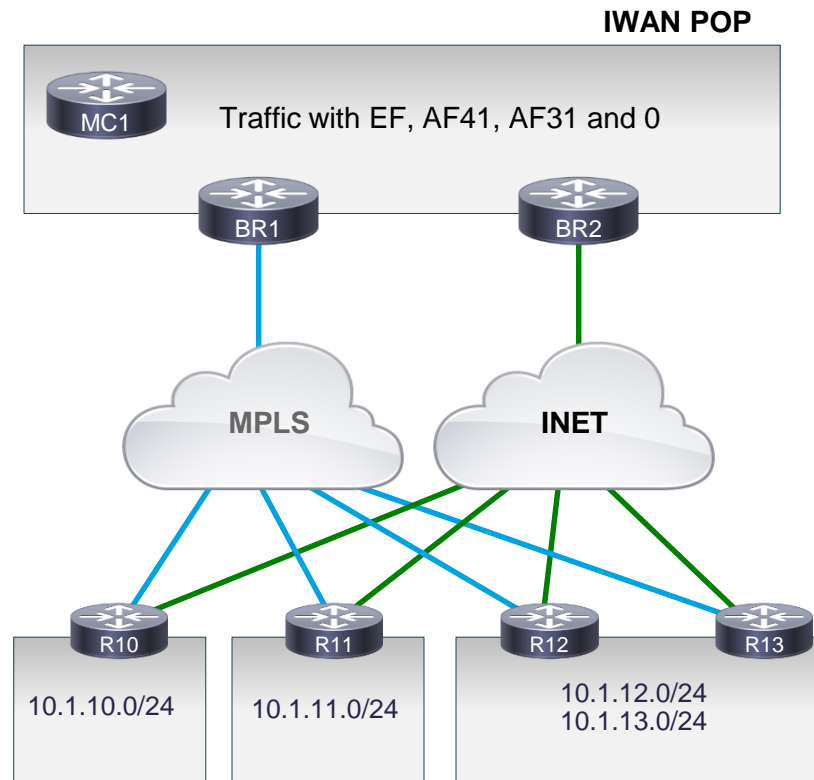
PfR Manages Traffic Class

Prefix	DSCP	AppID	Dest Site	Next-Hop
10.1.11.0/24	EF	N/A	Site 11	?
10.1.11.0/24	AF41	N/A	Site 11	?
10.1.11.0/24	AF31	N/A	Site 11	?
10.1.11.0/24	0	N/A	Site 11	?
10.1.10.0/24	EF	N/A	Site 10	?
10.1.10.0/24	AF41	N/A	Site 10	?
10.1.10.0/24	AF31	N/A	Site 10	?
10.1.10.0/24	0	N/A	Site 10	?

Traffic Class

- Destination Prefix
- DSCP Value
- Application (N/A when DSCP policies used)

Cisco *live!*



SD-WAN QoS APIC-EM IWAN App

APIC-EM – IWAN App

The screenshot displays the APIC-EM Enterprise Module interface. The top navigation bar includes the Cisco logo, 'APIC - Enterprise Module', and user information 'API', '\$', 'admin', and a settings icon. A sidebar on the left contains navigation icons. The main content area features three blue panels:

- Update Hub Site & Settings:** Status 'Configured' with a green checkmark and a progress bar. It shows '0 Scheduled Job(s)'. A circular icon on the left depicts a hub site connected to two branch sites.
- Administer Application Policy:** Shows '8 Business Category(s)', '7 Scavenger Category(s)', and '2 Default Category(s)'. It also shows '0 Scheduled Job(s)'. A circular icon on the left depicts a pie chart.
- Set up Branch Sites:** Shows '0 Unclaimed Device(s)' and '3 Site(s)'. It also shows '0 Scheduled Job(s)'. A circular icon on the left depicts three server racks.

A central circular callout box contains the text: 'Hub site is ready. Manage branch sites.' Below this, it lists: '2 Provisioned', '1 In-Progress', and '0 Failed'. At the bottom left, it says 'Page loaded in 330ms'. At the bottom right, there is a feedback icon and the text 'I wish this page would...'.



Click see/change application policies

IWAN App – Categorize Applications

Categorize applications
Add custom applications

APIC - Enterprise Module

Application Policy

Categorize Applications

Category	Count
voice-and-video	35
consumer-streaming	20
business-and-product...	18
file-sharing	11
consumer-file-sharin...	10

Top 5 Application Categories

Define Application Policy

Apply Changes

Add Application

Applications can be dragged and dropped to other categories; By default not all the applications are shown. Not all Categories are shown by default, [Show](#) hidden categories.

Category	Count
backup-and-storage	0
consumer-internet	10
email	9
instant-messaging	7
voice-and-video	35
browsing	
consumer-messaging	
epayment	
other	

Add Application

* Name: My-Custom-App1

Type: URL Server IP/Port DSCP

Protocol: UDP TCP

* Value: 172.16.3.2 : 5500

* Similar to App: sip-tls

* Category: voice-and-video

Jitter(ms): 1

Packet loss(%): 5

Delay(ms): 100

Add Cancel

Page loaded in 296ms

I wish this page would..

IWAN App – Categorize Applications

Application Policy

Categorize Applications

Category	Count
voice-and-video	35
consumer-streaming	20
business-and-product...	18
file-sharing	11
consumer-file-sharin...	10

Top 5 Application Categories

Define Application Policy

Business Critical Scavenger Default

Apply Changes

Add Application

Search Apps

Applications can be dragged and dropped to other categories; By default not all the applications are visible, you can make them visible [Teach me](#).
Not all Categories are shown by default, [Show](#) hidden categories.

Category	Count
backup-and-storage	4
consumer-internet	6
email	9
instant-messaging	7
voice-and-video	35
browsing	6
consumer-messaging	7
epayment	0
other	10
business-and-productivity-tools	18
consumer-streaming	20
file-sharing	11
social-networking	7
consumer-file-sharing	10
database	3
gaming	1
software-updates	9

voice-and-video details:

Name	Category
yahoo-messenger-video	voice-and-video
webex-app-sharing	voice-and-video
ms-lync	voice-and-video

Drag and drop each application (one or more) from one business class to the other

IWAN App – Define Application Policy

APIC - Enterprise Module

API [Settings] [User: HI, admin]

Application Policy

Categorize Applications

Category	Count
consumer_apps	48
voice-and-video...	28
business-and-pr...	18
other	17
file-sharing	12

Top 5 Application Categories

Define Application Policy

Apply Changes

Legend: Business Critical (Green), Scavenger (Grey), Default (Blue)

Business Critical

- business-and-prod... [mpls]
- email [mpls]
- software-updates [mpls]
- voice-and-video [mpls]
- database [mpls]
- file-sharing [mpls]
- browsing [mpls]
- backup-and-storage [mpls]

Scavenger

- gaming [No App Performance]
- consumer_apps [No App Performance]
- instant-messaging [No App Performance]
- social-networking [No App Performance]

Default

- other [No App Performance]

Application Performance: Application Performance

No path preference

Path Preference

Path 1: [inet]

Path 2: [mpls]

Save [Drop]

Page loaded in 31ms

I wish this page would...

Drag and Drop a business category among: business critical | scavenger | default

Application priority policy setting in IWAN app

- Path preference: Set primary and action on threshold crossing, which can be a second path or drop traffic
- Drag and drop business buckets

IWAN-App QoS Config

Classification and Marking Policy

Business-Irrelevant Class-Map (List of Categories that are Business-Irrelevant)

```
class-map match-any prm-biz-irrelevant-cats
match protocol attribute category consumer-file-sharing
match protocol attribute category consumer-messaging
match protocol attribute category consumer-internet
match protocol attribute category consumer-streaming
match protocol attribute category gaming
match protocol attribute category social-networking
match protocol attribute category instant-messaging
```

RFC 4594-Based Marking Policy-Map

```
policy-map prm-nbar-12-cls
class prm-nbar-12-cls#VOICE
set dscp ef
class prm-nbar-12-cls#BROADCAST-VIDEO
set dscp cs5
class prm-nbar-12-cls#INTERACTIVE-VIDEO
set dscp cs4
class prm-nbar-12-cls#MULTIMEDIA-CONFERENCING
set dscp af41
class prm-nbar-12-cls#MULTIMEDIA-STREAMING
set dscp af31
class prm-nbar-12-cls#SIGNALING
set dscp cs3
class prm-nbar-12-cls#NETWORK-CONTROL
set dscp cs6
class prm-nbar-12-cls#NETWORK-MANAGEMENT
set dscp cs2
class prm-nbar-12-cls#TRANSACTIONAL-DATA
set dscp af21
class prm-nbar-12-cls#BULK-DATA
set dscp af11
class prm-nbar-12-cls#SCAVENGER
set dscp cs1
class class-default
```

Parent Class-Maps to Combine Category-Based BR with Traffic-Classes

```
class-map match-all prm-nbar-12-cls#BROADCAST-VIDEO
match protocol attribute traffic-class broadcast-video
match class-map prm-biz-relevant-cats
class-map match-all prm-nbar-12-cls#BULK-DATA
match protocol attribute traffic-class bulk-data
match class-map prm-biz-relevant-cats
class-map match-all prm-nbar-12-cls#INTERACTIVE-VIDEO
match protocol attribute traffic-class real-time-interactive
match class-map prm-biz-relevant-cats
class-map match-all prm-nbar-12-cls#NETWORK-CONTROL
match protocol attribute traffic-class network-control
match class-map prm-biz-relevant-cats
class-map match-all prm-nbar-12-cls#MULTIMEDIA-CONFERENCING
match protocol attribute traffic-class multimedia-conferencing
match class-map prm-biz-relevant-cats
class-map match-all prm-nbar-12-cls#VOICE
match protocol attribute traffic-class voip-telephony
match class-map prm-biz-relevant-cats
class-map match-all prm-nbar-12-cls#SIGNALING
match protocol attribute traffic-class signaling
match class-map prm-biz-relevant-cats
class-map match-all prm-nbar-12-cls#NETWORK-MANAGEMENT
match protocol attribute traffic-class ops-admin-mgmt
match class-map prm-biz-relevant-cats
class-map match-all prm-nbar-12-cls#TRANSACTIONAL-DATA
match protocol attribute traffic-class transactional-data
match class-map prm-biz-relevant-cats
class-map match-all prm-nbar-12-cls#MULTIMEDIA-STREAMING
match protocol attribute traffic-class multimedia-streaming
match class-map prm-biz-relevant-cats
class-map match-all prm-nbar-12-cls#SCAVENGER
match class-map prm-biz-irrelevant-cats
```

Business-Relevant Class-Map (List of Categories that are Business-Relevant)

```
class-map match-any prm-biz-relevant-cats
match protocol attribute category business-and-productivity-tools
match protocol attribute category voice-and-video
match protocol attribute category backup-and-storage
match protocol attribute category software-updates
match protocol attribute category file-sharing
match protocol attribute category email
match protocol attribute category database
match protocol attribute category browsing
```

Implements Category-to-Business-Relevance mapping

Vs.

Application-to-Business-Relevance mapping

Summary and References

Key Takeaways

Ingress LAN Marking NBAR2 QoS Attributes

Traffic-Class
Business-Relevance

Coming in IWAN 2.2 CVD

Egress WAN Queuing QoS and App Control

WAN Queuing
Sub-Line Rate Interfaces
DMVPN Per Tunnel QoS
Enterprise to SP Mapping

IWAN 2.1 CVD

IWAN Considerations Design Issues

Aggregate Priority Load
Latency for Low Speed
IPSec Anti-Replay

IWAN 2.1 CVD



Cisco Design Guides for Intelligent WAN

IWAN Technology Design Guide
IWAN DIA and Guest Wireless Design Guide
IWAN WAAS and Akamai Design Guide

<http://www.cisco.com/go/cvd/wan>



Design Overview	Technology	Type	Design Models
WAN Design	IWAN / WAN	All	Overview
Technical Design Guide	Profile	Type	Design Models
IWAN Technology IWAN Config Files	Base	ASR 1K CSR 1K (Hub MC) ISR 4K ISR G2	Hybrid Dual Internet Single Router Dual Router Transit Site Hub BR Scaling Feb 2016
IWAN DIA and Guest	Advanced	ISR 4K	Remote Site Direct Internet Access Remote Site Guest Wireless
IWAN WAAS and Akamai	Advanced	ISR 4K	WAAS Akamai Connect

Recommended Reading



Coming
Soon

Cisco *live!*

Other IWAN Related Sessions

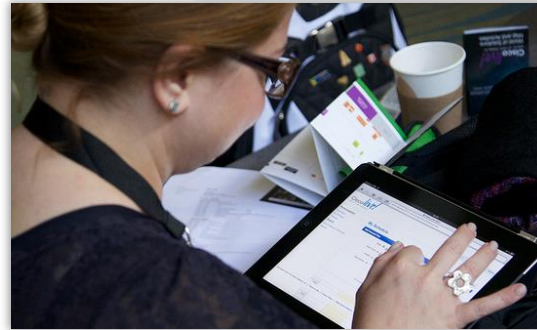
- TECCRS-2004 – Implementing the Intelligent WAN
- BRKCRS-2000 – Intelligent WAN Architecture
- BRKRST-2043 – IWAN AVC/QoS Design
- BRKRST-2362 – IWAN Implementing Performance Routing (PfRv3)
- BRKRST-2514 – Cisco Intelligent WAN (IWAN) & Application Optimization
- BRKCRS-2007 – Migrating Your Existing WAN to Cisco's IWAN
- BRKCRS-1244 – SP Virtual Managed Services (VMS) for Intelligent WAN (IWAN)
- BRKNMS-1040 – IWAN and AVC Management with Cisco Prime Infrastructure
- BRKSDN-2099 – IWAN Management via APIC-EM (SDN Controller)
- BRKARC-3004 – APIC-EM: Controller Workflow and Use Cases

Call to Action (Last session of the last day, so I hope you did it already)

- Visit the World of Solutions for
 - Cisco Campus
 - Walk in Labs
 - Technical Solution Clinics
- Meet the Engineer
- Lunch and Learn Topics
- DevNet zone related sessions

Complete Your Online Session Evaluation

- Please complete your online session evaluations after each session
- Complete 4 session evaluations & the Overall Conference Evaluation (available from Thursday) to receive your Cisco Live T-shirt
- All surveys can be completed via the Cisco Live Mobile App or the Communication Stations



Thank you



We're ready. Are you?