NETWORKERS 2004

Cisco Systems

DEPLOYING QUALITY OF SERVICE FOR CONVERGED NETWORKS

SESSION RST-2510

Agenda

- Introduction
- Deployment Guide
- Monitoring QoS
- Case Studies
- Summary

Reference Materials

- QoS Page on CCO

  http://www.cisco.com/go/qos

- QoS Configuration Guide

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/qos_vcg.htm

- Network-Based Application Recognition

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/dtnbarad.htm

- Cisco AVVID Network Infrastructure QoS Design Guide

  http://www.cisco.com/application/pdf/en/us/guest/netsol/ns17/c649/ccmigration_09186a00800d67ed.pdf

- Cisco Auto QoS

  http://www.cisco.com/warp/public/732/Tech/qos/autoqos/

- Deploying Control Plane Policing

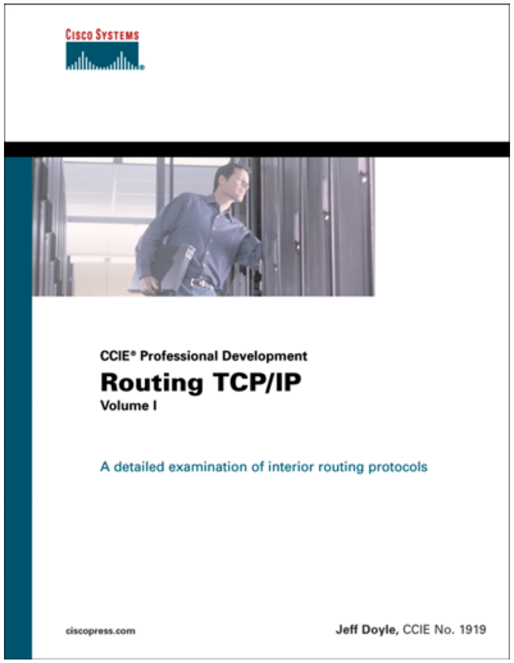
  http://www.cisco.com/warp/public/732/Tech/security/docs/copp.pdf

Associated Sessions

- **RST-1607 QoS in MPLS Networks**
- **NMS-2T30 Deploying QoS to Protect Voice, Video and Critical Data**
- **NMS-2032 NetFlow for Accounting, Analysis and Attack**
- **RST-4313 Multi Topology Routing**

Recommended Reading

- IP Quality of Service [1-57870-116-3]
- Cisco DQOS Exam Certification Guide (DQOS Exam #9E0-601 and QOS Exam #642-641) [1-58720-058-9]
- Cisco Catalyst QoS: Quality of Service in Campus Networks [1-58705-120-6]



Cisco Systems

CCIE® Professional Development

Routing TCP/IP

Volume I

A detailed examination of interior routing protocols

ciscopress.com

Jeff Doyle, CCIE No. 1919

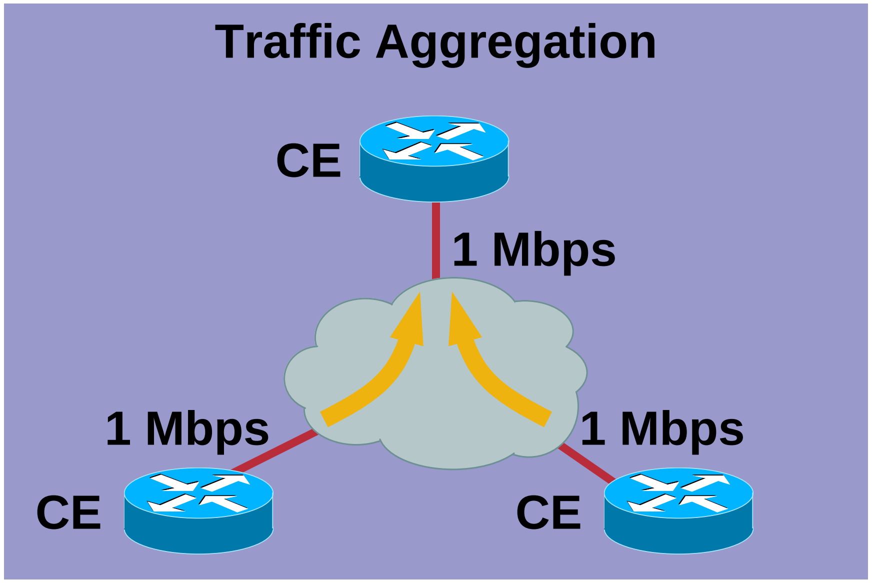
Available on-site at the Cisco Company Store

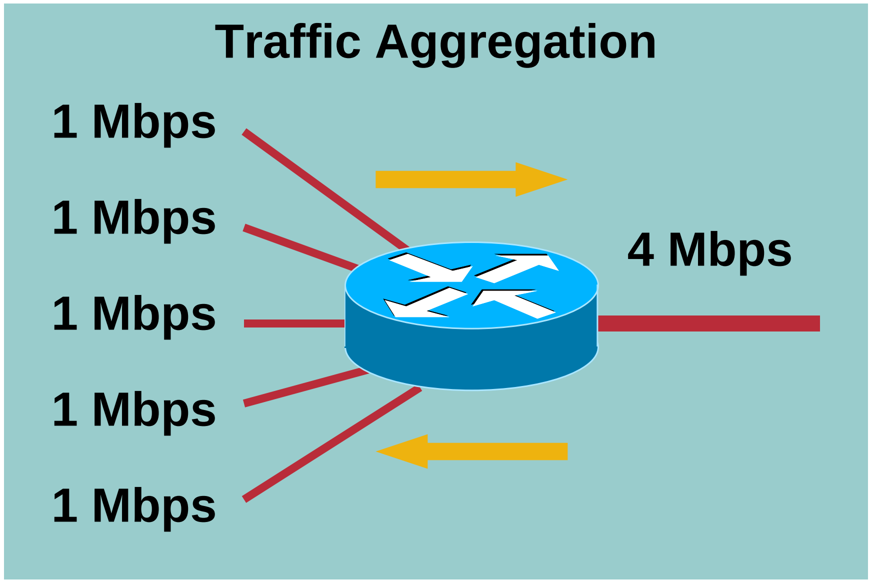
INTRODUCTION

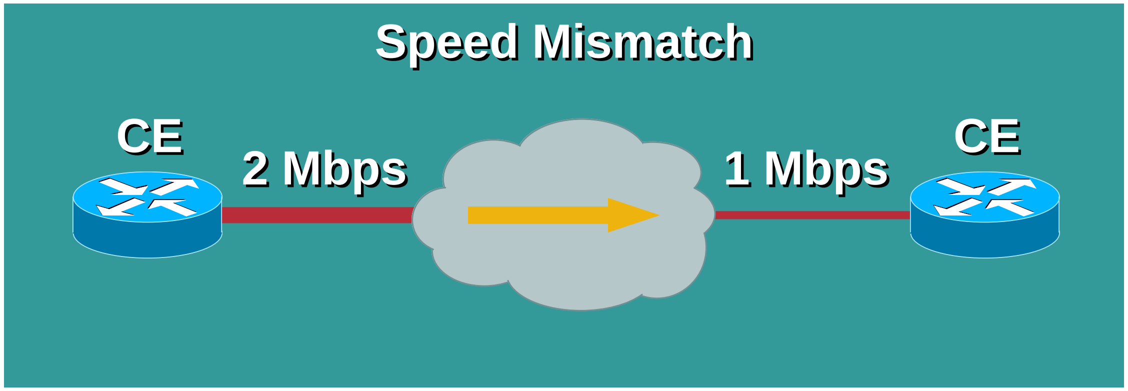
Motivation Behind QoS

- Applications are sensitive to delay, jitter and packet loss
- There are non-adjustable components (e.g. propagation delay, switching delay, CRC errors)
- There are adjustable components associated with link congestion (buffering delay and packet loss)
- Some congestion is likely in most networks
- Over-provisioning is NOT the solution
- Always good to carry an “insurance” policy

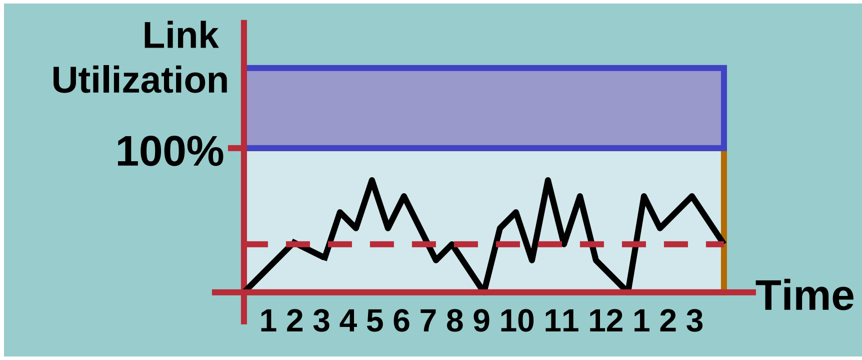
Congestion Scenarios



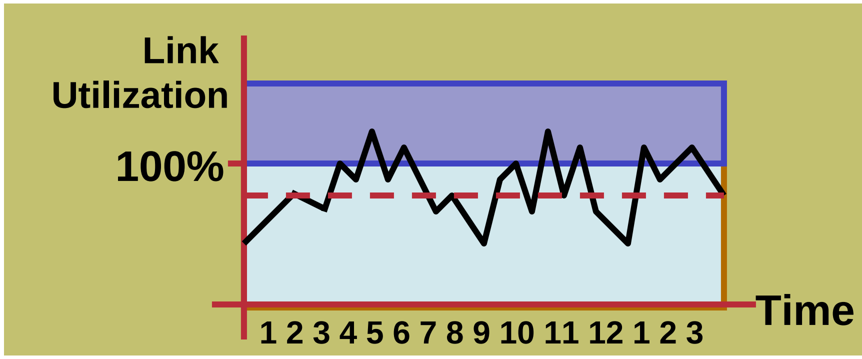




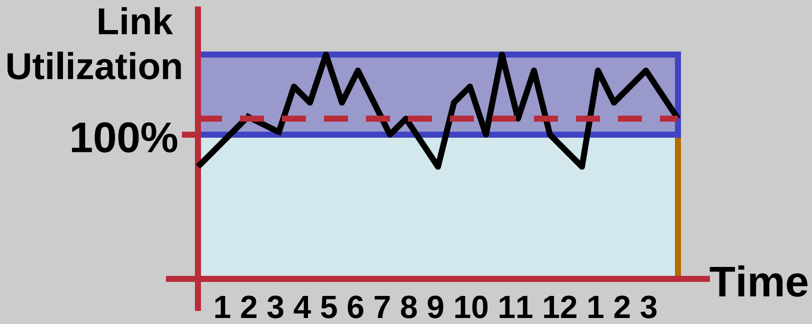
QoS Applicability



- Link overprovisioned
- May not be cost effective
- No QoS required but a safety net

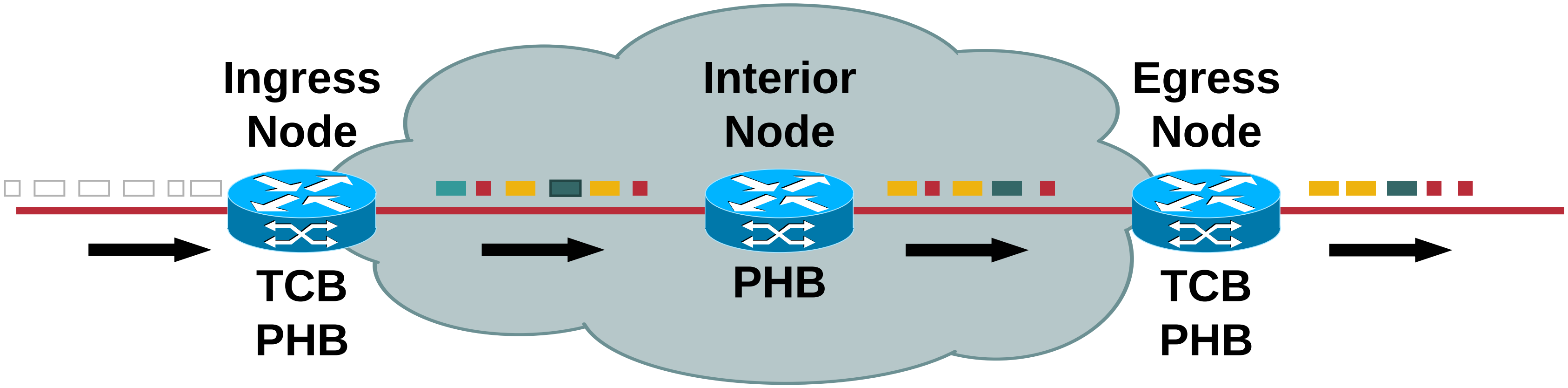


- Transient congestion
- QoS most useful



- Link highly oversubscribed
- QoS somewhat useful but more bandwidth required

Differentiated Services Architecture (RFC 2274, RFC 2275)



Ingress Node

Interior Node

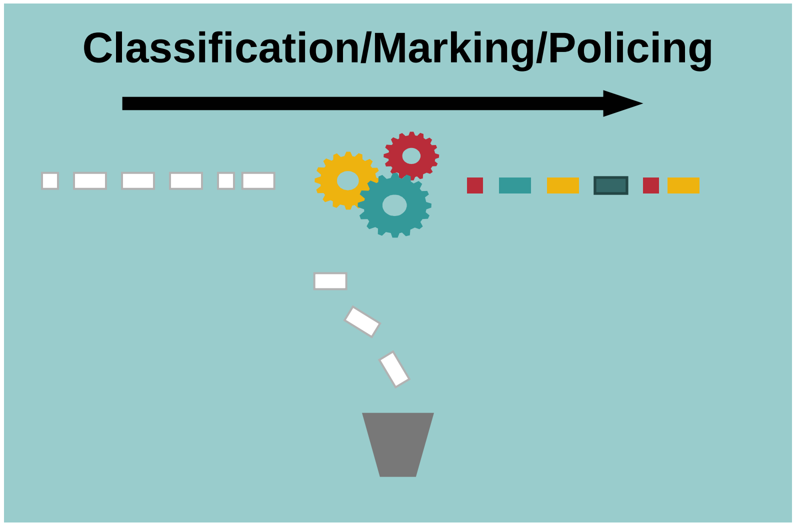
Egress Node

TCB PHB

PHB

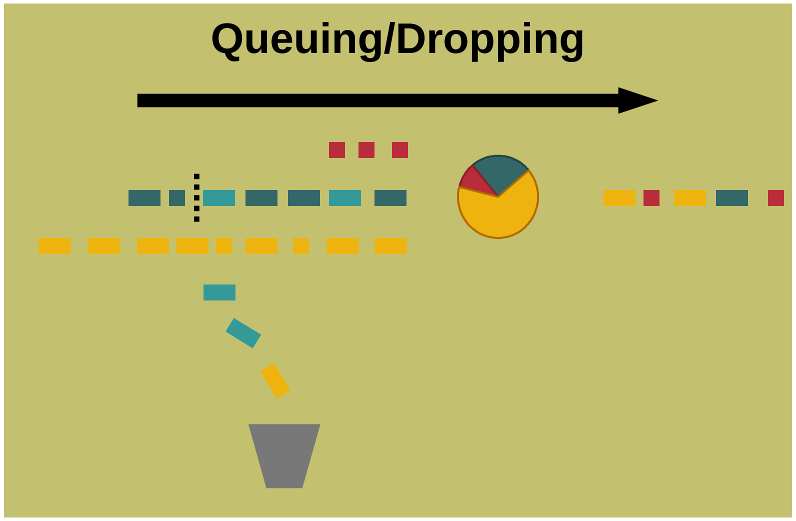
TCB PHB

Traffic Classification and Conditioning (TCB)



Classification/Marking/Policing

Per-Hop Behavior (PHB)



Queuing/Dropping

Per-Hop Behaviors (PHB)

- Expedited Forwarding (EF)
  - Building block for low delay/jitter/loss
  - Served at a certain rate with short/empty queues
- Assured Forwarding (AF)
  - High probability of delivery if profile is not exceeded
  - Four classes and three levels of drop precedence
  - Specific resources (BW, buffer space) allocated to each class at each node
- Best Effort (BE)

Integrated Services Architecture (RFC-2210, 2211,2212,2215)

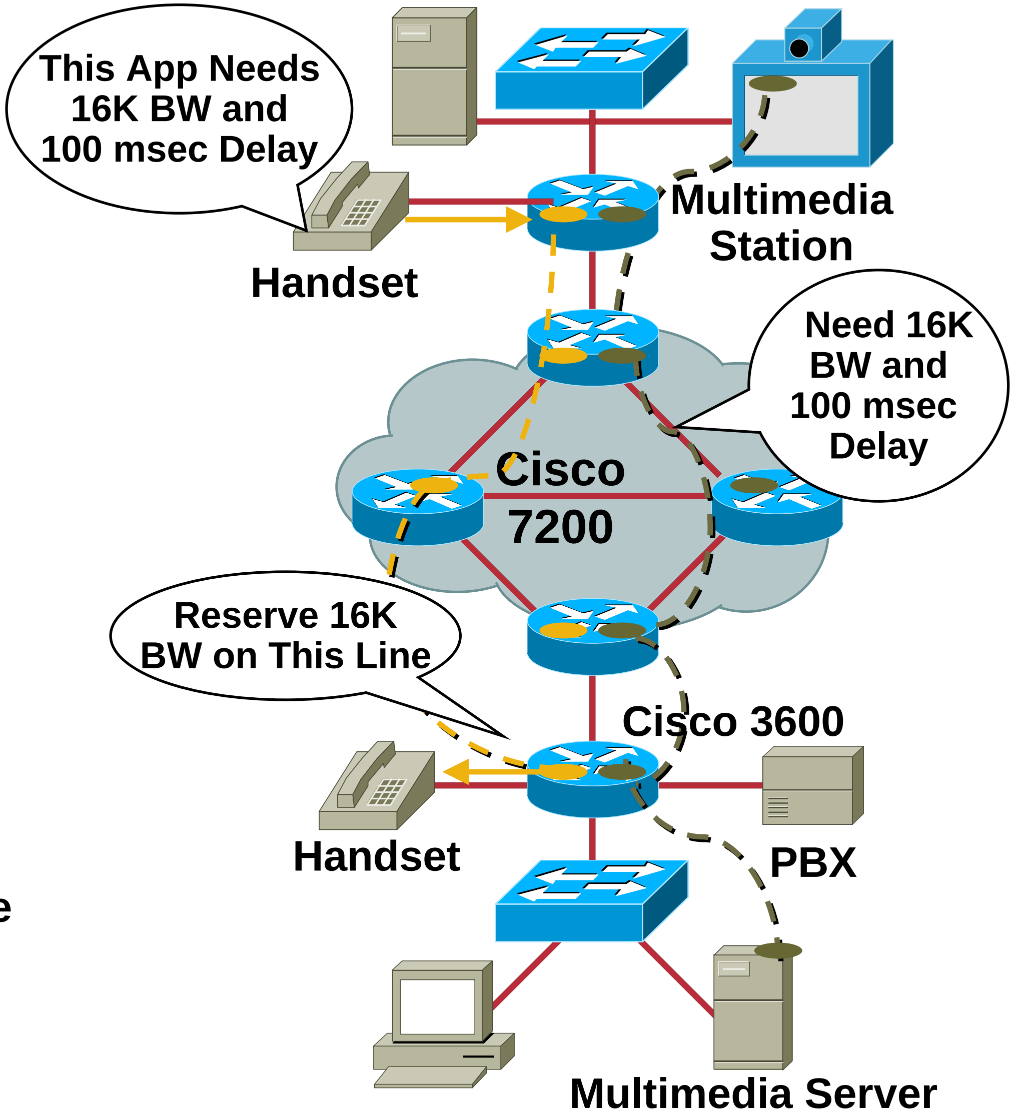
Imagine A Custom Postal Service For You!!

- Preserve the end-to-end semantics of IP for QoS
- Key end-points are the senders and the receivers
- Applications request desired service from the network for a set of microflows
- Benefits of IntServ/RSVP
  - Fairly automatic—only need to provision RSVP bandwidth on the interface
  - Integrates well with a policy infrastructure
- Disadvantages of IntServ/RSVP
  - State and signalling overhead for large networks
  - Constant refresh messages

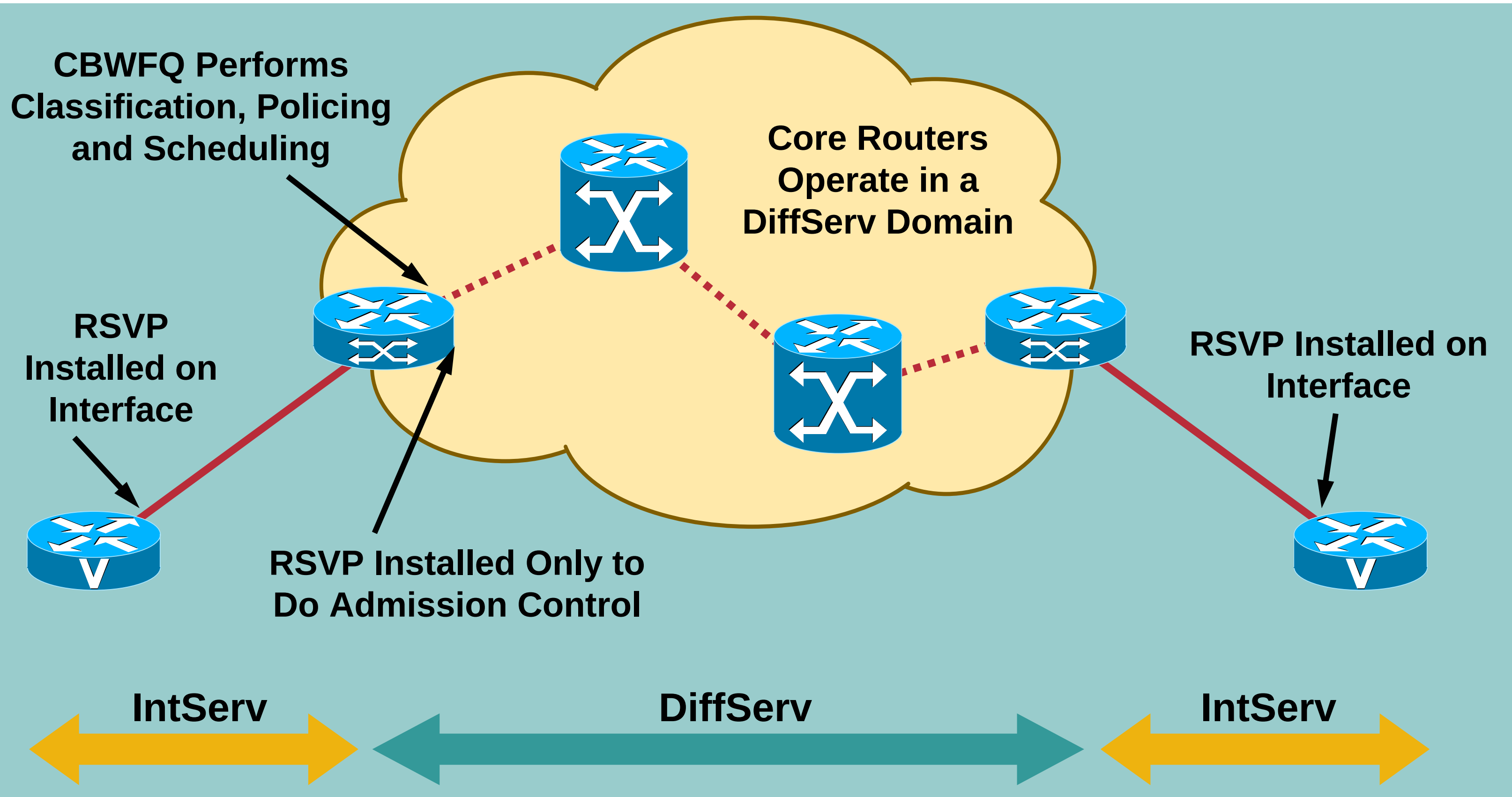
Integrated Services Architecture (Cont.): The 3 Components of IntServ

- Specification of what sender is sending: (rate, MTU, etc.)—the TSpec
- Specification of what the receiver needs: (bandwidth, path MTU, etc.)—the RSpec
- Specification of how the signalling is done to the network by the sender and the receiver:

  RSVP is the signalling protocol for IntServ (Resource ReSerVation Protocol)


This App Needs 16K BW and 100 msec Delay
Multimedia Station
Handset
Need 16K BW and 100 msec Delay
Cisco 7200
Reserve 16K BW on This Line
Cisco 3600
Handset
PBX
Multimedia Server

IntServ/DiffServ Integration



CBWFQ Performs Classification, Policing and Scheduling

Core Routers Operate in a DiffServ Domain

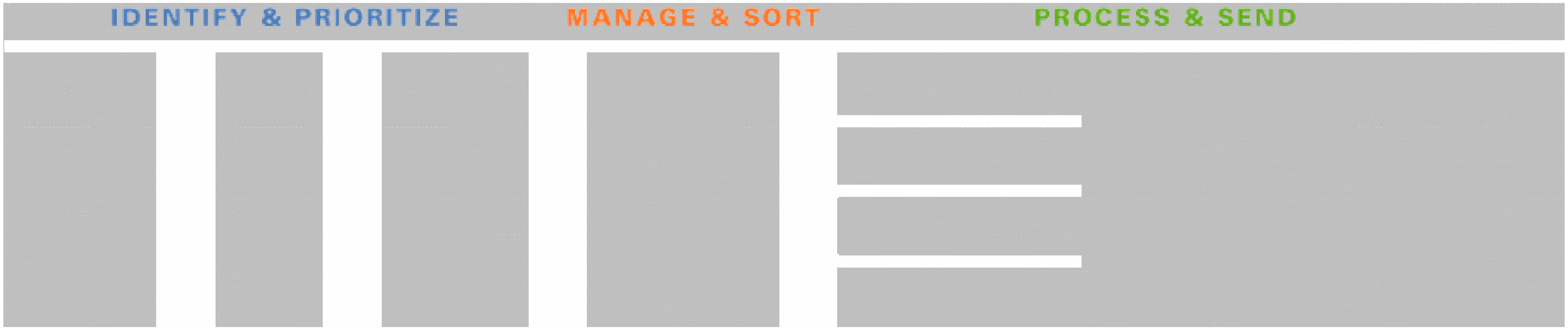
RSVP Installed on Interface

RSVP Installed on Interface

RSVP Installed Only to Do Admission Control

DEPLOYMENT GUIDE

The QoS Building Blocks



- **Defines the mechanisms that control traffic management**
- **User defines parameters that control the behavior of those mechanisms**

Five Steps to a Successful QoS Deployment

- Step 1: Identify and Classify Applications
- Step 2: Define QoS Policies
- Step 3: Test QoS Policies
- Step 4: Implement Policies
- Step 5: Monitor and Adjust

Deployment Guide
Step 1: Identify and Classify Applications

- Which applications are “mission critical” to the business
- Network resources to meet needs of an application
  - Network delay, delay variation, drop
- Derived from application properties
  - Application performance and quality requirements
  - Applications with different properties/requirements should be queued separately
  - Properties of the underlying transport protocol stack

Deployment Guide
Step 2: Define Policies

- Network topology and traffic flow
- Capacity of your network devices (CPU, software, etc.) and network links (speeds, overhead, congestion, etc.)
- Bottleneck and non-bottleneck links
- Trusted and untrusted boundary settings
- Point-to-point vs. point-to-cloud model
- We will discuss about this in detail…

Deployment Guide
Step 3: Test Policies

- Test QoS policies in the lab first
- Test policy in a small portion of the production network
- Run baseline tests without QoS
- Run baseline tests with QoS to compare application performance

Deployment Guide
Step 4: Implement Policies

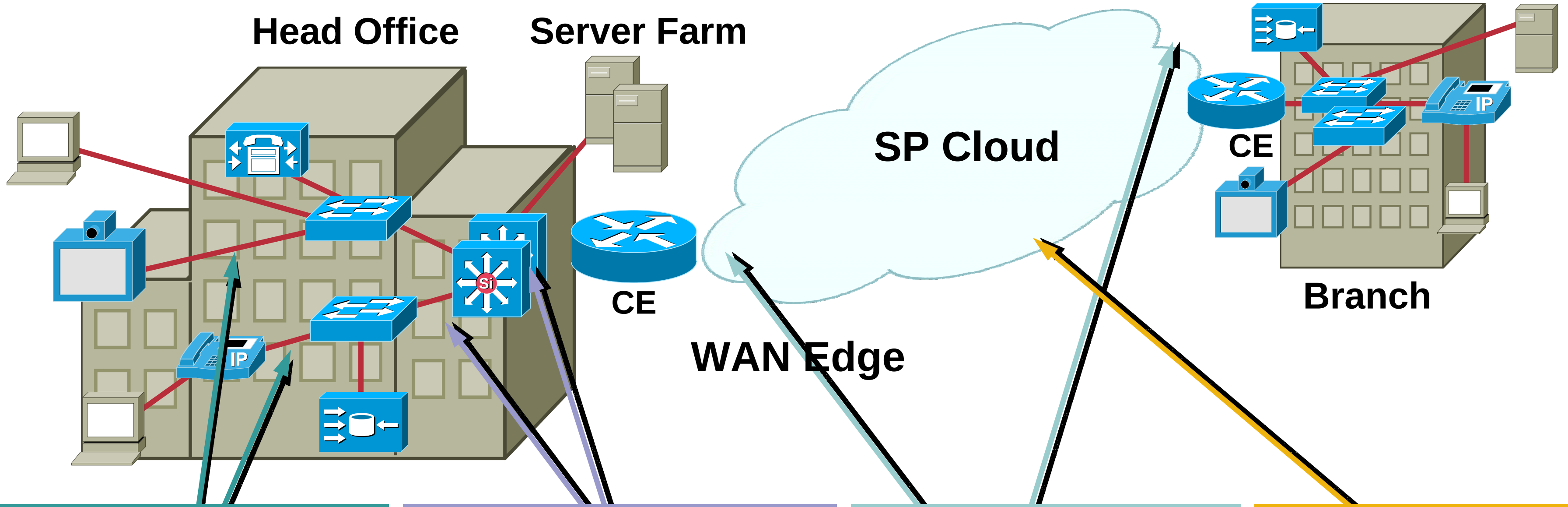
- Classify and mark as close to the edge as possible
- Work toward your core applying inbound/outbound policies
- Phased deployment—apply your policies incrementally
- Be judicious in policy application
(e.g. trivial traffic from branch to hub)

Deployment Guide
Step 5: Monitor and Adjust

- **Monitor applications performance (delay, loss, jitter etc.) for different classes**
  - **Use tools like Service Assurance Agent (SAA)**
- **Adjust policies where necessary**
- **More on this later…**

Consider the Following Network Topology

Deploying QoS End-to-End Across the Network



QoS—Campus Access

Speed and Duplex Settings

Classification/Trust on IP Phone and Access Switch

Multiple Queues on Access Ports

QoS—Campus Distribution

Layer 3 Policing, Marking

Multiple Queues on All Ports; Priority Queuing for VoIP

WRED within Data Queue for Congestion Management

QoS—WAN Edge

Define SLA

Classification, Marking

Low-Latency Queuing

Link Fragmentation and Interleaving

WRED and Shaping

QoS—SP Cloud

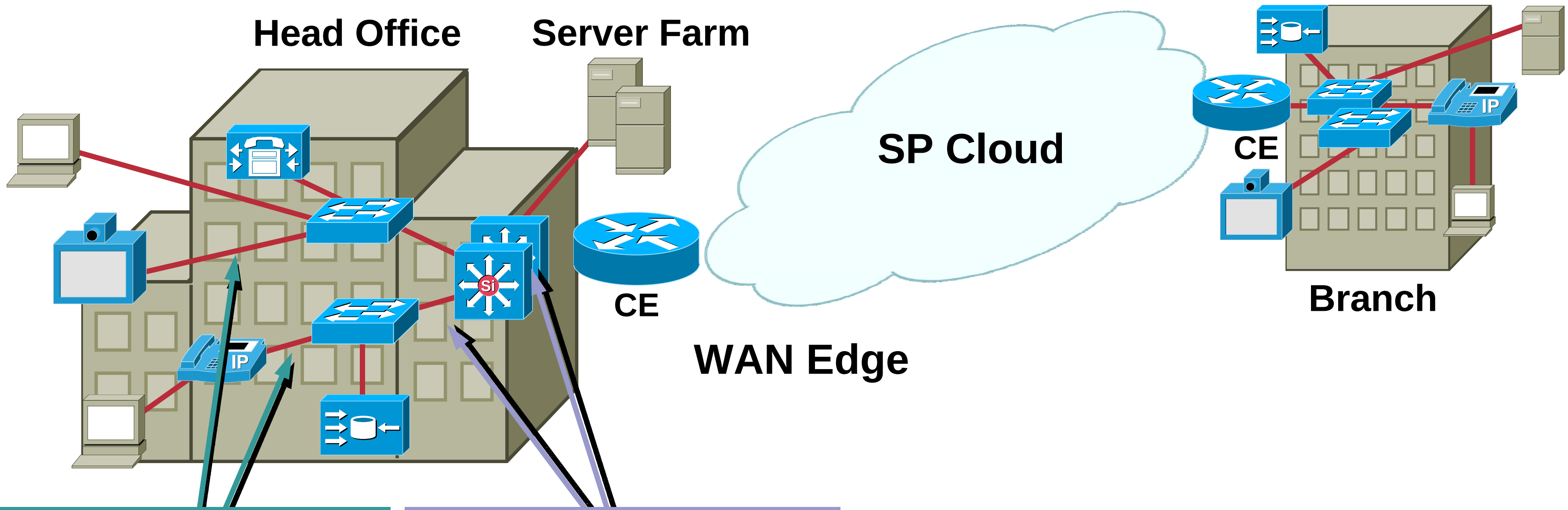
Capacity Planning

Queuing

WRED

Consider the Following Network Topology

Let Us Talk About the Access and Distribution Layers



QoS—Campus Access

- Speed and Duplex Settings
- Classification/Trust on IP Phone and Access Switch
- Multiple Queues on Access Ports

QoS—Campus Distribution

- Layer 3 Policing, Marking
- Multiple Queues on All Ports; Priority Queuing for VoIP
- WRED within Data Queue for Congestion Management

QoS in the Campus and Distribution
Is It Required?

Cisco.com

- “Buffer management is as important as bandwidth management”
- Just throwing more bandwidth in the LAN will not solve the problem
- Multiple queues are required on all interfaces to ensure mission critical traffic is not impacted by Transmit buffer congestions and packet drops

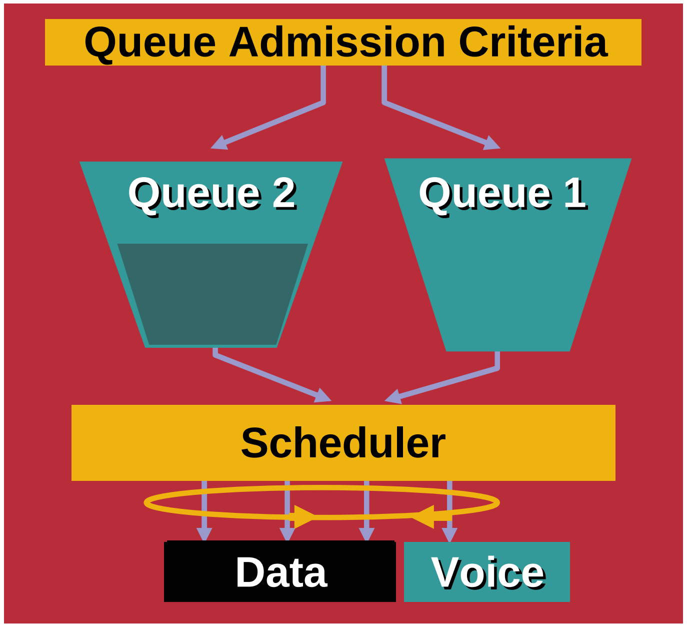
QoS in the Campus and Distribution: Output Scheduling

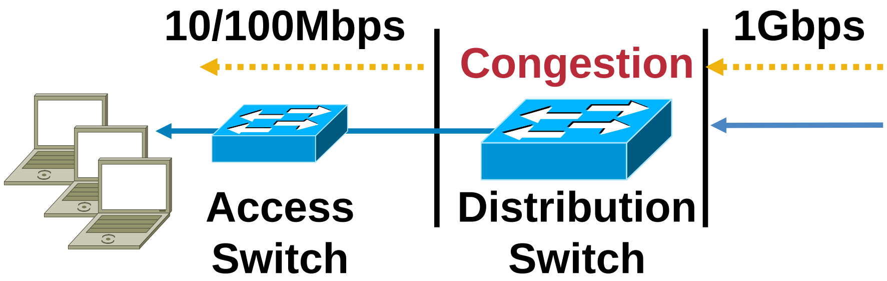
- **Multiple queues with classification criteria and scheduling mechanisms must be configured**

  Strict Priority Scheduling (SPS) or Weighted Round Robin (WRR) scheduling

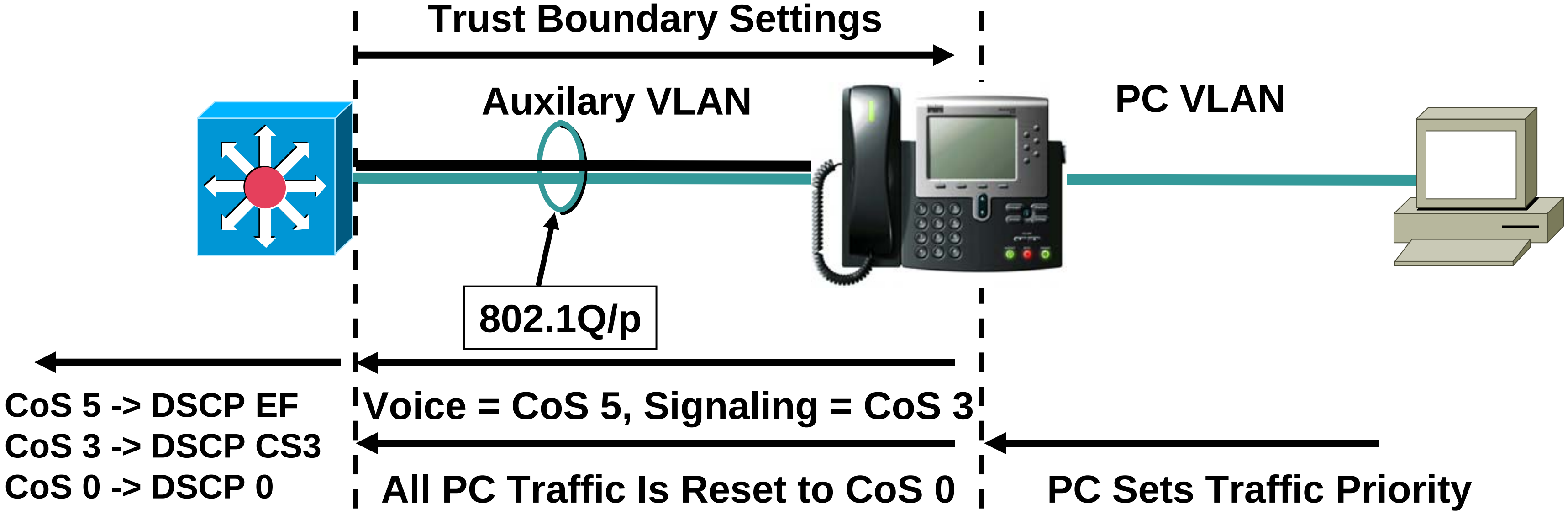
- **Admit traffic to queues based on CoS value**
- **Use policing to protect the uplink from over-subscription**

  Aggregation points are hotspots for buffer overruns and transmit ring drops





Classification Tools:
Trust Boundary Extension and Operation



Trust Boundary Settings

Auxilary VLAN

PC VLAN

802.1Q/p

CoS 5 -> DSCP EF
CoS 3 -> DSCP CS3
CoS 0 -> DSCP 0

Voice = CoS 5, Signaling = CoS 3

All PC Traffic Is Reset to CoS 0

PC Sets Traffic Priority

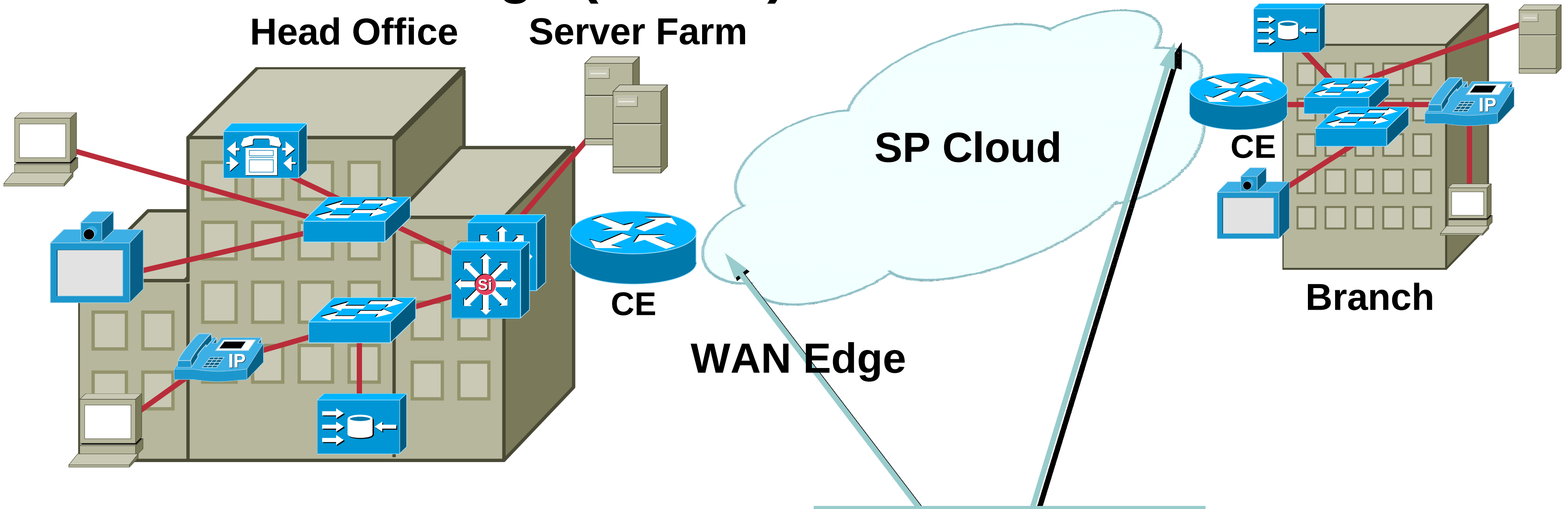
- Trust boundary settings

  untrusted, trust-cos, trust-ipprec, trust-dscp, trust-ext <trusted>

- Switch and Phone exchange CDP; trust boundary is extended to IP phone
- IP Phone sets CoS to 5 for VoIP and to 3 for call signaling
- PC traffic reset to CoS 0 by IP phone
- CoS→DSCP mapping for output scheduling on switch

Consider the Following Network Topology

At the WAN Edge (CE/PE)

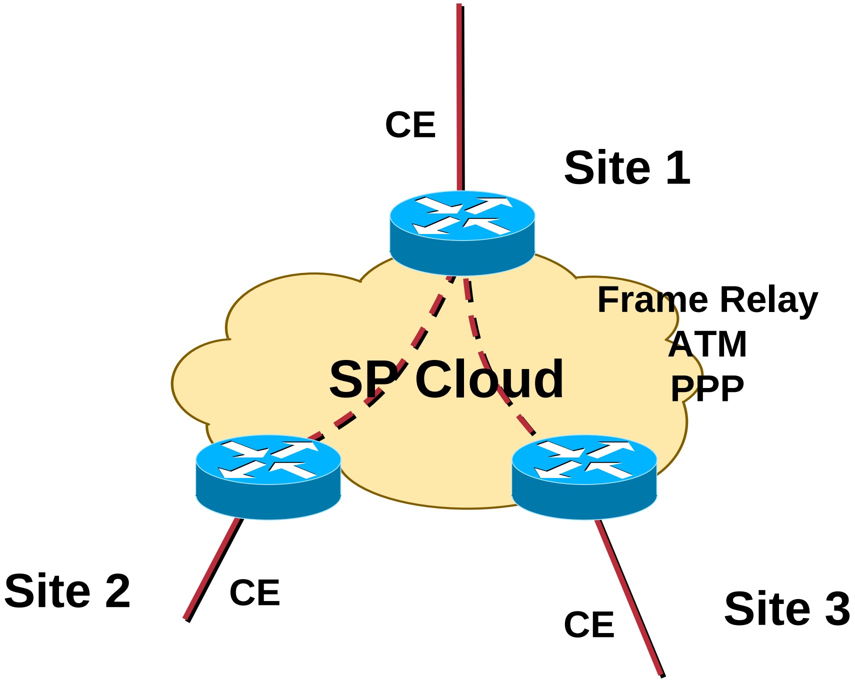


QoS—WAN Edge

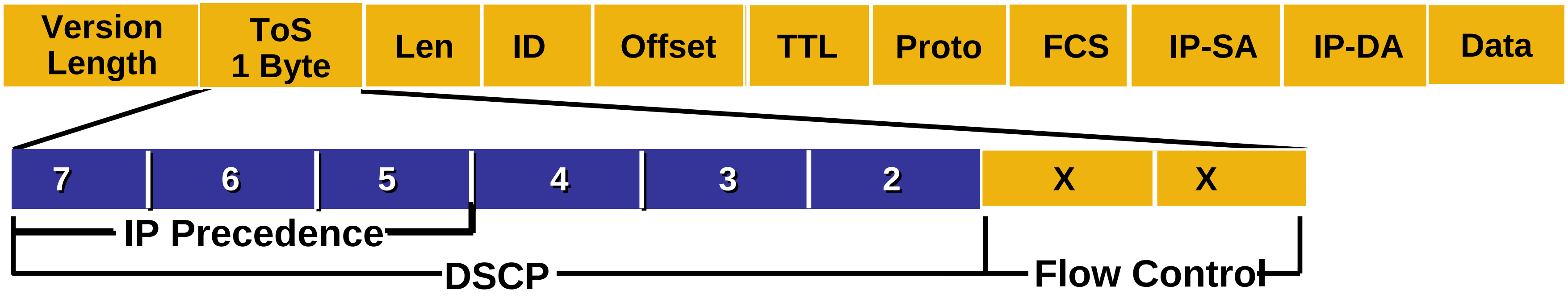
- Classification, Marking
- Low-Latency Queuing
- Link Fragmentation and Interleaving
- WRED and Shaping
- SLA Definition

Define Policies: Enterprise Network with Traditional L2 Service

- SP sells Layer 2 service
- Point-to-point
  SLA from SP
- Enterprise WAN likely to get congested
- IP QoS required for VVD integration
- SP not involved in IP QoS



Identifying Applications (CE–PE Edge) Classification and Marking



Version Length | ToS 1 Byte | Len | ID | Offset | TTL | Proto | FCS | IP-SA | IP-DA | Data

7 | 6 | 5 | 4 | 3 | 2 | X | X

IP Precedence

DSCP

Flow Control

- Classification criteria

  Incoming interface, IP Address, VLAN id or FR DLCI

  Standard or extended source/destination access lists

  DSCP or IP precedence value

  Layer 3 packet length

  Network-Based Application Recognition (NBAR)

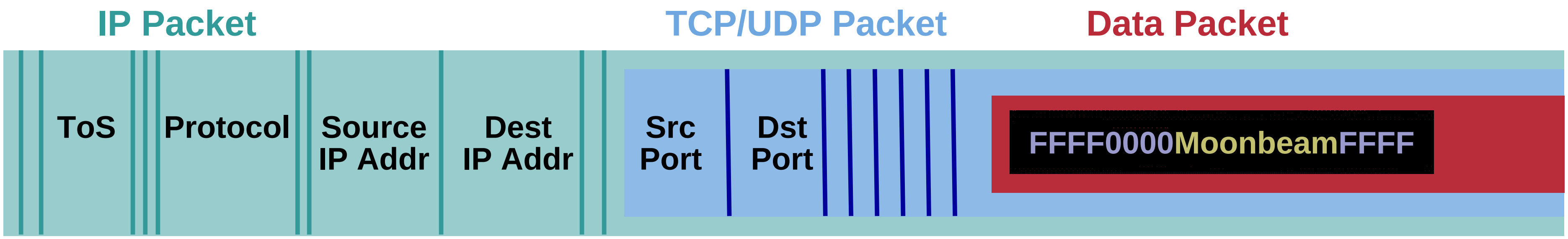
- Marking—setting a value in the frame (Layer2) or packet (Layer3)

  Packets marked in the edge for classification in the core

Identifying Applications (CE/PE): Network-Based Application Recognition (NBAR)

- IP packet classifier capable of classifying applications that have:
  - Statically assigned TCP and UDP port numbers
  - Non-TCP and non-UDP IP protocols
  - Dynamically assigned TCP and UDP port numbers during connection establishment
  - Classification based on deep packet inspection—NBAR's ability to look deeper into the packet to identify applications
  - HTTP traffic by URL, host name or MIME type using regular expressions (*, ?, [ ]), Citrix ICA traffic, RTP Payload type classification
  - Protocol Discovery analyzes application traffic patterns in real time and discovers traffic running on the network
- Currently supports over 100 protocols/applications

NBAR User-Defined Custom Application Classification



- Name—Name the match criteria—up to 24 characters

  my_protocol
- Offset—Specify the beginning byte of string or value to be matched in the data packet, counting from ZERO for the first byte

  Skip first 8 bytes
- Format—Define the format of the match criteria—ASCII, hex or decimal

  ascii
- Value—The value to match in the packet—if ASCII, up to 16 characters

  Moonbeam
- [Source or destination port]—Optionally restrict the direction of packet inspection; defaults to both directions if not specified

  [source | destination]
- TCP or UDP—Indicate the protocol encapsulated in the IP packet

  tcp
- Range *or* selected port number(s)

  "range" with start and end port numbers, up to 1000

  1 to 16 individual port numbers

  range 2000 2999

Example

```
ip nbar custom my_protocol
  8 ascii Moonbeam tcp
  range 2000 2999

class-map custom_protocol

match protocol my_protocol

policy-map my_policy
  class custom_protocol
  set ip dscp AF21

interface <>

service-policy output
  my_policy
```

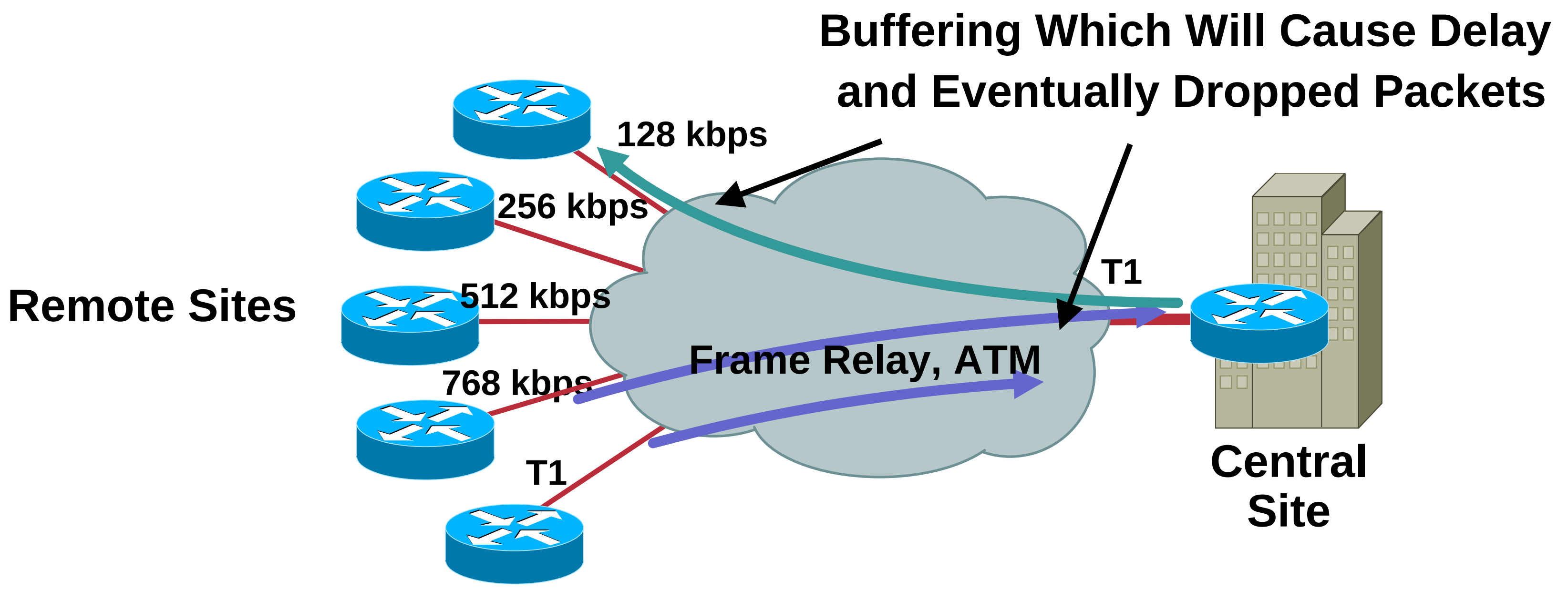
12/03

Identifying Applications (PE)
Packet Length (L3) Based Classification

- Light-weight method of ensuring EF service on low-speed access
  - Large data packets invading LLQ cause delay
- Determine packet size distribution on various links
- SPs restrict the uploads but allow unlimited downloads
  - Upstream bandwidth is more expensive
  - Small TCP ACK packets going upstream should not be dropped

```
match packet length min <n> max <m>
```

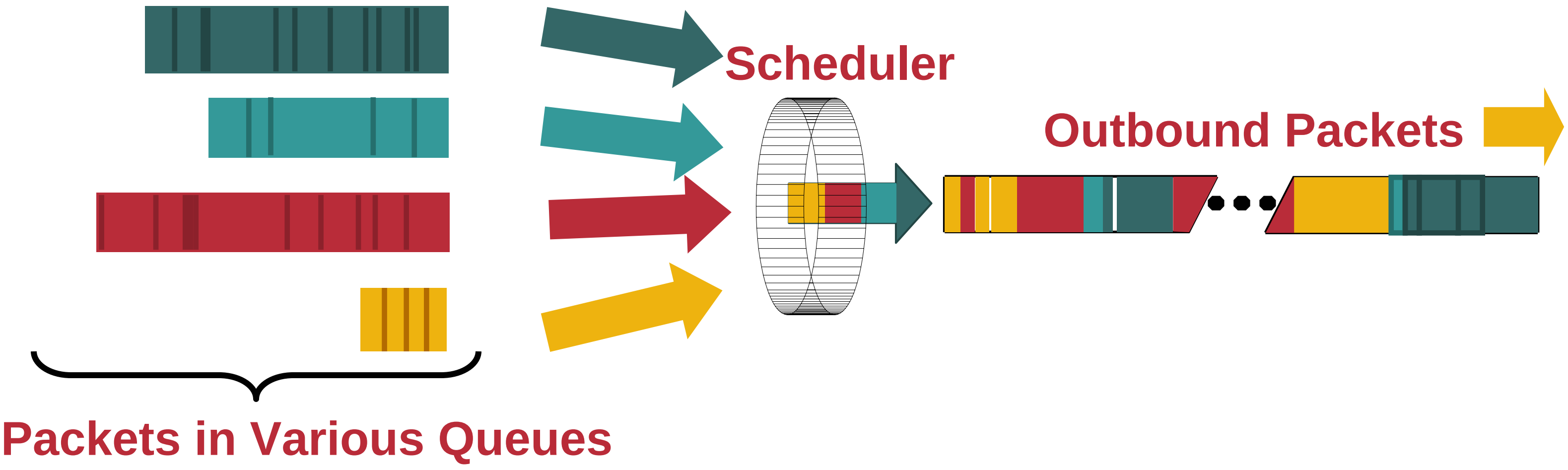
The Need for Traffic Shaping



- Central to remote site speed mismatch
- To avoid remote to central site oversubscription
- To prohibit bursting above committed/subscribed rate

```
Shape <average | peak> <cir> <bc>
```

The Need for Congestion Management (Queuing)



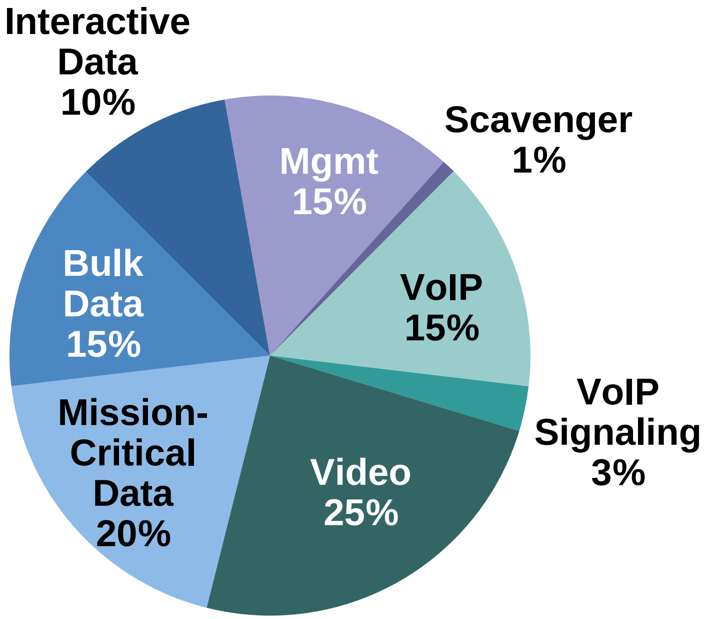
- The queuing system aggregates packet streams into multiple queues
- Provide a different service to each queue
- Low-Latency Queuing (LLQ) used for highest-priority traffic (voice/video)
- Class-Based Weighted-Fair Queuing (CBWFQ) used for guaranteeing minimum bandwidth to data applications

Queuing: Output Attributes of a Queue

- Priority (priority)—Low delay, strict priority queue
  - Data transmitted ahead of all others queues
  - Allowed to utilized otherwise idle bandwidth
- Min Bandwidth (bandwidth)—Guarantee the specified BW
  - Oversubscription is allowed
  - In absence of oversubscription, Σ minBW(of all queues) <= available BW
- Max Bandwidth (Shape)—Max BW the queue receives
- Excess Bandwidth (bandwidth remaining)—Divide excess or unused bandwidth
  - Queues that already sent more than the min but less than max

Queuing: Sample Policy for WAN Bandwidth Allocation

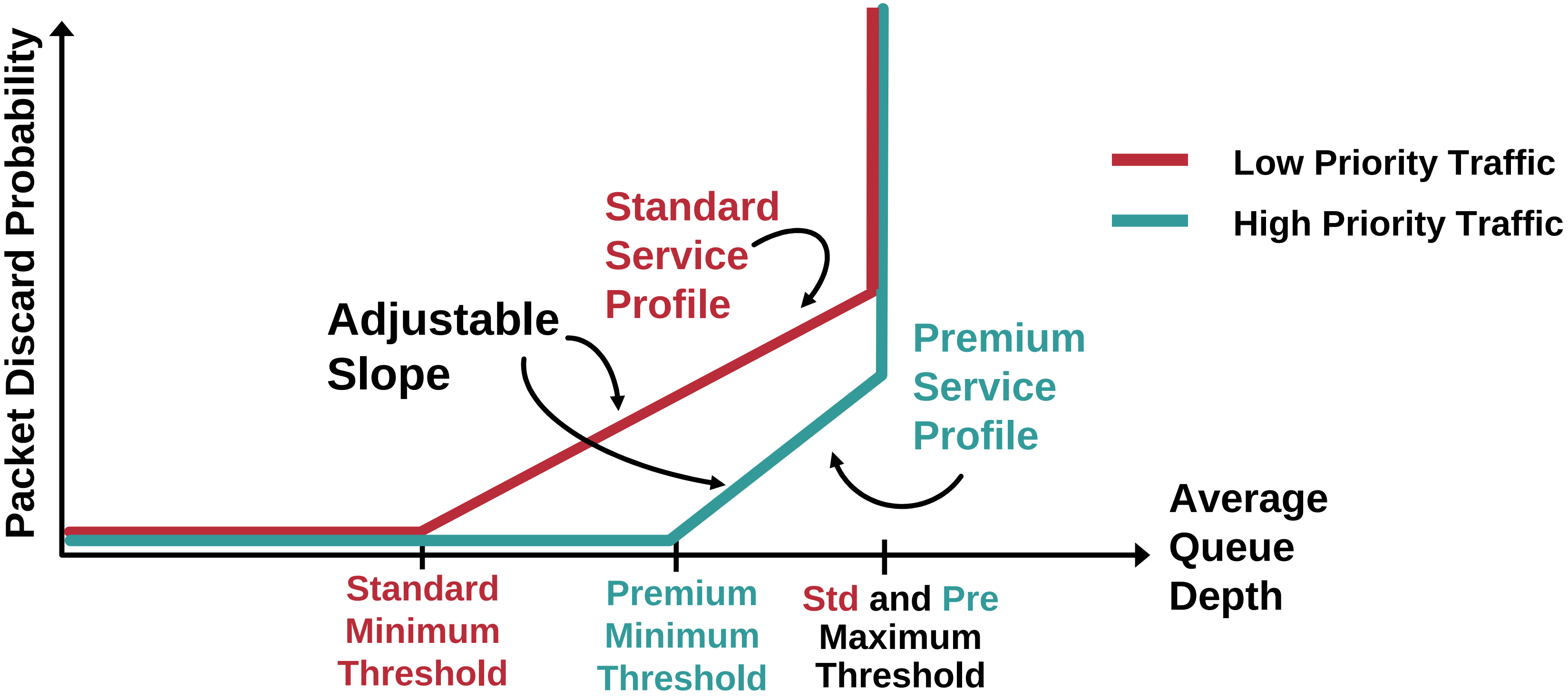
```
policy-map Multiservice
  class VoIP
    priority percent 15
  class VoIP-Signaling
    bandwidth remaining percent 3
  class video
    bandwidth remaining percent 25
  class Mission-Critical-Data
    bandwidth remaining percent 20
  class Bulk-Data
    bandwidth remaining percent 15
  class Interactive-Data
    bandwidth remaining percent 10
  class Management
    bandwidth remaining percent 15
  class Scavenger
    bandwidth remaining percent 1
  class class-default
    fair-queue
```



The Need for Congestion Avoidance: Active Queue Management

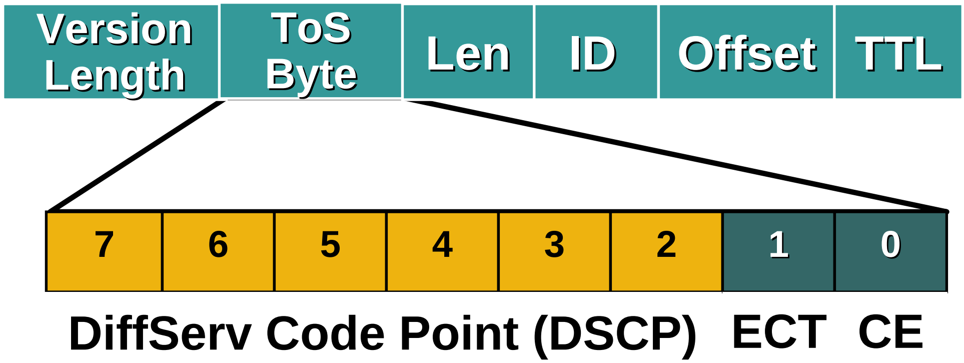
- Dropping can occur in the edge or core due to policing or buffer exhaustion
- If a queue fills up, all packets at tail end of queue get dropped—called tail-drop
- Tail-drop results in simultaneous TCP window shrinkage of large number of sessions, resulting in "global synchronization"
- Weighted Random Early Detection (WRED) enables intelligent packet drop decision when average queue depth exceeds a minimum threshold

Congestion Avoidance: WRED Attributes for Multiple Service Levels



```
random-detect [dscp-based]
random-detect exponential-weighting-constant <value>
random-detect precedence <precedence> <min-
threshold> <max-threshold> <mark-prob-denominator>
```

Weighted Random Early Detection: Explicit Congestion Notification (ECN)



Non ECN-Capable (ECT, CE)	0	0
ECN Capable Endpoints (ECT)	0	1
ECP Capable Endpoints (ECT)	1	0
Congestion Experienced (ECT,CE)	1	1

```
random-detect
random-detect ecn
```

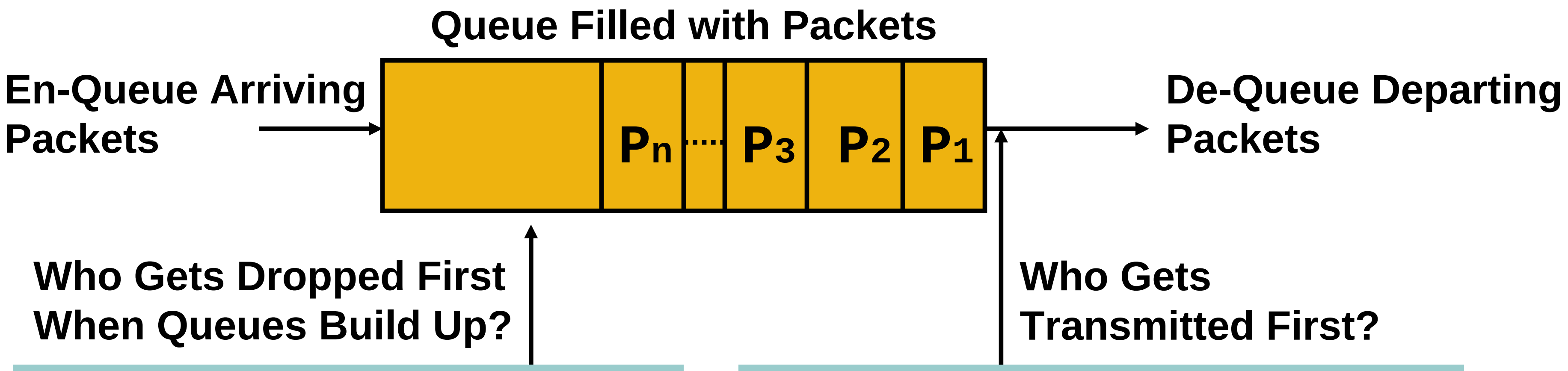
- Some applications prefer not to wait for TCP retransmit timer to expire

  Short web transfers and low bandwidth Telnet

- No packet drop

  Congestion notification signal is sent to end host

Attributes of a Queue: Summary



Queue Filled with Packets

En-Queue Arriving Packets

De-Queue Departing Packets

Who Gets Dropped First When Queues Build Up?

Who Gets Transmitted First?

Attributes Controlling the Queue Depth (Drop Policy):

- Active Queue Management (WRED, DWRED, WRED-ECN)
- Tail drop

Attributes Controlling Output from the Queue:

- Min BW guarantee
- Max BW == shaping
- Excess BW == BW remaining percentage
- Priority level

The Need for RTP Header Compression

PROBLEM: IP (20B) + UDP (8B)+ RTP (12B) Header = 2 x Payload

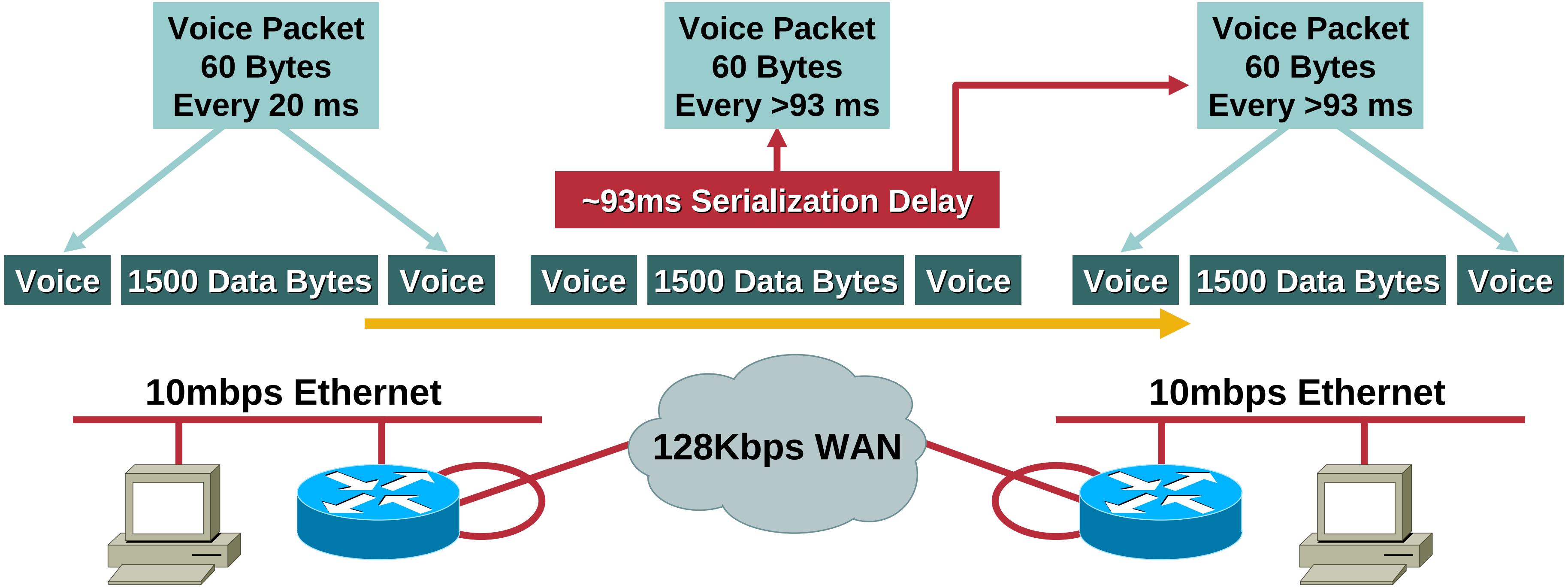
CODEC	PPP 6 Bytes of Header	ATM 53 Bytes Cells with a 48 Byte Payload	Frame Relay 4 Bytes of Header
G.711 at 50 pps	82.4 kbps	106 kbps	81.6 kbps
G.711 at 33 pps	75.5 kbps	84 kbps	75 kbps
G.729A at 50 pps	26.4 kbps	42.4 kbps	25.6 kbps
G.729A at 33 pps	20 kbps	28 kbps	19.5 kbps

BENEFIT: Reduction in Voice Bandwidth Requirement (2–5 B Header)

CODEC	PPP 6 Bytes of Header	PPPoATM 53 Bytes Cells with a 48 Byte Payload	Frame Relay 4 Bytes of Header
G.711 at 50 pps	68 kbps	84.8 kbps	67 kbps
G.711 at 33 pps	66 kbps	56 kbps	65.5 kbps
G.729A at 50 pps	12 kbps	21.2 kbps	11.2 kbps
G.729A at 33 pps	10.5 kbps	14.kbps	10 kbps

The Need for Fragmentation and Interleaving on Slow-Speed Links

Problem: Large Packets “Freeze Out” Voice



- Implemented via Multilink PPP over FR, ATM, and leased lines
- Fragments are interleaved with the real-time packets, reducing the serialization delay experienced by voice packets

Benefit: Reduce the Jitter and Latency in Voice Calls

Define Policies
Putting It All Together…

Define a Per-Hop Behavior (PHB)
Condition Traffic Entering/Exiting the Network (TCB)

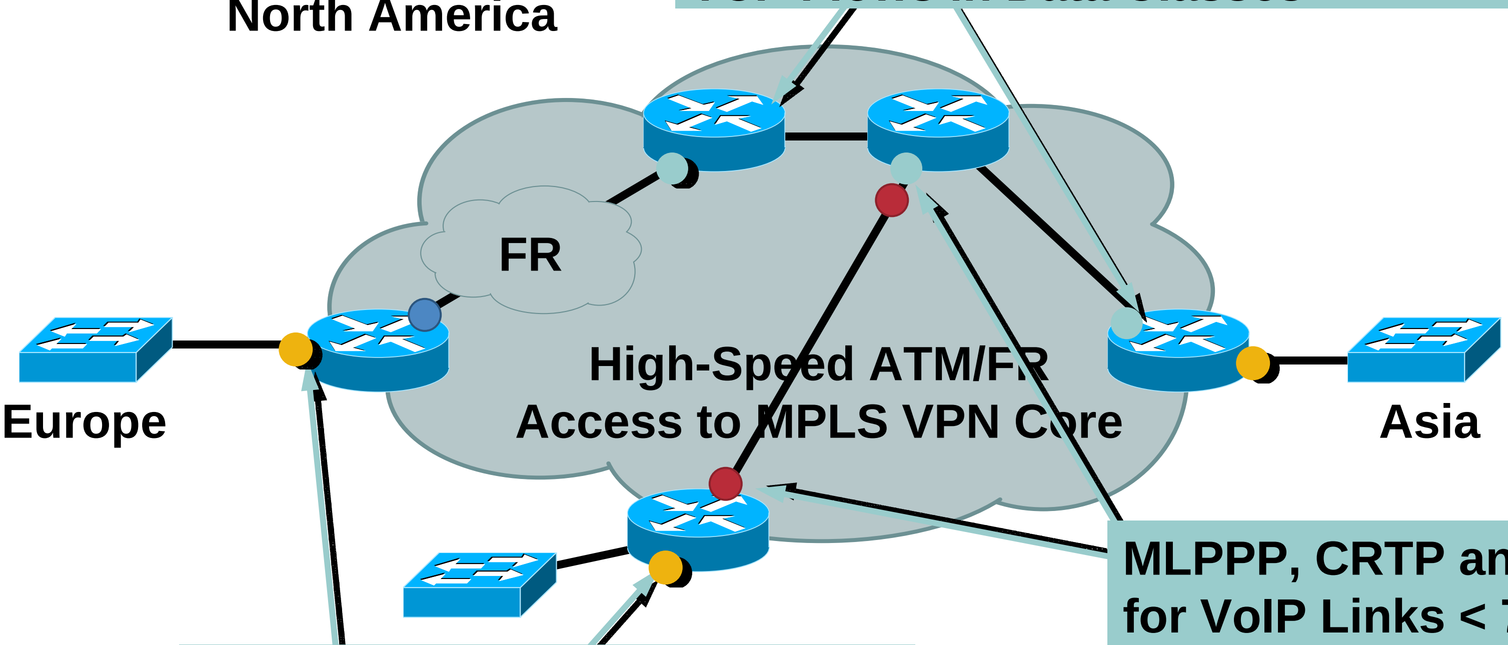
For Example:

	Real-Time Interactive	Real-Time Streaming	Interactive	Background and Bulk	Best Effort
Marking	EF	AF3x	AF2x	AF1x	Default
Policing	512k	256k	128k	128k	None
Queuing	Priority 512	Bandwidth Percent 25	Bandwidth Percent 20	Bandwidth Percent 10	Available
Dropping	Tail Drop	Tail Drop	WRED	WRED	WRED

Putting It All Together in a Large Enterprise: Example

- Implement a complete DSCP model
- Four or five classes of service
  - Real-Time—VoIP and streaming video (separate bandwidth class for video in case of slow speed links)
  - Interactive—Database lookups, Citrix and Telnet
  - Bulk—Large FTPs and backups
  - Best Effort—Default class and control traffic
- Slow speed VoIP links have RTP header compression and link fragmentation

Putting It All Together in a Large Enterprise: WAN Topology



LLQ (Output Policy) for VoIP, Streaming Video and Traffic from Data Center

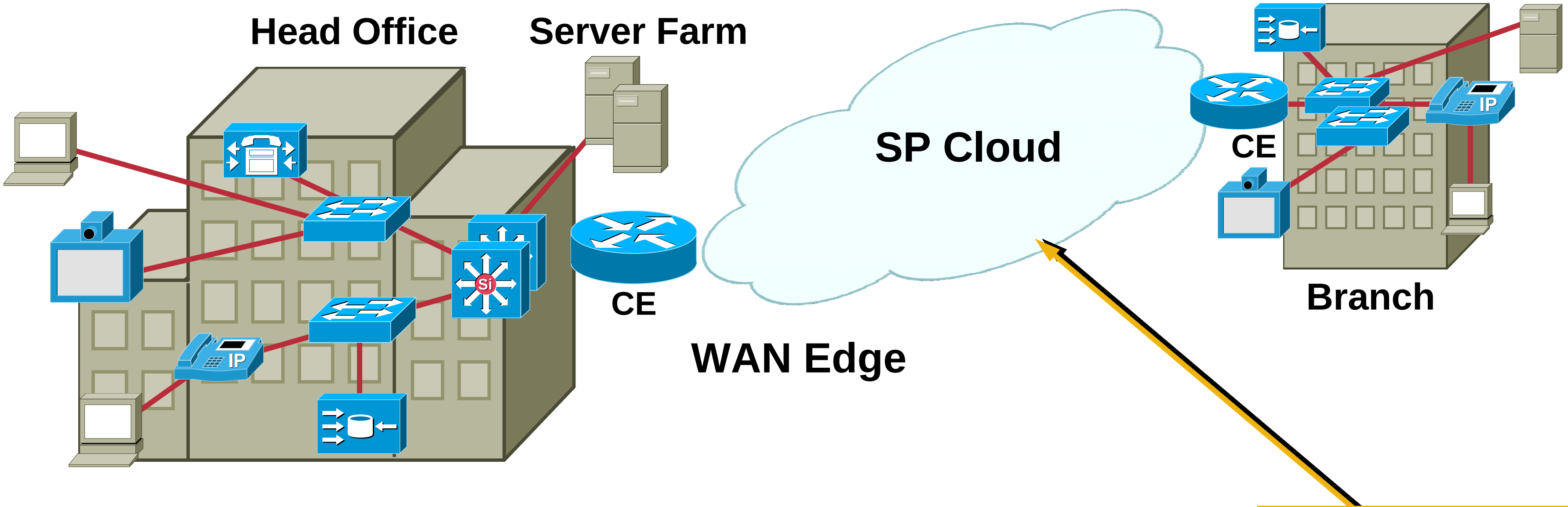
WRED for Active Queue Management of TCP Flows in Data Classes

MLPPP, CRTP and LFI for VoIP Links < 768K

Packets Entering the Network Are Colored at Edge

Consider the Following Network Topology

But…You Could Be Buying a Layer 3 Service

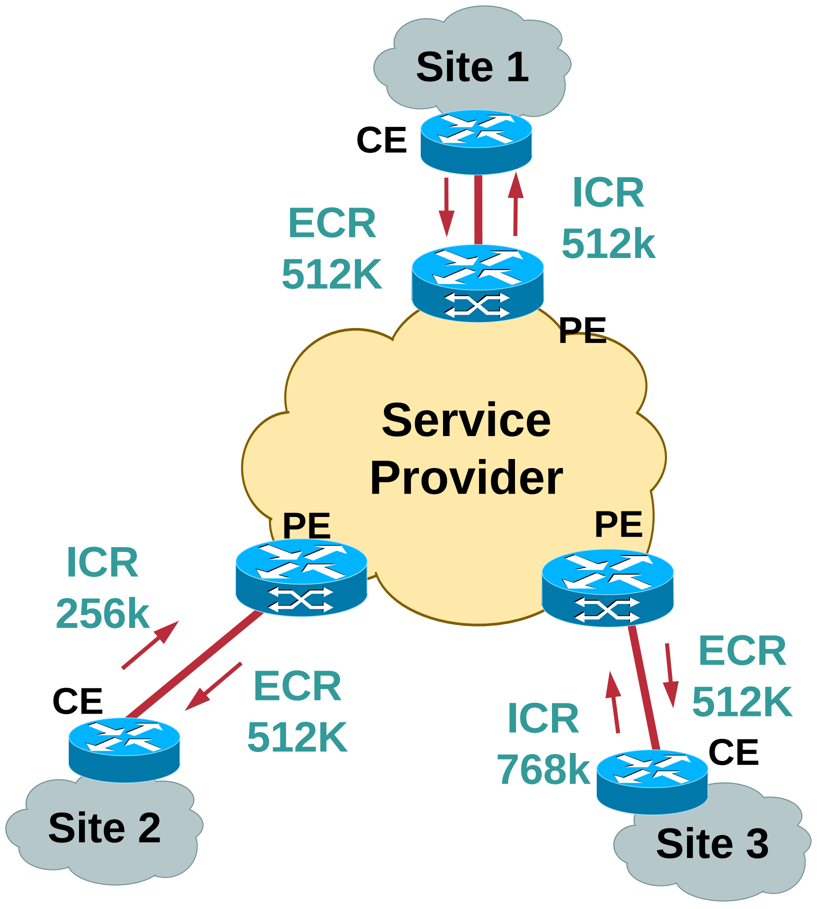


QoS—SP Cloud

Capacity Planning
Queuing
WRED

Define Policies
Enterprise Network with IP Service

- Customer buys Layer 3 service from SP
- Point-to-cloud SLA from SP for conforming traffic
- Enterprise WAN likely to get congested
- SP involved in IP QoS
- Any site can transmit up to ICR into the cloud
- Any site can receive up to ECR from the cloud

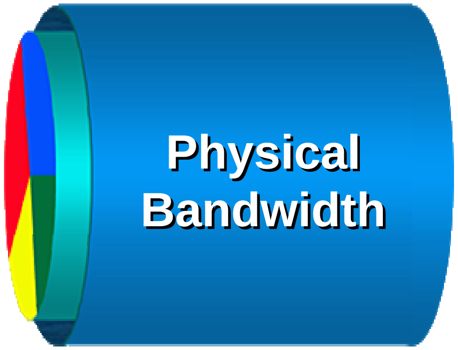


ECR—Egress Committed Rate
ICR—Ingress Committed Rate

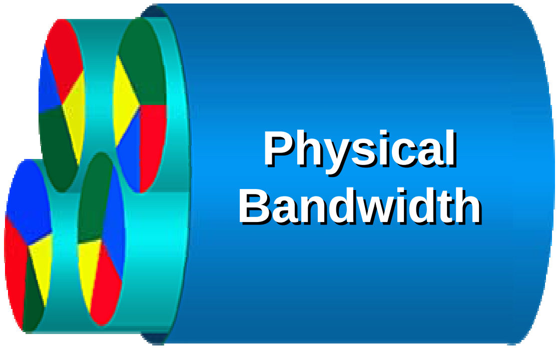
Define Policies (Cont.)
Know the SLA Offered by Your SP

- SLA typically includes between 3 and 5 classes
- Real-time traffic gets fixed bandwidth allocation
- Data traffic gets variable bandwidth allocation with minimum guarantee
- Frequently, bandwidth allocations defined as percentage of sub-rate (e.g. PVC CIR, shaped rate)
- Additional classes not visible to customer may exist at the edge (e.g. management/ control traffic)

SLA per Interface (Possibly Sub-Rate)



SLA per PVC/VLAN



The Need for Traffic Policing

- Restrict traffic class to certain rate, so that packets exceeding/violating contract can be remarked to a different DiffServ class or dropped
- RFC 2697: A single rate three color marker

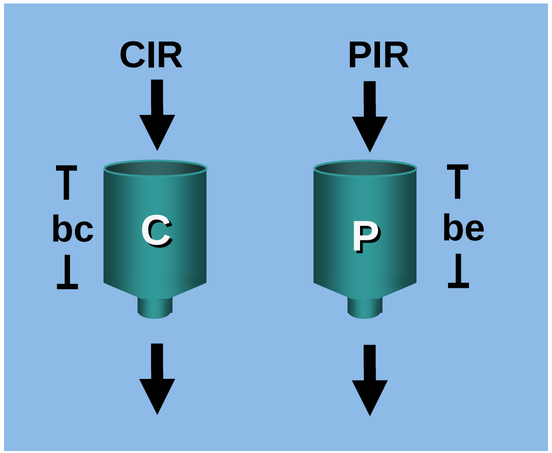
  Mark conforming traffic to low drop priority, mark exceeding traffic with high drop precedence, and drop violating traffic

- RFC 2698: A two rate three color marker

  Need to enforce peak rate for a service separately from a committed rate, modeling the FR concept in pure IP networks

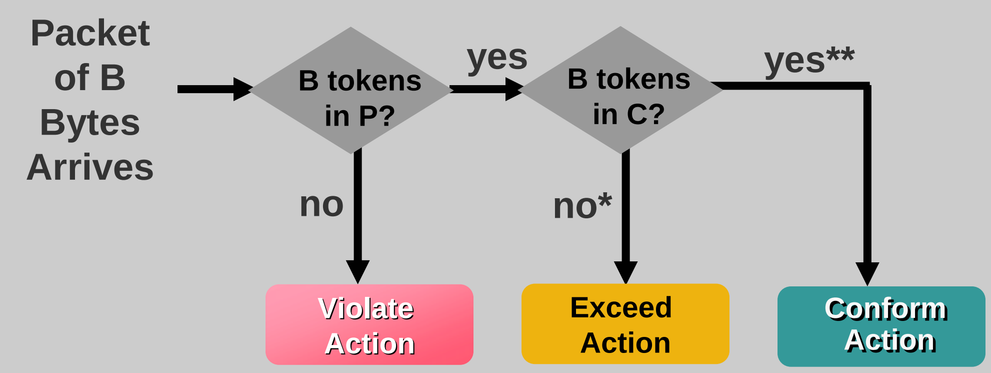
- Color-aware policer support for tighter SLAs

Two-Rate, Three-Color Policer (RFC 2698)



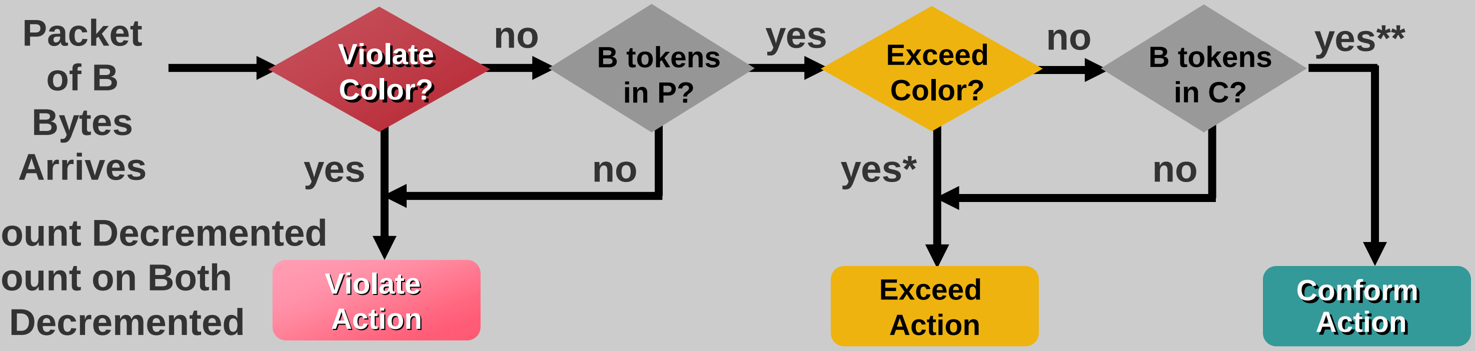
CIR—Committed Information Rate
PIR—Peak Information Rate
bc—Committed (max) Burst
be—Peak (max) Burst

Color-Blind Policer



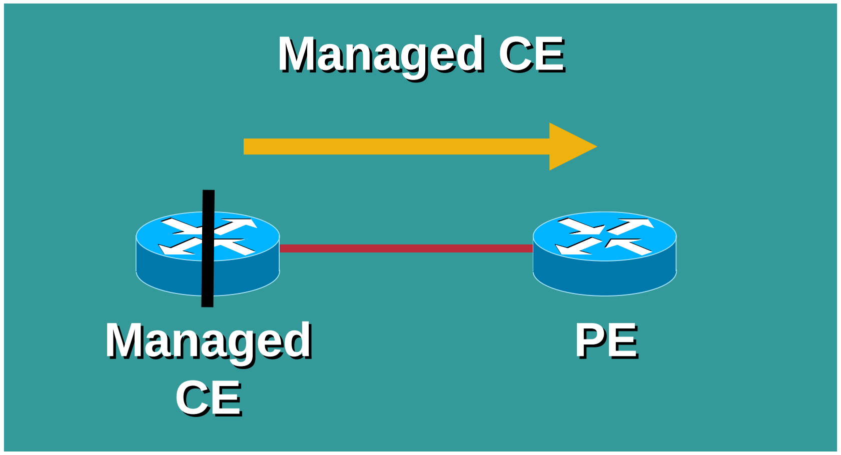
* Token Count Decremented
** Token Count on Both Buckets Decremented

Color-Aware Policer

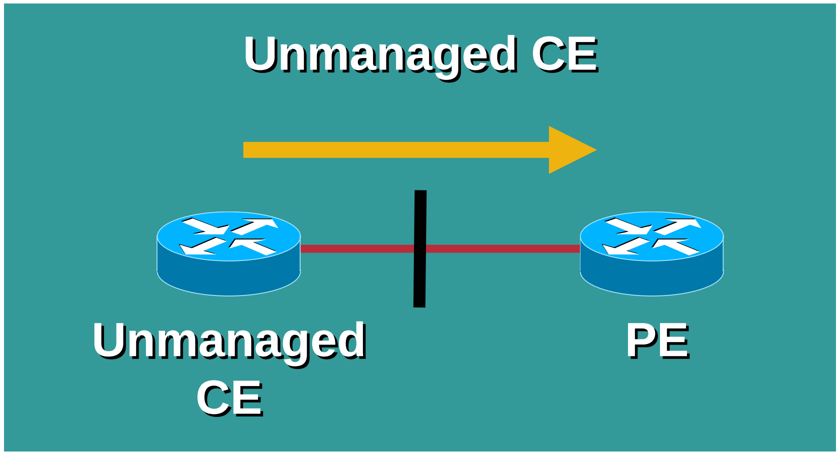


* Token Count Decremented
** Token Count on Both Buckets Decremented

At the CE PE Edge
Traffic Leaving the Enterprise Network

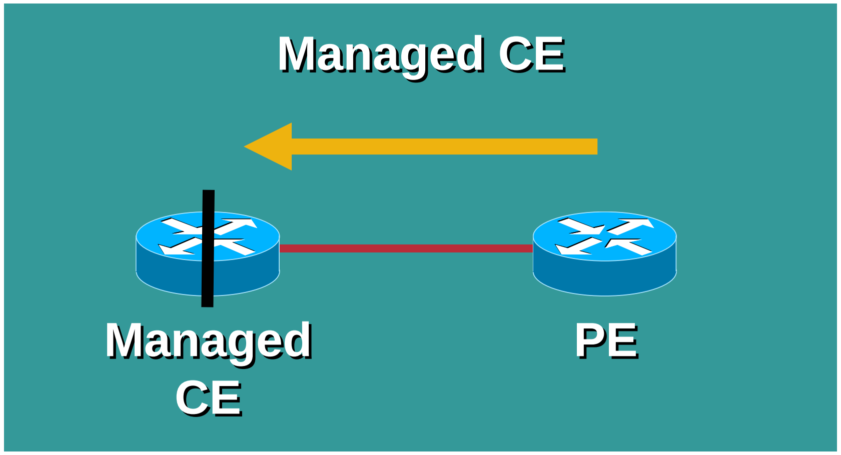


- Output QoS policy on CE controlled by SP
- SP enforces SLA using the output QoS policy on CE
- Output policy uses queuing, dropping and optionally, shaping
- Elaborate traffic classification or mapping of existing markings
- Slow links require LFI/cRTP

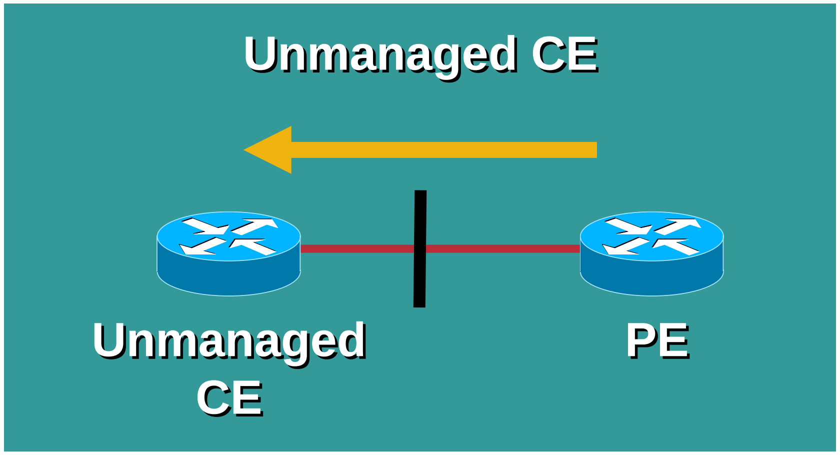


- Output QoS policy on CE controlled by customer
- SP enforces SLA using input QoS policy (policing) on PE
- Customer defines output policy with queuing, dropping, shaping based on business priorities
- Elaborate traffic classification or mapping of existing customer markings on PE router

At the CE PE Edge (Cont.)
Traffic Leaving Service Provider Network



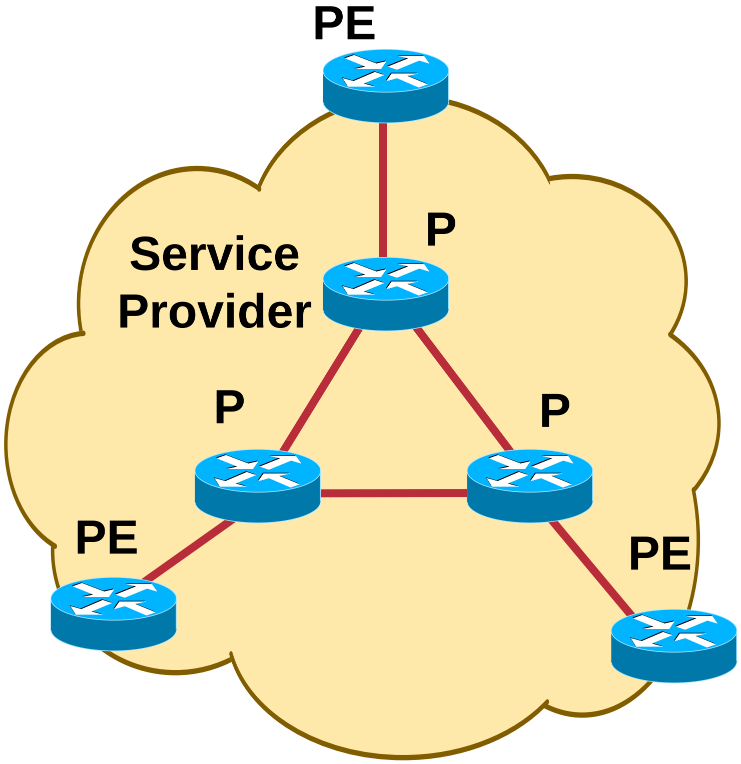
- SP enforces SLA using the output QoS policy on PE
- Output policy uses queuing, dropping and optionally, shaping
- Slow links require LFI/cRTP
- No input QoS policy on CE needed



- SP enforces SLA using the output QoS policy on PE
- Output policy uses queuing, dropping and optionally, shaping
- Slow links require LFI/cRTP
- Input QoS policy on CE irrelevant

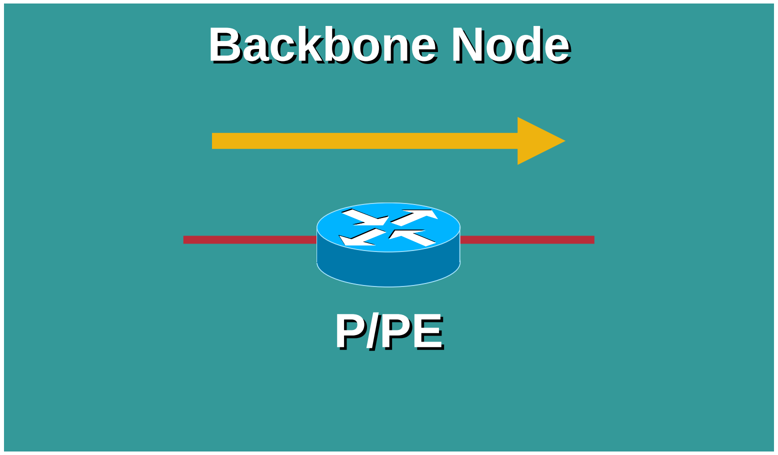
Define Policies
Service Provider Backbone (P to P)

- **QoS complexity resides at the edge**
- **Backbone only deals with classes**
- **Over-provisioning sometimes touted as best alternative**
  - **Expensive**
  - **DOS attacks**
  - **Failure conditions**
  - **Planning mistakes**
  - **Unexpected traffic demand**
  - **SP cannot generally solve end-to-end QoS for customers with over-provisioning**



Define Policies
Service Provider Backbone (P to P)

- SP implements SLA using output QoS policy
- Subset of classes may be used
- Typically, 2 or 3 classes (real time, business, BE)
- Output policy uses queuing and dropping
  - LLQ and WRED

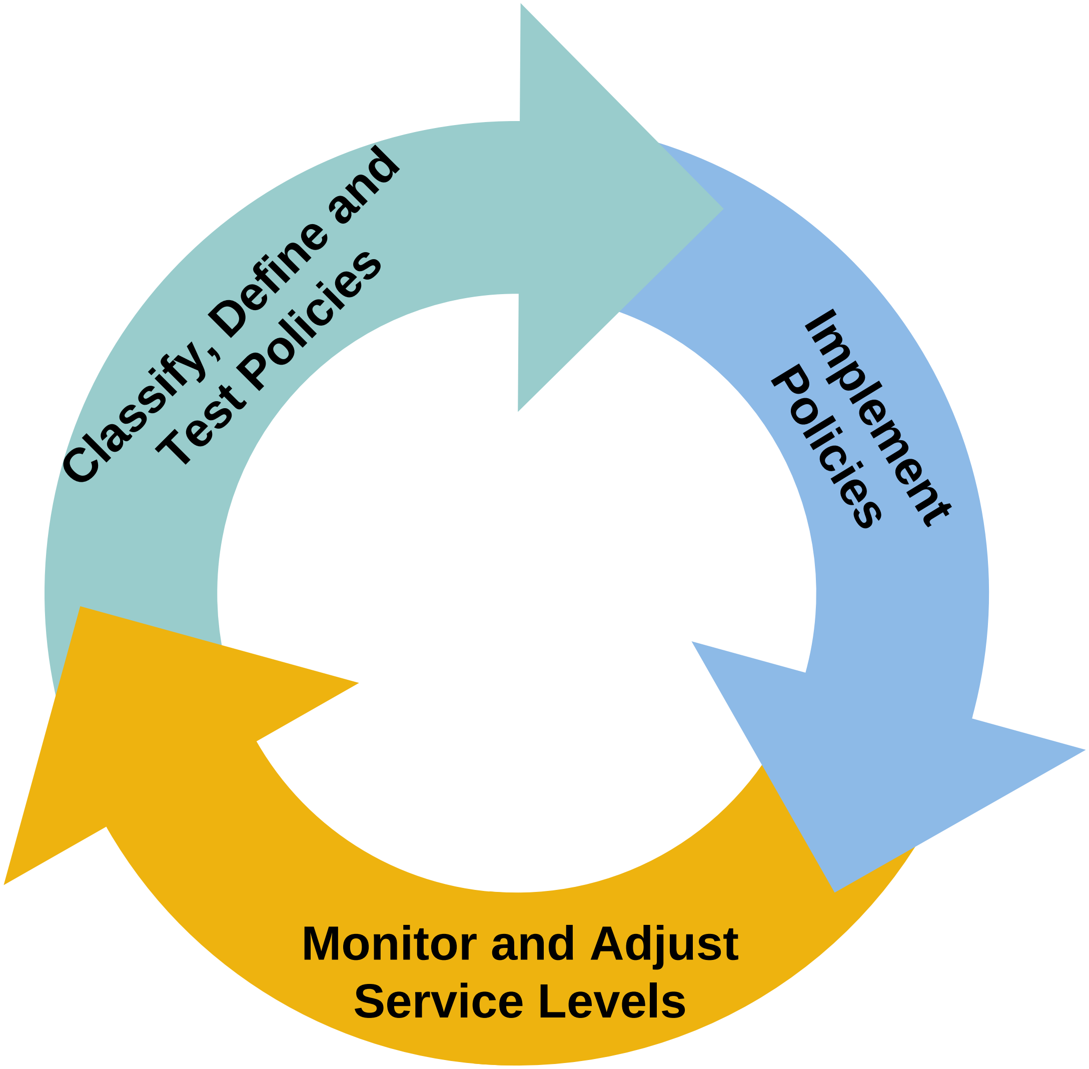


Deployment Guide: Summary

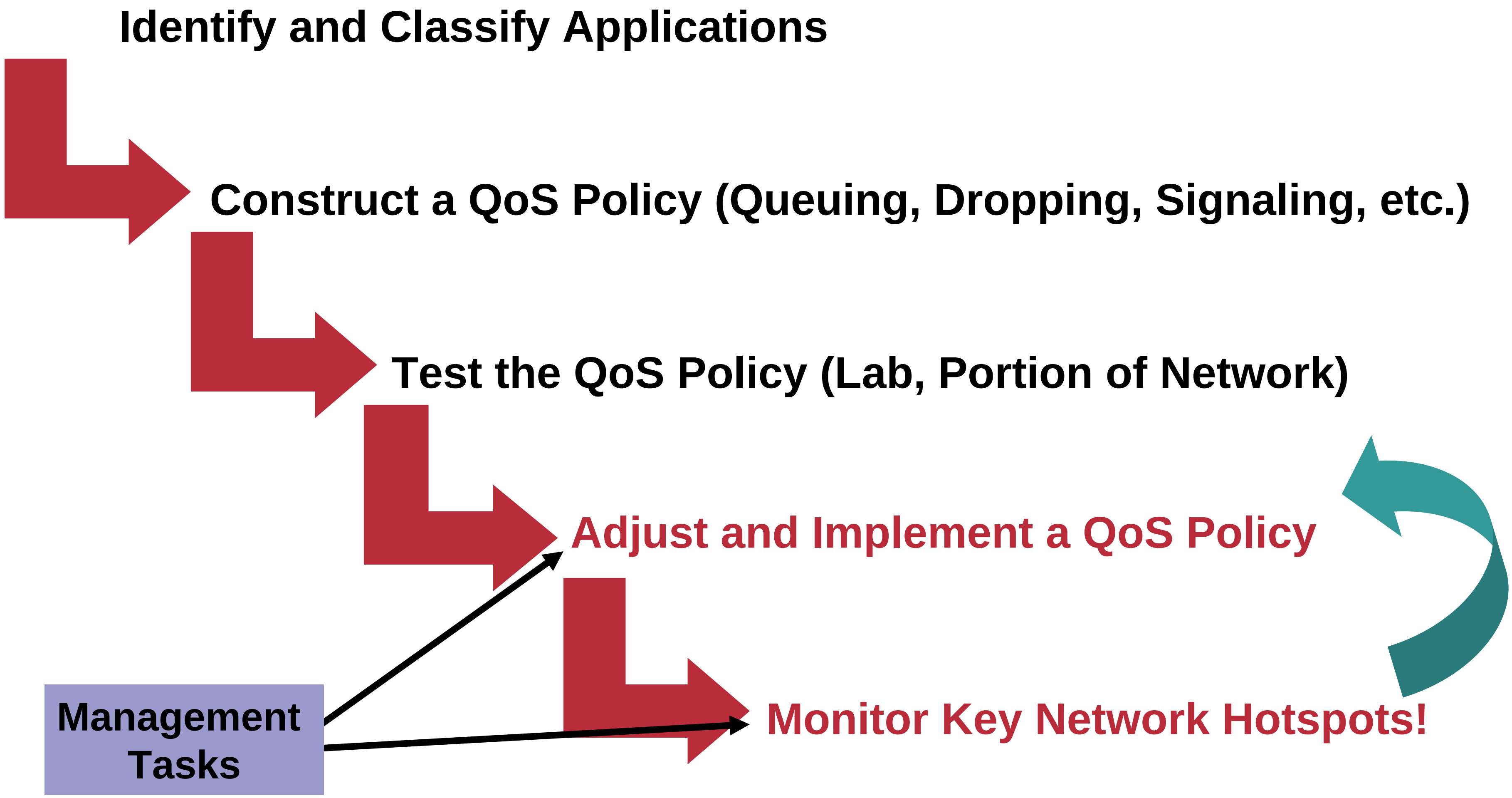
- Aggregation and speed transition links are potential choke points
- Buffer management, marking and policing in the campus, access and distribution layers
- Protect mission critical applications first
- Single class for latency sensitive traffic, additional traffic classes to implement data SLAs
- Optional class for routing and management traffic
- Less than best effort service for scavenger (P2P, worms) class
- Most other application traffic fall in Best-Effort class
- Point to point SLAs different from point to cloud SLAs
- Queuing and shaping enabled at the egress WAN edge
- Remarking and policing enabled at the ingress provider edge
- Queuing and WRED dropping enabled in the SP core

QoS MANAGEMENT

The QoS Management Circle


Classify, Define and Test Policies
Implement Policies
Monitor and Adjust Service Levels

Remember the Five Steps to Deploying QoS?



Identify and Classify Applications

Construct a QoS Policy (Queuing, Dropping, Signaling, etc.)

Test the QoS Policy (Lab, Portion of Network)

Adjust and Implement a QoS Policy

Monitor Key Network Hotspots!

Management Tasks

Adjust, Implement and Monitor QoS Policies

1. Provisioning QoS policies in large scale networks

   The Modular QoS CLI (MQC)

   Cisco Auto QoS

   Cisco QoS Policy Manager (QPM), Secure Device Manager (SDM) and Cisco Internet Solutions Center (ISC)

2. Monitoring QoS Policies

   Cisco IOS® Service Assurance Agent (SA Agent), CBQoSMIB and NBAR PD MIB

   CiscoWorks Service Management Solution (SMS), Infovista IV Suite, Concord e-Health

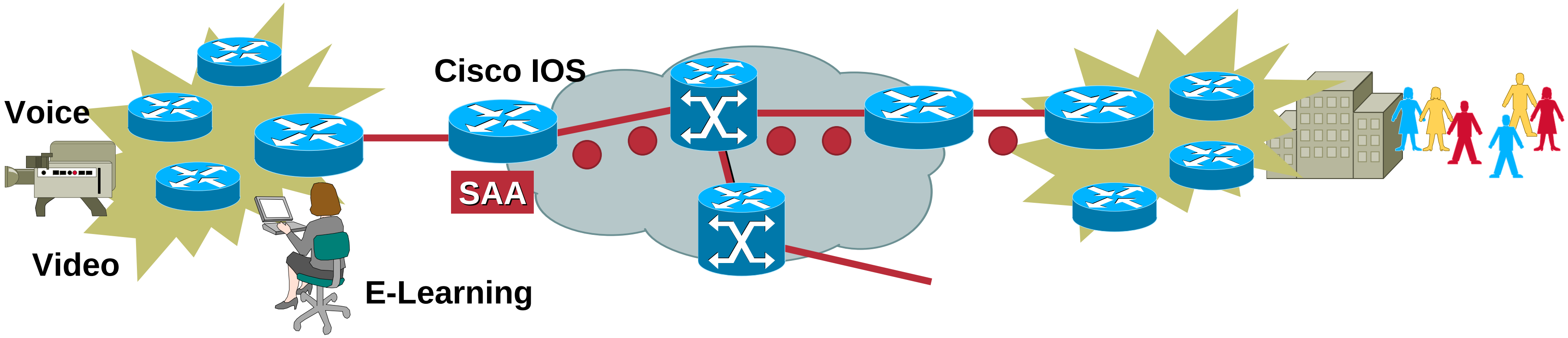
QoS Management

1. Service Assurance Agent
2. Cisco Class-Based QoS MIB
3. NBAR Protocol Discovery MIB

Service Assurance Agent (SAA)

Provides Active Monitoring of Network Infrastructure

- Is the packet loss acceptable?
- What is the network latency and application jitter?
- Are the network applications performing well?
- Can you monitor Service Level Agreements?



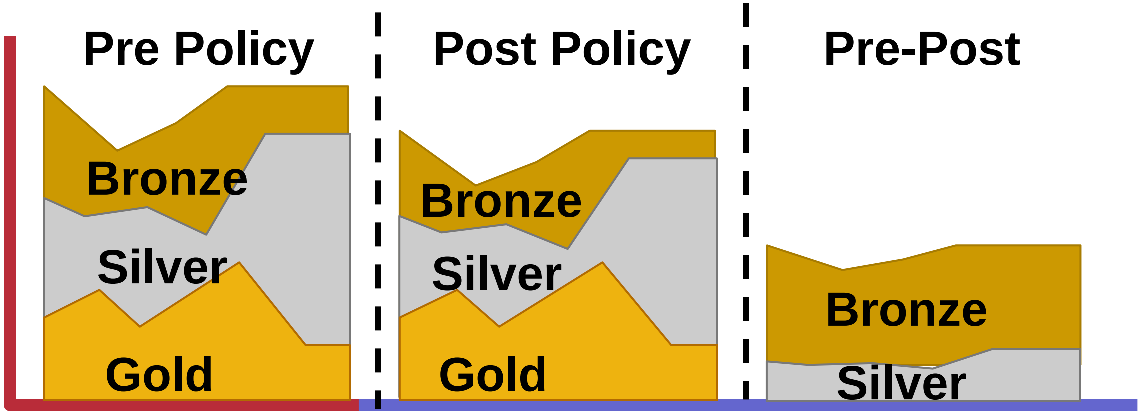
Service Assurance Agent (SAA): Measuring the Network

- **Active traffic generation within Cisco IOS® using SAA probes**
  - **Monitor network performance and health**
  - **Test and troubleshoot network problems**
- **Measurement of key end-to-end network metrics**
  - **Network delay, packet loss, network delay variation (jitter), connectivity status**
  - **History and distributions of network statistics**
- **Scheduling of application probes and threshold violation notification**

QoS Management

1. Service Assurance Agent
2. Cisco Class-Based QoS MIB
3. NBAR Protocol Discovery MIB

Class-Based QoS MIB (CBQoSMIB)



- **Primary accounting mechanism for MQC-based QoS**
- **Statistics for active MQC configurations on a per-policy/per-class, per-interface or PVC basis**
- **Monitor pre-and post-policy bit rates**

  For example, "How many packets are being dropped or marked?"
- **Read access only, no SNMP configuration**

QoS Management

1. Service Assurance Agent
2. Cisco Class-Based QoS MIB
3. NBAR Protocol Discovery MIB

Cisco NBAR Protocol Discovery MIB

Benefits

- Read/Write SNMP MIB support
- Real-time statistics on applications
- Per-interface, per-application, bi-directional (input and output) statistics
  - Bit rate (bps), Packet counts and Byte counts
- Top-N application views
- Application threshold settings

Cisco NBAR Protocol Discovery Statistics

```
router# sh run int fa6/0
!
interface FastEthernet0/0
 ip address 10.0.147.3 255.255.255.0
 ip nbar protocol-discovery
end

Router# show ip nbar protocol-discovery interface FastEthernet 6/0
   FastEthernet6/0
                         Input                                    Output
   Protocol                       Packet Count                             Packet Count
                                  Byte Count                               Byte Count
                                  5 minute bit rate (bps)                  5 minute bit rate (bps)
                                                                                         ---------
   http                           316773                                   0
                                  26340105                                 0
                                  3000                                     0
   pop3                           1487                                     7367
                                  2301891                                  339213
                                  3000                                     0
   snmp                           279538                                   14644
                                  319106191                                673624
                                  0                                        0
   ftp                            8979                                     7714
                                  906550                                   694260
                                  0                                        0
   …
   Total                          17203819                                 151684936
                                  19161397327                              50967034611
                                  4179000                                  6620000
```

Cisco NBAR Protocol Discovery Thresholds and Traps

- User can set thresholds on individual protocols on an interface, or on a statistic regardless of protocol
  - Multiple thresholds for any combination of supported protocols/and or all protocols
- Configurable statistic types
  - Interface in, out and sum of bytes, packets, and bit rate
- If the threshold is breached, the information is stored for prolonged period of time
- A notification (trap) is generated and sent to the user with a summary of threshold information

CASE STUDIES

Case Studies

- Securing the Network Infrastructure

  Control Plane Policing

- Deploying QoS for the Enterprise

  Accelerated Deployment via Cisco AutoQoS

- Site-to-Site VPN

  QoS for an Enterprise Running IPSec VPN End-to-End Through an SP Network

- Enterprise Network with IP Services

  QoS End-to-End Through an SP Network Selling IP Services

Securing the Network Infrastructure: Protecting the Control Plane

- Denial of Service (DoS) attacks generate IP traffic streams directed to the Route Processor (RP) at very high data rate
- Control plane is forced to spend an inordinate amount of time, processing this undesirable traffic
- QoS based Control Plane Policing (CoPP) guarantees the stability of the control plane and the ability to manage your network

  Single point of application for permit, deny and rate-limit policies

Securing the Network Infrastructure: Customer Example

- Large SP experienced a sudden surge of incoming Address Resolution Protocol (ARP) packets destined to their edge routers during a worm attack
- Sudden surge of ARP monopolized the Route Processor resources, starving other important processes and resulting in a high CPU %
- Customer defined a Control Plane Policing Policy to limit the ARP packets that access the RP and protect the CPU

```
Class-map copp-arp
 Match protocol arp
Policy-map control-plane
 Class-map copp-arp
   police 8000 1500 1500 conform-action transmit
exceed-action drop
```

Case Studies

- Securing the Network Infrastructure

  Control Plane Policing

- Deploying QoS for the Enterprise

  Accelerated Deployment via Cisco AutoQoS

- Site-to-Site VPN

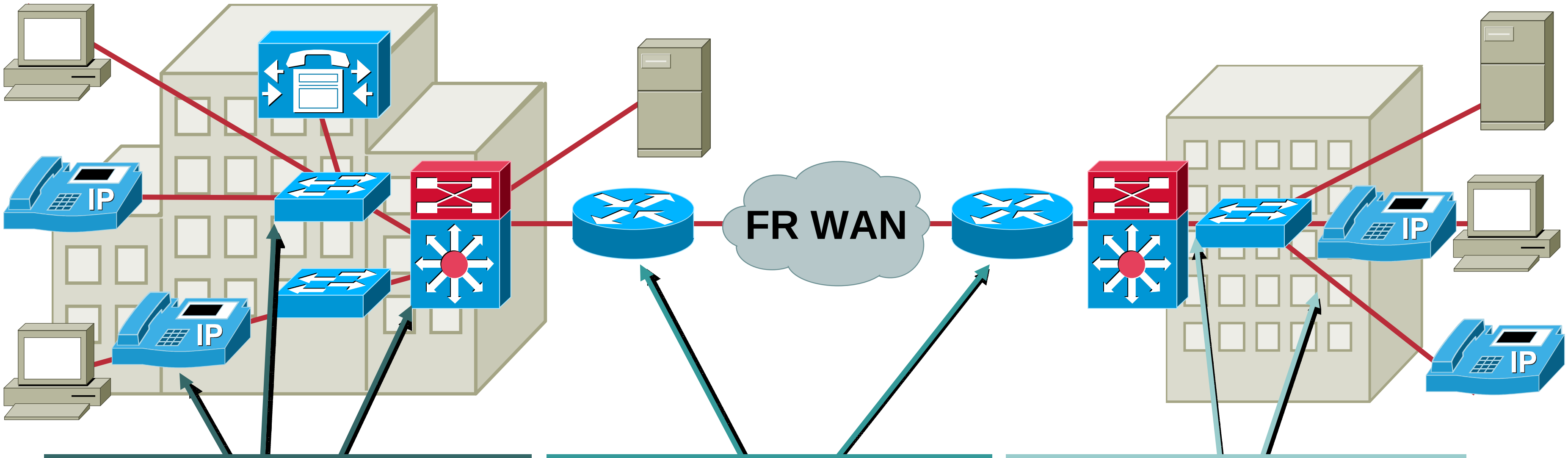
  QoS for an Enterprise Running IPSec VPN End-to-End Through an SP Network

- Enterprise Network with IP Services

  QoS End-to-End Through an SP Network Selling IP Services

Deploying QoS for the Enterprise

Goal: Deploy Consistent, End-to-End QoS for V/V/D



Access Layer	WAN	Distribution Layer
Classification and Trust Boundary Marking/Remarking Egress Queue Scheduling Buffer Management	Intelligent Classification Bandwidth Provisioning Admission Control Shaping Link Fragmentation and Interleaving Header Compression	Layer 3 Policing Egress Scheduling (Multiple Queues with WRR) Priority Queuing for VoIP Buffer Management

Cisco AutoQoS in the LAN

- **Simplified QoS configuration**
- **Optimal voice performance**
  - **Parameters based on Cisco Best Practices, extensive lab testing, and input from a broad base of AVVID installations**
- **Intelligent policy generation**
  - **Support for Cisco IP Phone and Cisco Soft Phone**
  - **Automatically decides on trust and extended trust boundary settings**
  - **Configures CoS to DSCP to Queue mapping, WRR settings, etc.**

Cisco AutoQoS in the LAN (Cont.)

Catalyst® 6500 Series Switch

User Enables AutoQoS

```
set port macro 4/1 ciscoipphone 10 110
```

Port 4/1 has been fully configured for ciscoipphone. Data vlan set to 10, auxiliary vlan set to 110, port based autoqos configured

Global autoqos configured on all ports.

```
set qos autoqos
```

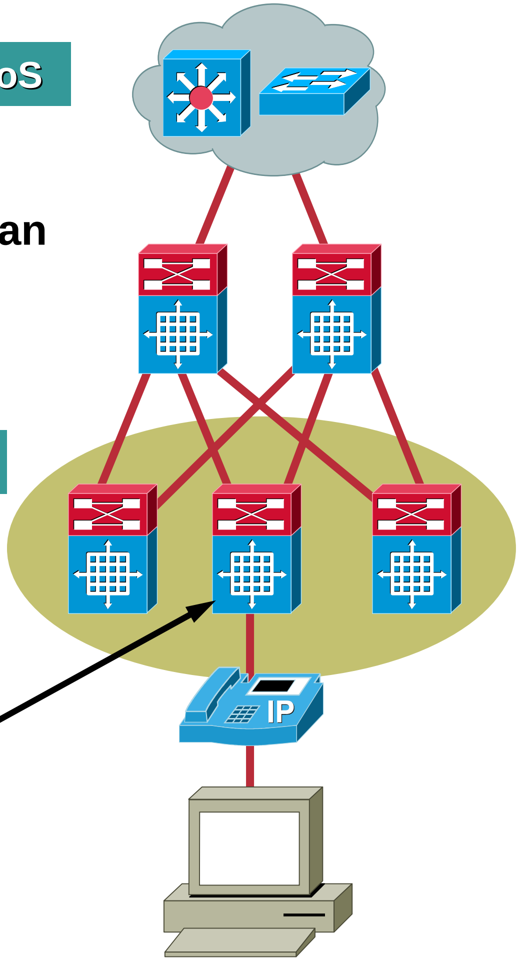
Generated by AutoQoS

All ingress and egress QoS scheduling parameters configured on all ports. CoS to DSCP, DSCP to COS and IP Precedence to DSCP maps configured. Global QoS configured

```
set port qos autoqos 4/1 voip ciscoipphone
```

Port 4/1 has been fully configured for voip. Global autoqos configured on all ports

Generated by AutoQoS



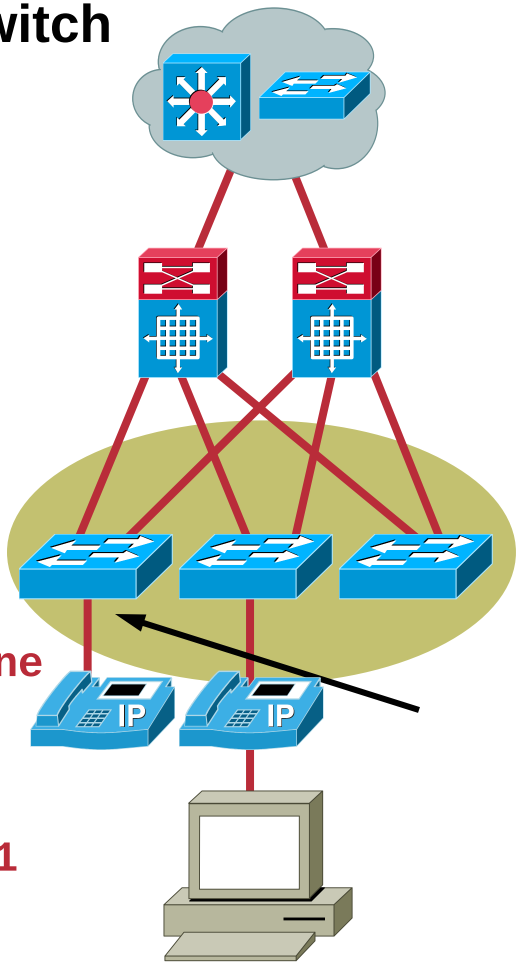
Cisco AutoQoS in the LAN (Cont.)

Catalyst 3550 Series Switch

```
Interface FastEthernet0/1
mls qos trust device cisco-phone
mls qos trust cos
auto qos voip cisco-phone
wrr-queue bandwidth 20 1 80 0
wrr-queue min-reserve 1 5
wrr-queue min-reserve 2 6
wrr-queue min-reserve 3 7
wrr-queue min-reserve 4 8
wrr-queue cos-map 1 0 1 2 4
wrr-queue cos-map 3 3 6 7
wrr-queue cos-map 4 5
priority-queue out
```

You Enable AutoQoS

Generated by AutoQoS



```
Interface GigabitEthernet0/1
mls qos trust device cisco-phone
mls qos trust cos
auto qos voip cisco-phone
wrr-queue bandwidth 20 1 80 0
wrr-queue queue-limit 80 1 20 1
wrr-queue cos-map 1 0 1 2 4
wrr-queue cos-map 3 3 6 7
wrr-queue cos-map 4 5
priority-queue out
```

You Enable AutoQoS

Generated by AutoQoS

Deploying QoS for the Enterprise: Cisco AutoQoS in the WAN

- Simplifies QoS configuration for voice, video, data in two simple steps
- Automatically discovers statistics for all applications and protocols using NBAR/DSCP
- Automatically provisions up to 10 classes of service
- Generated parameters and configuration can be user modified
- Intelligent policy generation
    - Based on underlying network environment and site specific network traffic profile
    - Automatically enables required Link Specific QoS settings

Deploying QoS for the Enterprise: Cisco AutoQoS in the WAN

Comprehensive QoS Deployment in Two Steps

- **Run AutoDiscovery to profile traffic:**

  Collects data from the offered traffic for several days, a week, etc., as desired:

  Uses NBAR-based protocol discovery

  Performs statistical analysis

- **Generate and deploy MQC-based QoS policies:**

  Maps applications to their corresponding DiffServ classes

  Assigns appropriate values for bandwidth and scheduling parameters

Procedure:

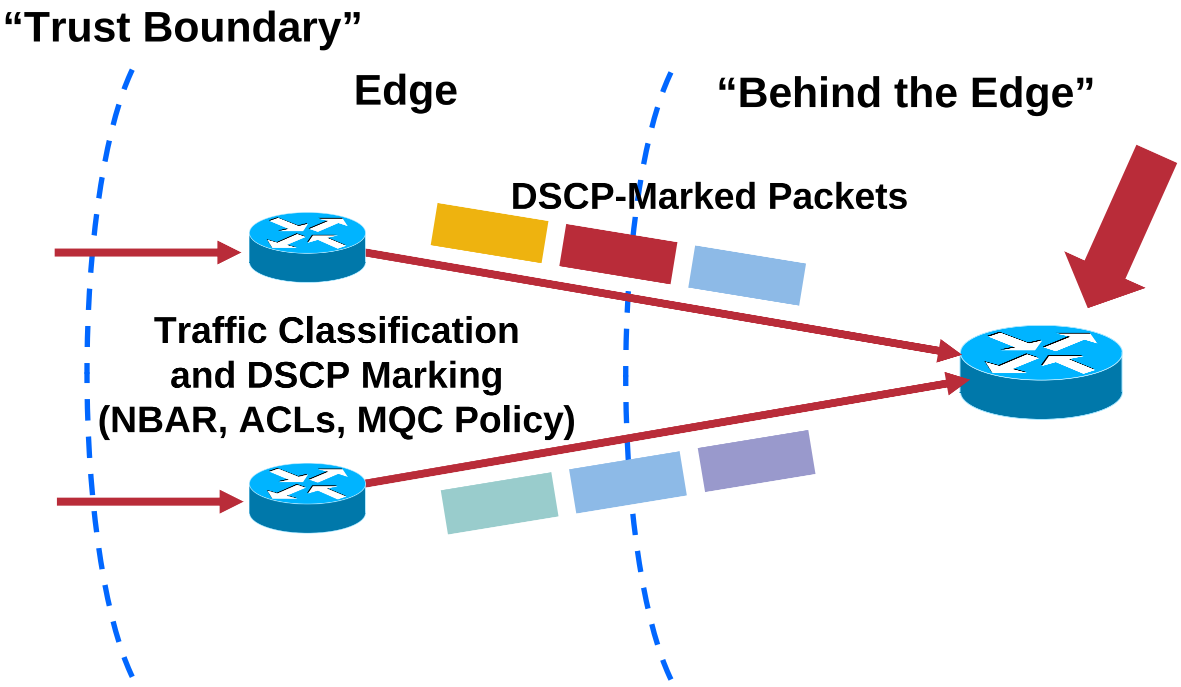
1. Invoke "auto discovery qos <trust>“ on the applicable link in “trust” or “untrust” mode

   Use "show auto discovery qos“ to view data collection in progress and recommended QoS policy

2. Automatically configure the link with “auto qos” command

   Use "show auto qos" to display the QoS policy settings deployed

AutoQoS for the Enterprise: “Trust” Option for Auto Discovery


“Trust Boundary”
Edge
“Behind the Edge”
DSCP-Marked Packets
Traffic Classification and DSCP Marking (NBAR, ACLs, MQC Policy)

>auto discovery **trust**

- **Use when DSCP values already assigned**

  AutoDiscovery does not inspect and reclassify traffic

  QoS policy based on statistics for DSCP-marked traffic received by router

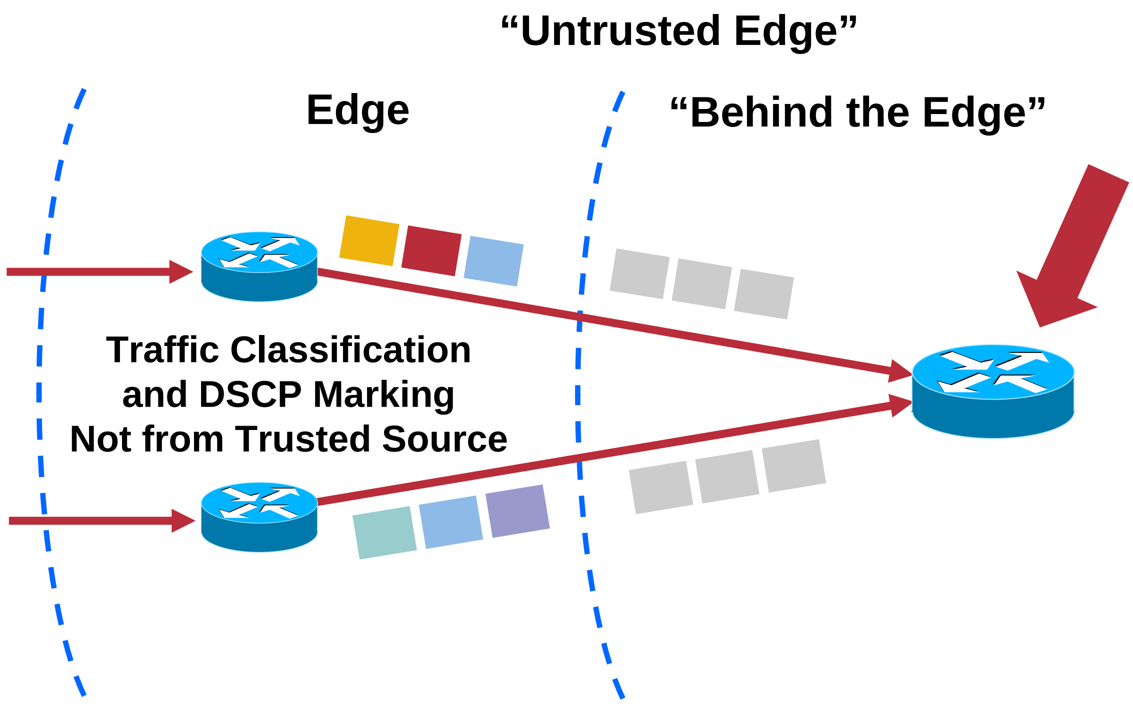
ACL = Access Control List

DSCP = Differentiated Services Code Point

MQC = Modular Quality-of-Service (QoS) Command Line Interface (CLI)

NBAR = Network-Based Application Recognition

AutoQoS for the Enterprise: “Untrust” Option for Auto Discovery



>auto discovery

- This is the default mode for enabling Auto Discovery
- Use when DSCP values and markings are not trusted

  AutoDiscovery inspects the traffic based on application properties using NBAR

  QoS policy based on statistics obtained using NBAR Protocol Discovery

ACL = Access Control List

DSCP = Differentiated Services Code Point

MQC = Modular Quality-of-Service (QoS) Command Line Interface (CLI)

NBAR = Network-Based Application Recognition

Deploying QoS for the Enterprise: AutoQoS DiffServ Class Provisioning

Auto Discovery	Cisco Auto QoS Policy
Application and Protocol-Types	Cisco Auto QoS Classmaps Match Statements
Offered Bit Rate (Average and Peak)	Minimum Bandwidth to Class Queues, Scheduling and WRED

Traffic Class	DSCP
IP Routing	CS6
Interactive Voice	EF
Interactive Video	AF41
Streaming Video	CS4
Telephony Signaling	CS3
Transactional/Interactive	AF21
Network Management	CS2
Bulk Data	AF11
Scavenger	CS1
Best Effort	0

11/03

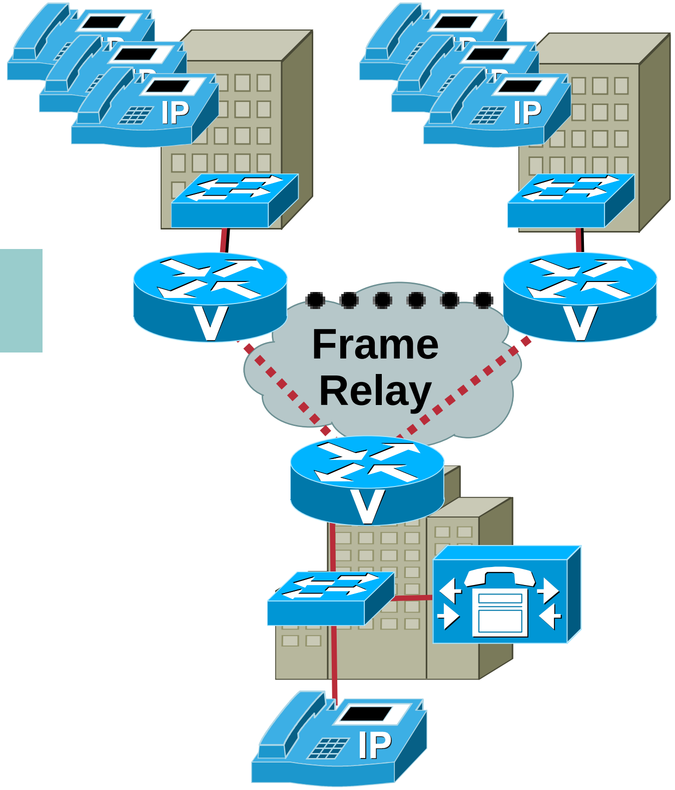
Deploying QoS for the Enterprise: Cisco AutoQoS in the WAN

With Cisco AutoQoS

```
interface Serial4/0 point-to-point
Encapsulation frame-relay
bandwidth 256
ip address 10.1.71.1 255.255.255.0
frame-relay interface-dlci 100
  auto discovery qos
```

Specify BW, IP Addr and FR DLCI

Enable Auto Discovery



Auto Discovery Notes

- Command should be enabled on interface of interest
- Do not change interface bandwidth when running auto discovery
- Cisco Express Forwarding must be enabled
- All previously attached QoS policies must be removed from the interface

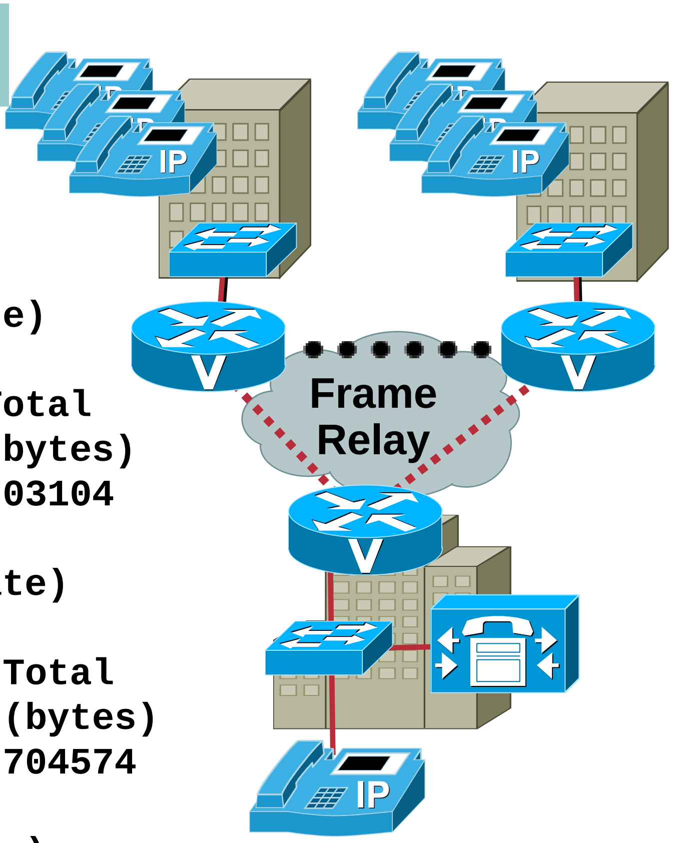
Deploying QoS for the Enterprise: Cisco AutoQoS in the WAN (Cont.)

With
Cisco AutoQoS

```
show auto discovery qos
```

Review the Generated QoS Policy/Statistics

```
AutoQoS Discovery enabled for applications
 Discovery up time: 2 days, 55 minutes
 AutoQoS Class information:
 Class VoIP:
  Recommended Minimum Bandwidth: 517 Kbps/50% (PeakRate)
  Detected applications and data:
  Application/       AverageRate        PeakRate     Total
  Protocol           (kbps/%)           (kbps/%)     (bytes)
  rtp audio          76/7               517/50       703104
 Class Interactive Video:
  Recommended Minimum Bandwidth: 24 Kbps/2% (AverageRate)
  Detected applications and data:
  Application/       AverageRate        PeakRate      Total
  Protocol           (kbps/%)           (kbps/%)      (bytes)
  rtp video          24/2               5337/52       704574
 Class Transactional:
  Recommended Minimum Bandwidth: 0 Kbps/0% (AverageRate)
  Detected applications and data:
  Application/       AverageRate        PeakRate      Total
  Protocol           (kbps/%)           (kbps/%)      (bytes)
  citrix               36/3                 74/7      30212
  sqlnet               12/1                 7/<1      1540
```



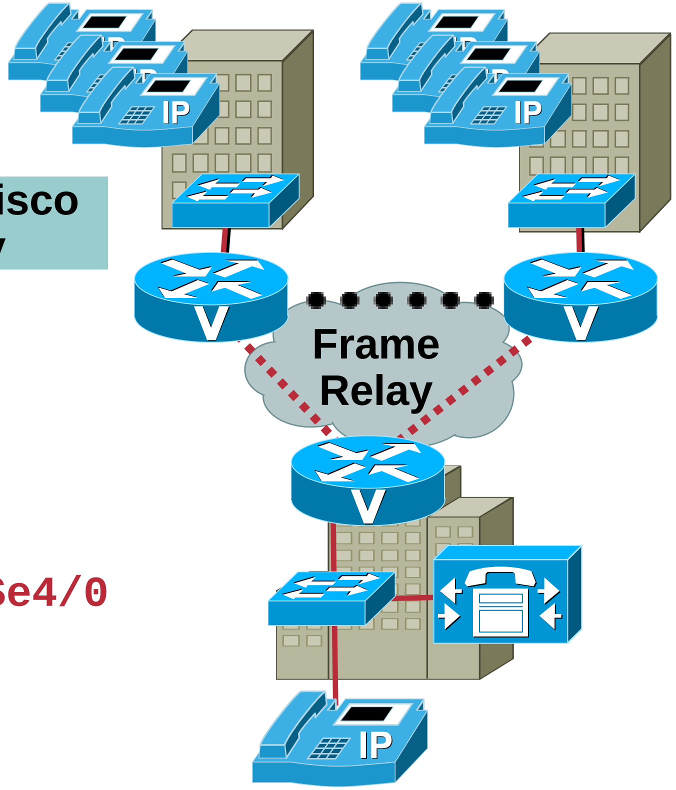
Deploying QoS for the Enterprise: Cisco AutoQoS in the WAN (Cont.)

With
Cisco AutoQoS

```
interface Serial4/0 point-to-point
 bandwidth 256
 ip address 10.1.71.1 255.255.255.0
frame-relay interface-dlci 100
  auto qos
```

Apply Generated Cisco AutoQoS Policy

```
  policy-map AutoQoS-Policy-Se4/0-Parent
     class class-default
     shape average 256000
      service-policy AutoQoS-Policy-Se4/0
  !
   class-map match-any AutoQoS-Transactional-Se4/0
    match protocol sqlnet
    match protocol citrix
   class-map match-any AutoQoS-Voice-Se4/0
    match protocol rtp audio
   class-map match-any AutoQoS-Inter-Video-Se4/0
    match protocol rtp video
```

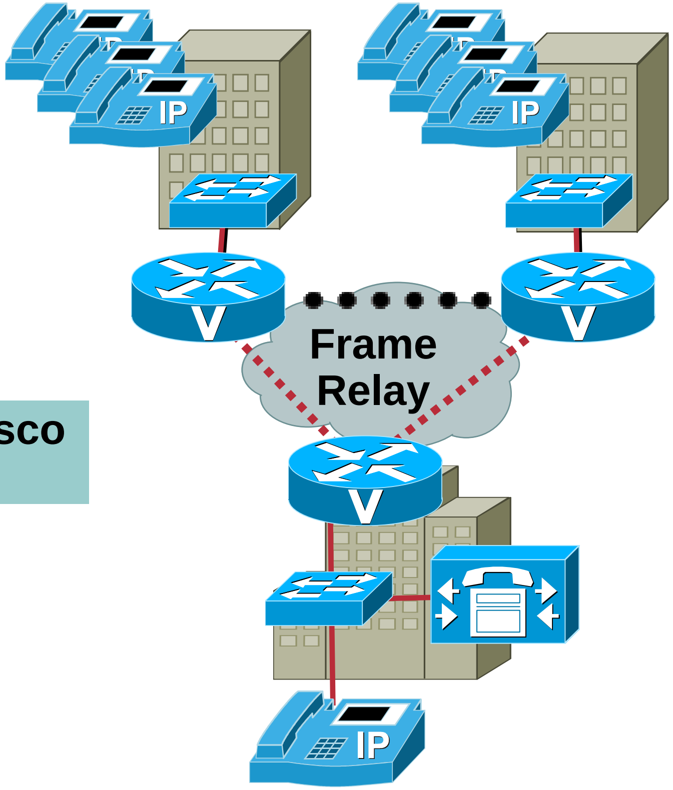


Deploying QoS for the Enterprise: Cisco AutoQoS in the WAN (Cont.)

With Cisco AutoQoS

```
policy-map AutoQoS-Policy-Se4/0
   class AutoQoS-Voice-Se4/0
    priority percent 70
    set dscp ef
   class AutoQoS-Inter-Video-Se4/0
    bandwidth remaining percent 10
    set dscp af41
   class AutoQoS-Transactional-Se4/0
  bandwidth remaining percent 1
    set dscp af21
   class class-default
    fair-queue
!
interface Serial4/0 point-to-point
  frame-relay interface-dlci 100
   class AutoQoS-FR-Serial4/0-100
!
map-class frame-relay AutoQoS-FR-Serial4/0-100
frame-relay cir 256000
frame-relay mincir 256000
frame-relay fragment 320
service-policy output AutoQoS-Policy-Se4/0-Parent
```

Apply Generated Cisco AutoQoS Policy



Deploying QoS for the Enterprise: Cisco AutoQoS in the WAN (Cont.)

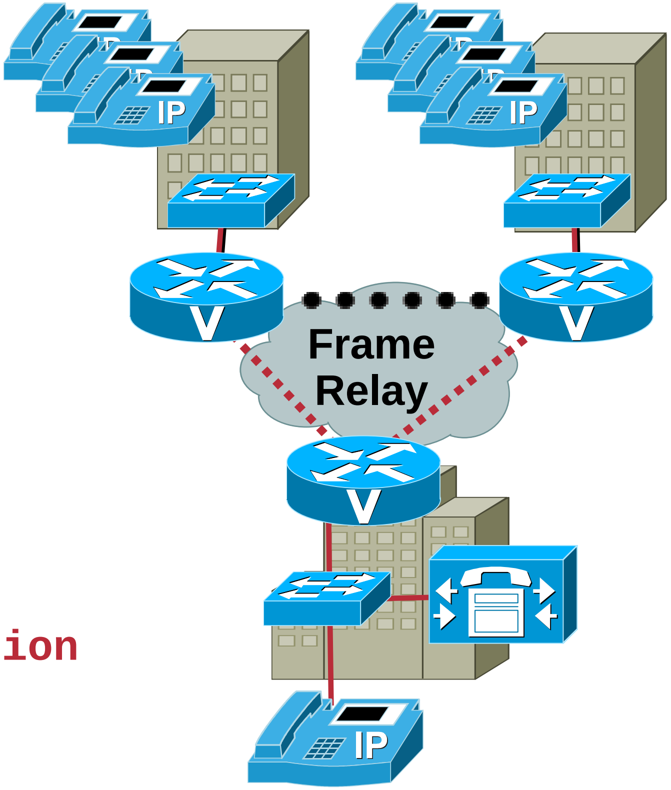
With Cisco AutoQoS

- **Provides Remote Monitoring (RMON) alerts, if packets are dropped**

  Thresholds are activated in RMON alarm table to monitor drops in Voice Class

  Default drop threshold is 1bps

  Provisioning and monitoring support added via Security Device Manager (SDM)



```
rmon event 33333 log trap AutoQoS description
“AutoQoS
SNMP traps for Voice Drops” owner AutoQoS

rmon alarm 33350 cbQoSCMDDropBitRate.2881.2991 30
Absolute rising-threshold 1 33333 falling-threshold 0
Owner AutoQoS
```

RMON Event Configured and Generated by Cisco AutoQos

Case Studies

- Securing the Network Infrastructure

  Control Plane Policing

- Deploying QoS for the Enterprise

  Accelerated Deployment via Cisco AutoQoS

- Site-to-Site VPN

  QoS for an Enterprise Running IPSec VPN End-to-End Through an SP Network

- Enterprise Network with IP Services

  QoS End-to-End Through an SP Network Selling IP Services

Site-to-Site VPN: Requirements

- Enterprise customer buys a point to point service from service provider and requires 4 classes of service:

  Real-time (Voice): no loss, low latency, low jitter, guaranteed bandwidth

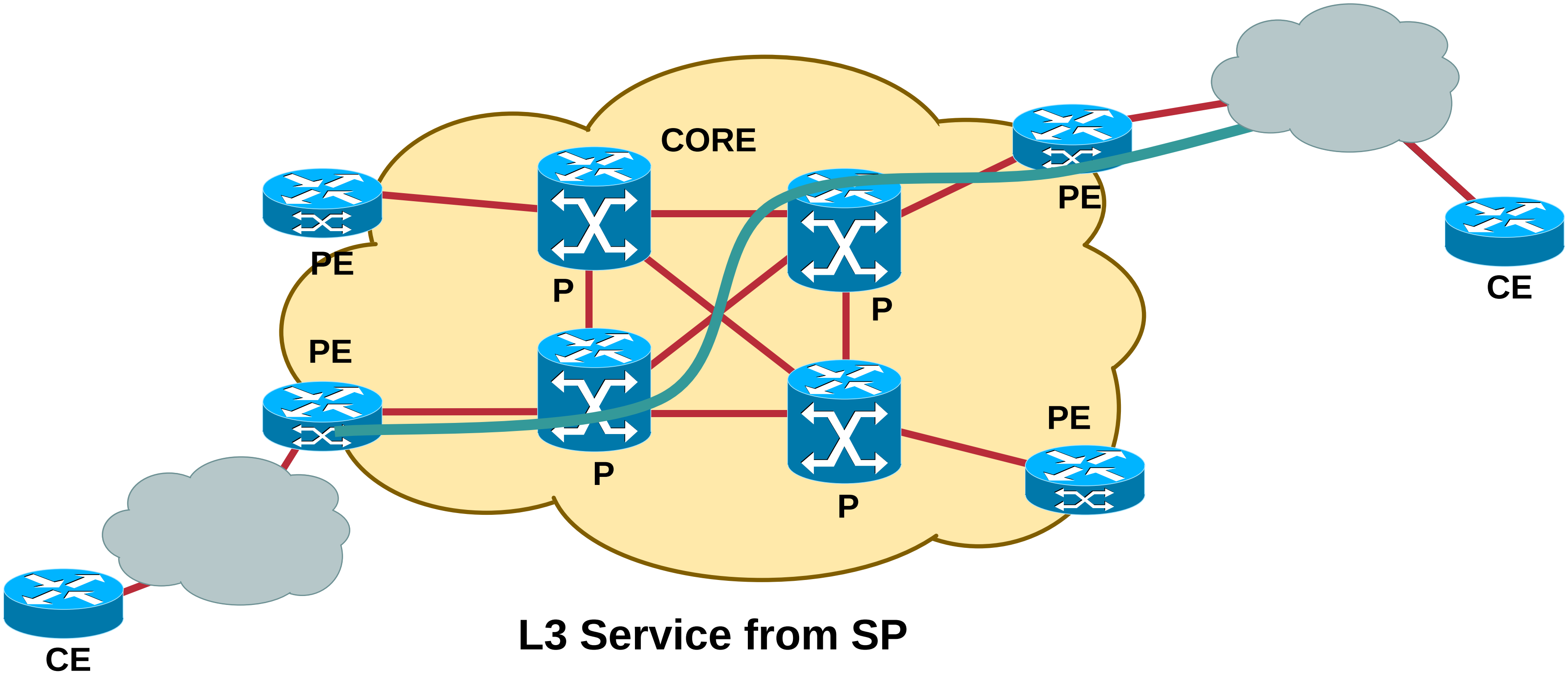
  Business Class (ERP applications): low loss, guaranteed bandwidth

  Interactive Class (Telnet,): low loss, low latency, guaranteed bandwidth

  Normal (other traffic): Best Effort

- Site-to-Site VPN service, two site example

Site-to-Site VPN: Topology



L3 Service from SP

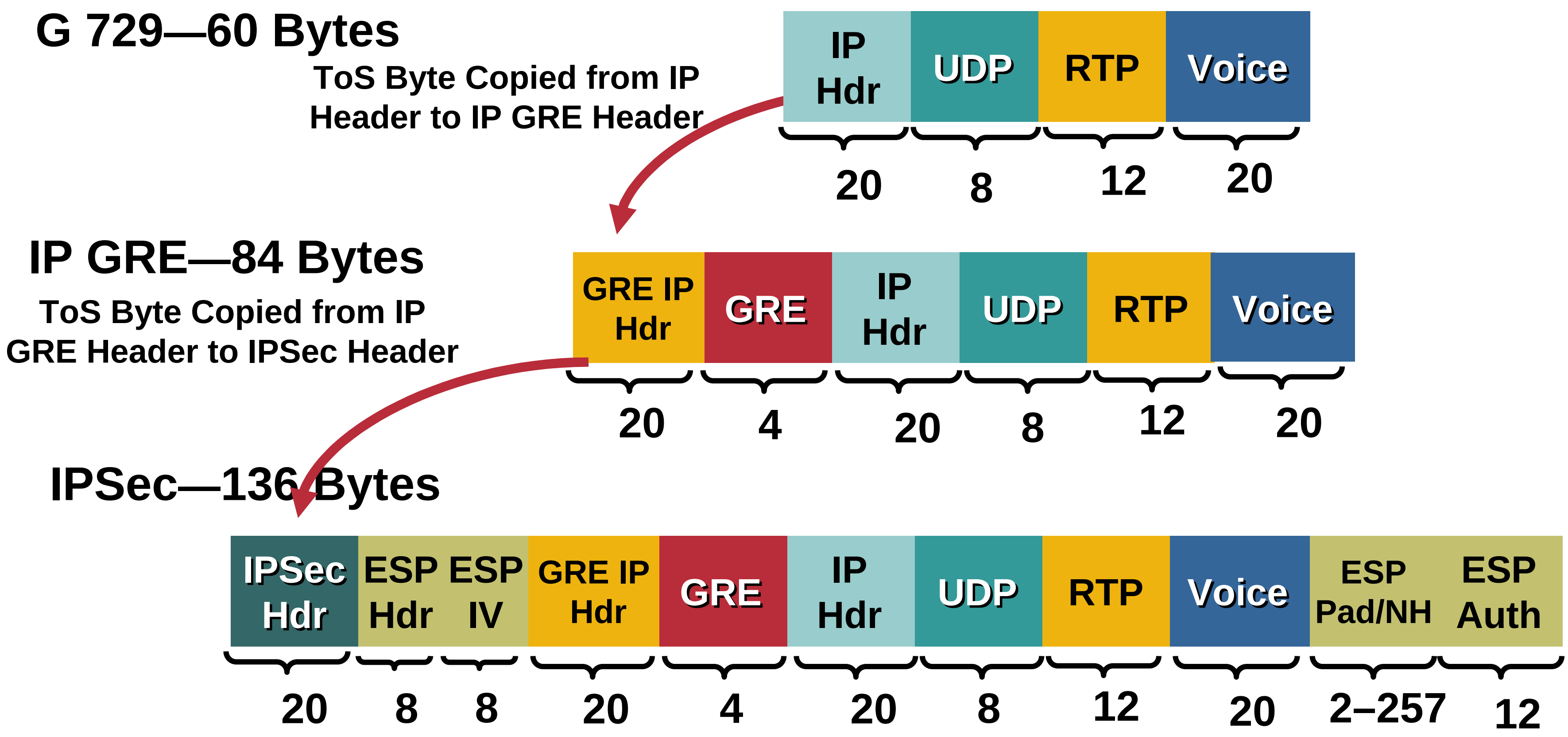
Customer Needs Site-to-Site IP VPN Service with 4 Different Service Classes

Site-to-Site VPN: Issues

QoS Requirements Are the Same Except

- Additional header and trailer overhead of IPSec and GRE
- Voice delay budget increased by crypto engine processing
- Crypto engines randomly drops packets when congested
  - Voice quality suffers through IPSec tunnel
- RTP Header Compression and IPSec are incompatible standards
- Voice and data in same IPSec/GRE tunnel, both encrypted
- QoS reordering of IPSec sequenced packets can lead to anti-replay drops

Site-to-Site VPN Issues: G 729 CODEC Overhead with GRE and IPSec



G 729—60 Bytes

ToS Byte Copied from IP Header to IP GRE Header

IP Hdr	UDP	RTP	Voice
20	8	12	20

IP GRE—84 Bytes

ToS Byte Copied from IP GRE Header to IPSec Header

GRE IP Hdr	GRE	IP Hdr	UDP	RTP	Voice
20	4	20	8	12	20

IPSec—136 Bytes

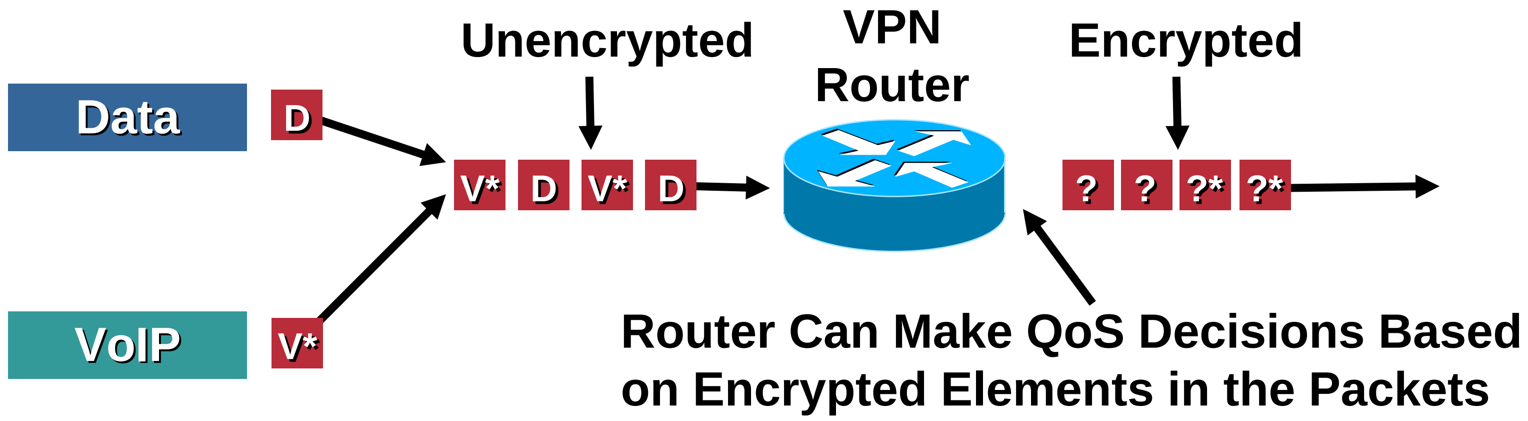
IPSec Hdr	ESP Hdr	ESP IV	GRE IP Hdr	GRE	IP Hdr	UDP	RTP	Voice	ESP Pad/NH	ESP Auth
20	8	8	20	4	20	8	12	20	2–257	12

Resulting Layer 3 Packet Sizes:

G.729 = 136 bytes @ 50 pps = 54.4 kbps

G.711 = 280 bytes @ 50 pps = 112 kbps

Site-to-Site VPN: When to Use QoS Pre-Classify


Data
D
VoIP
V*
Unencrypted
V* D V* D
VPN Router
Encrypted
? ? ?* ?*
Router Can Make QoS Decisions Based on Encrypted Elements in the Packets

- Currently required when using hardware encryption and service-policy on output interface
- Maintains original IP Header (port, protocol, source/dest IP address, etc.) for output QoS policy
- Unrequired when QoS policy uses ToS byte only
- Apply to both crypto map and IP GRE tunnel (if IP GRE is used)

Case Studies

- Securing the Network Infrastructure

  Control Plane Policing

- Deploying QoS for the Enterprise

  Accelerated Deployment via Cisco AutoQoS

- Site-to-Site VPN

  QoS for an Enterprise Running IPSec VPN End-to-End Through an SP Network

- Enterprise Network with IP Services

  QoS End-to-End Through an SP Network Selling IP Services

Enterprise Network with IP Services: The WAN

- SP sells L3 services with following four levels of service

  Real-Time

  Business High

  Business Low

  Best Effort

- Business driver for Enterprise—ad-hoc any to any video conferencing from more than 60 sites across the US

  Each site connected via T1 connection at minimum

  VC units run standard 384Kbps IPVC streams

- Customer also has several mission critical business applications that need prioritization

- Managed CE environment

Enterprise Network with IP Services: Challenges

- Point-to-cloud model—SP is involved in QoS
- Challenges

  Current provisioning mechanism guaranteed more than 150% of available bandwidth

  No accounting for routing protocols and L2 overhead

  SP not preserving DSCP marking across their cloud—Remark DSCP to indicate to themselves whether packets are within or violating contract

  DLSW+ application configured to set its ToS value to 5 by default (same as IPVC)

Enterprise Network with IP Services: the Solution

- Customer purchased services in the ratio 5:6:2:1
- Customer migrated to a complete DSCP model
  - Simpler from a classification and provisioning perspective
  - Monitoring and management advantages
- Workaround for SP remarking: NBAR deployed at WAN edge to re-classify and re-mark INBOUND traffic from the WAN
- Routing and control traffic in business high class
- Percentage based provisioning mechanism
- QoS Policy Manager (QPM) for monitoring traffic statistics via CBQoSMIB

Enterprise Network with IP Services: Configuration

```
class-map match-all VIDEO
  match access-group 120
class-map match-all SAP
  match protocol custom-10
class-map match-all SNA
  match protocol dlsw
class-map match-all TELNET
  match protocol telnet
class-map match-all NOTES
  match protocol notes
class-map match-any WWW
  match protocol http
  match protocol secure-http
class-map match-all FTP-GRAPHICS
  match access-group 105
  match protocol ftp
```

```
class-map match-all REAL-TIME
  match ip dscp ef
class-map match-any BUSINESS-HIGH
  match ip dscp af31
  match ip dscp af32
  match ip dscp af33
  match ip dscp cs3
class-map match-any BUSINESS-LOW
  match ip dscp af21
  match ip dscp af22
  match ip dscp af23
```

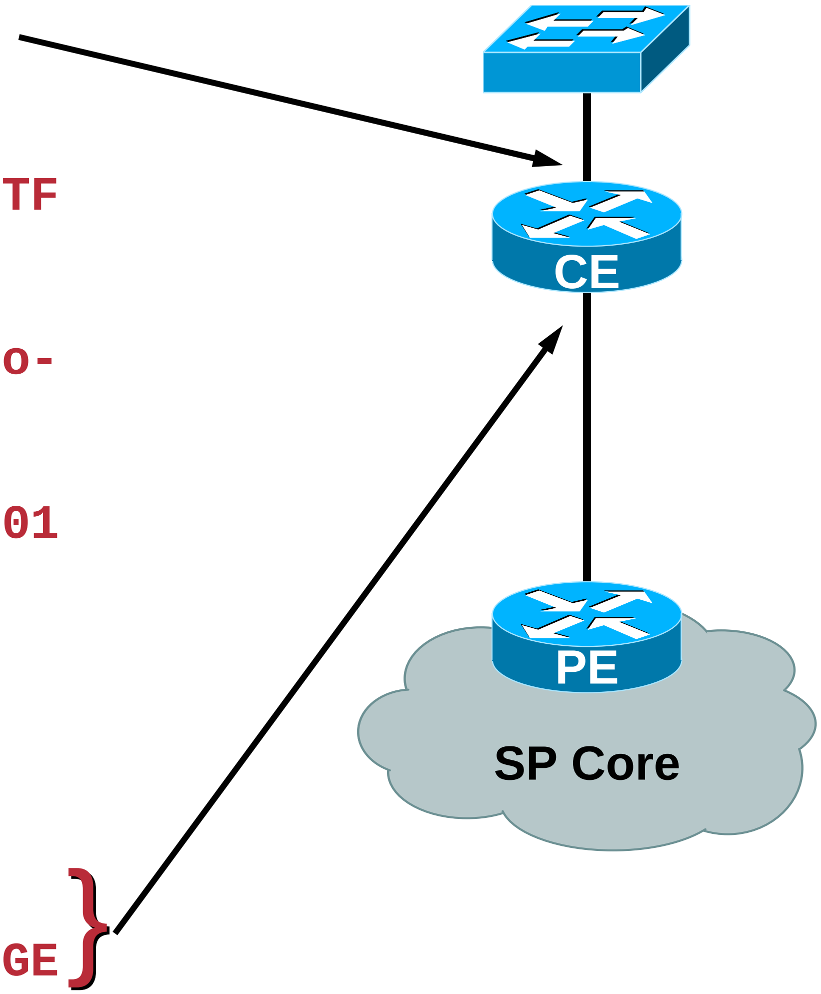
Enterprise Network with IP Services: Configuration (Cont.)

```
policy-map MARKING
  class VIDEO
   set ip dscp ef
  class SAP
   set ip dscp af31
  class SNA
   set ip dscp af32
  class TELNET
   set ip dscp af33
  class NOTES
   set ip dscp af21
  class WWW
   set ip dscp af22
  class FTP-GRAPHICS
   set ip dscp af23
  class SCAVENGER
   set ip dscp cs1
  class class-default
   set ip dscp default
```

```
policy-map WAN-EDGE
  class REAL-TIME
    priority 512
  class BUSINESS-HIGH
   bandwidth percent 45
   random-detect dscp-based
  class BUSINESS-LOW
   bandwidth percent 15
   random-detect dscp-based
  class SCAVENGER
   bandwidth percent 1
  class class-default
   fair-queue
   random-detect dscp-based
```

Enterprise Network with IP Services: Configuration (Cont.)

```
interface FastEthernet0/0
 service-policy input MARKING
!
interface Serial0/0
 encapsulation frame-relay IETF
 frame-relay traffic-shaping
!
interface Serial0/0.1 point-to-
point
 description SP Ckt
 frame-relay interface-dlci 101
  class FRTS
!
map-class frame-relay FRTS
 frame-relay cir 1536000
 frame-relay bc 15360
 frame-relay mincir 1536000
 service-policy input MARKING
 service-policy output WAN-EDGE
```



SUMMARY

Summary

- QoS must be deployed end-to-end to be effective
- Newer QoS tools enable easier deployment and more sophisticated Service Level Agreements (SLAs)
- Enterprise WAN edge QoS is dependent on the kind of service that is purchased from the service provider
- Lots of tools for QoS provisioning and management

Complete Your Online Session Evaluation!

WHAT: Complete an online session evaluation and your name will be entered into a daily drawing

WHY: Win fabulous prizes! Give us your feedback!

WHERE: Go to the Internet stations located throughout the Convention Center

HOW: Winners will be posted on the onsite Networkers Website; four winners per day

Cisco Systems