Voice over IP

SWITCH Module 7

Agenda

- Intro
- Quality of Service
- VoIP and QoS Configuration for Catalyst
- Power over Ethernet

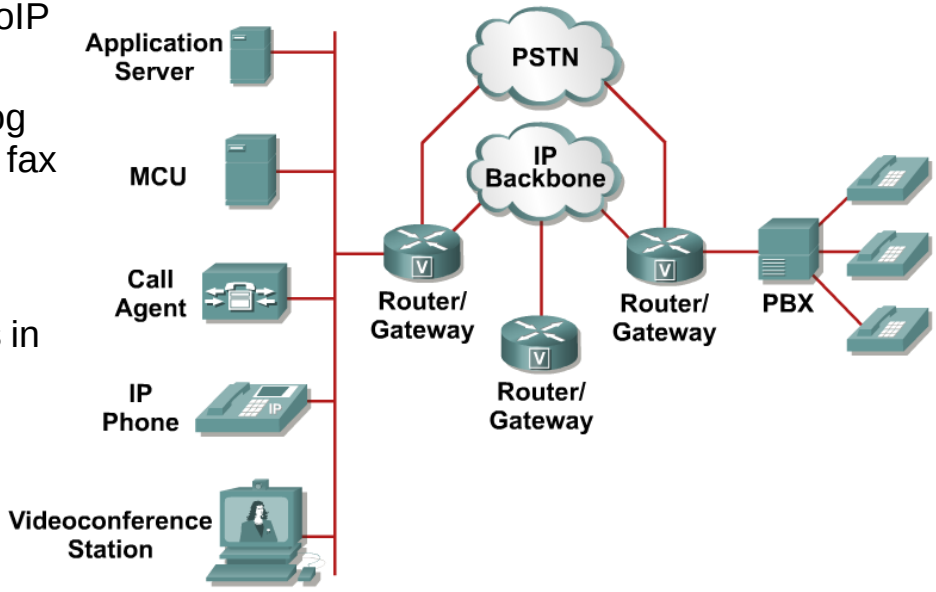
VoIP Intro

Voice over IP

- **VoIP** = delivery of voice communications over IP networks
- VoIP became IP telephony – telephony services (voice, fax, sms, chat, …) are transported via the IP network, rather than the public switched telephone network (PSTN)
- IP Communications (Unified Communications) combine telephone service, faxes, voicemail, e-mail, chat, web conferences etc.

VoIP Network Components

- **IP Phones** and **Videoconferencing Station**
  - Provides IP voice and video to the desktop
- **Gateway**
  - Provides translation between VoIP and non-VoIP networks
  - It also provides physical access for local analog and digital voice devices, such as telephones, fax machines, key sets, and PBXs
- **Multipoint Control Unit (MCU)**
  - Provides real-time connectivity for participants in multiple locations to attend the same videoconference or meeting
- **Call Agent**
  - Provides call control for IP phones, CAC, bandwidth control and management, and translation for IP addresses or tel. numbers
- **Application server**
  - Provides services such as voice mail, unified messaging, and Cisco Unified Communications Manager Attendant Console



VoIP Protocols

- VoIP generally uses two types of protocols
- **Signaling protocols**
  - Call Control
  - Device control
- **Media protocols**
  - RTP

Signaling Protocols

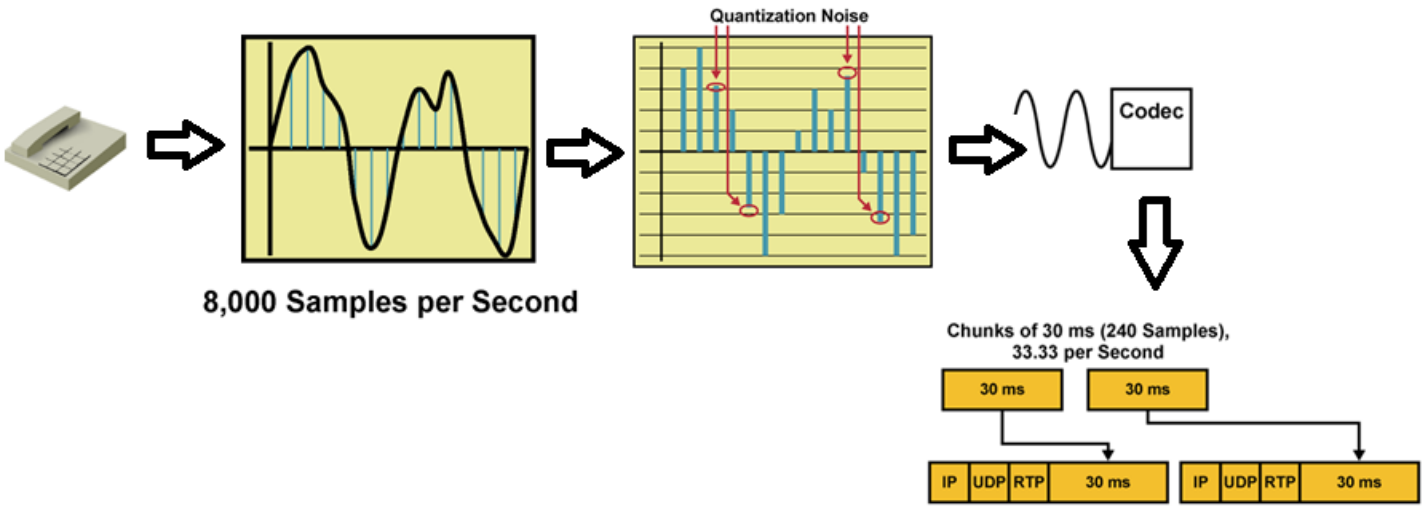
- Identify the state of connection between telephones
- **Call Control**
  - **H.323** protocol family (H.225, H.245)
  - **Session Initiation Protocol (SIP)**
  - **Skinny Call Control Protocol** (Skinny)
- **Device Control**
  - H.248/Megaco (Media Gateway Control)
  - SIGTRAN

Media Protocols

- Transfer voice, video, DTMF tones etc.
- **Real-time Transport Protocol (RTP)**
  - RFC 3550
  - Most used protocol for delivering audio
  - Built on the UDP
  - Timestamps (for synchronization)
  - Sequence numbers (for packet loss and reordering detection)
  - Payload format (codec)
  - RTCP - QoS feedback and synchronization between the media streams
- Voice is digitized and compressed using codecs
  - Different bandwidth requirements – less bandwidth usually means worse voice quality

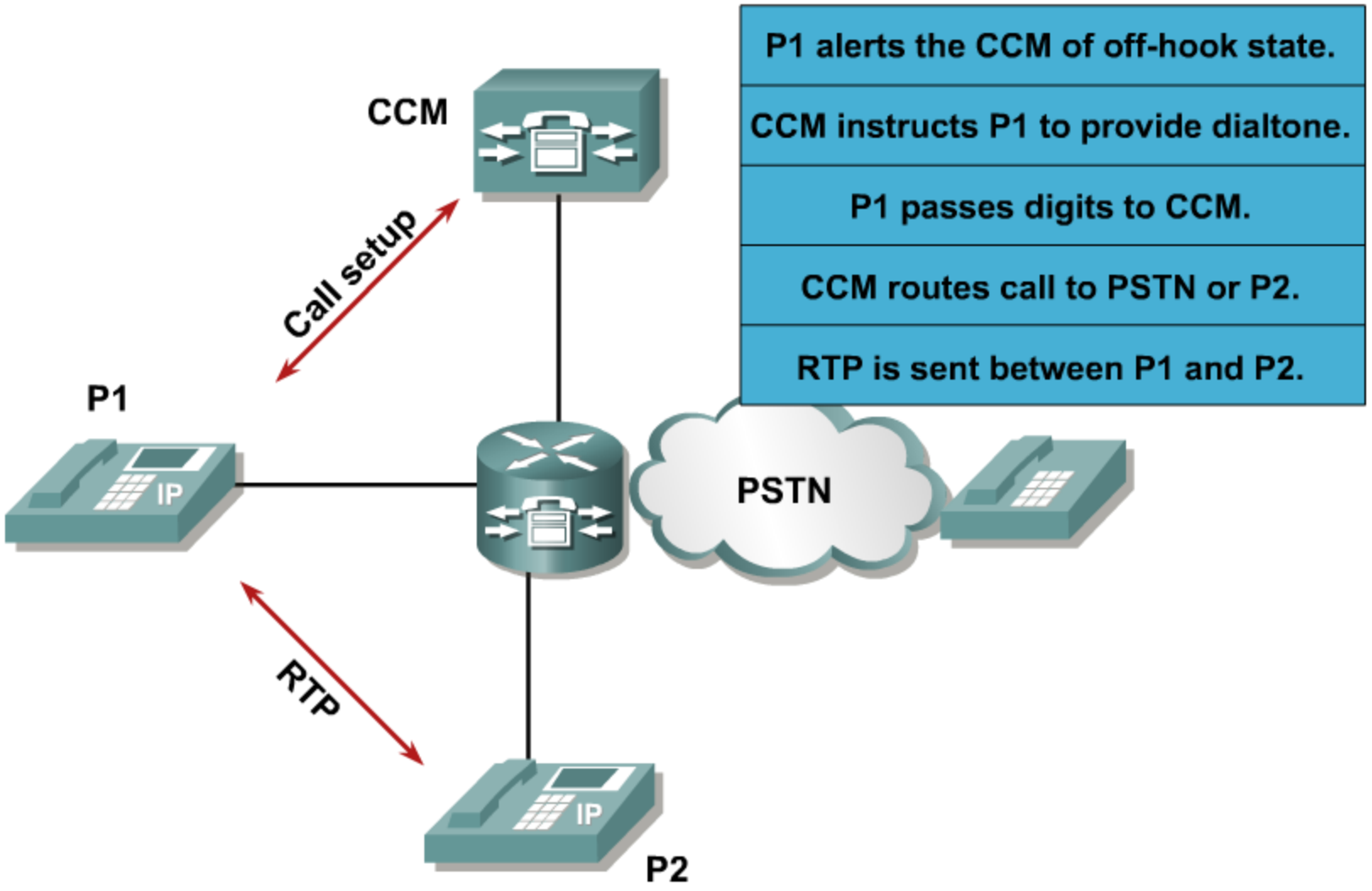
Voice Codecs

- By default 20msec of voice data are packetized
- Sampling ► Quantization ► Compression ► Packetization



Codec	G.711	G.726 r32	G.726 r24	G.726 r16	G.728	G.729	G.723 r63	G.723 r53
Bandwidth	64 kbps	32 kbps	24 kbps	16 kbps	16 kbps	8 kbps	6.3 kbps	5.3 kbps

Basic Phone Call



QoS in Networks

IP Networks

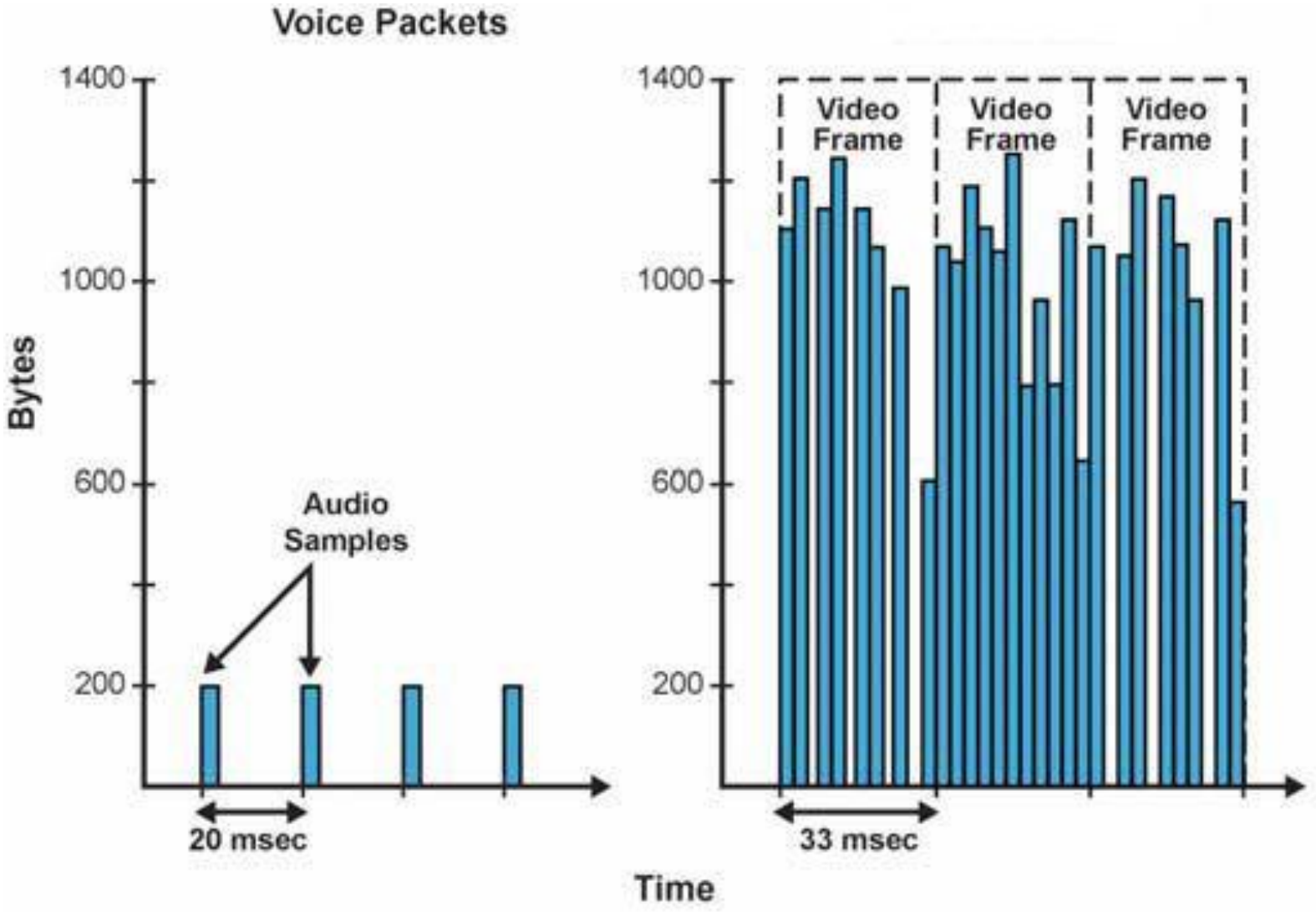
- „IP over everything“ is slowly changing to „Everything over IP“ or so called **Internet of Everything (IoE)**
- Nowadays network trend is to provide several services (data, voice, video etc.) using packet IP infrastructure
  - Increasing load
  - Traffic characteristic is changing:
    - Services transfer different type of data – different requirements
    - Best effort delivery is no longer sufficient
- *It is important to determine which applications will be deployed*
  - Peer-to-peer TelePresence
  - Video-on-demand Training
  - IP surveillance

Traffic Characteristic

- **VoIP**
  - Smooth
  - Low-bandwidth
  - Requires bandwidth guaranty
    - 8kbps to 64kbps depends on codec
    - + network overhead (12kbps – 80kbps)
  - Packets drop can be eliminated
    - Depends on codec 0,1% - 5%
    - Acceptable 1%
  - Delay sensitive
    - < 150 ms
    - > 200 ms = quality degradation
  - Jitter
    - Anything bellow < 30ms is good
    - but 10ms are considered to be a standard treshold

- **Data**
  - Bursty
  - Maximum network utilization (TCP window)
  - Does not require bandwidth guaranty
  - Drop sensitive
  - Delay is usually not a problem

Voice and Video Traffic Profiles

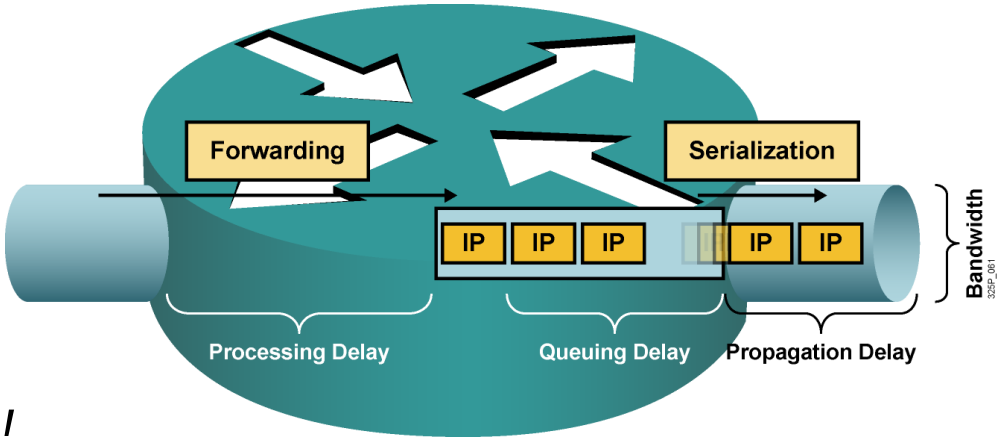


Different Requirements

Requirement	Data	Voice	Video
Bandwidth	High	Low	High
Delay	If less than a few msec, not applicable	< 150 msec	< 150 msec for real-time video
Jitter	Not applicable	Low	Low (< 10 msec)
Packet Loss	< 5%	< 1%	< 0.5%
Availability	High	High	High
Inline Power	No	Optional	Optional for select devices
Security	High	Medium	Low or Medium
Provisioning	Medium Effort	Significant Effort	Medium Effort

Internet Today

- Provides best-effort data delivery
  - Flat system, without packet categorization
  - Voice packets are routed using “best” route
    - Different characteristic for every route – throughput, latency
    - Dynamic conditions, asymetric routing
- As demands exceeds capacity, service degrades gracefully
  - **Packet losses**
    - Congestion, errors in the transmission
  - **Packet delay**
    - = processing + queueing delay + serialization + propagation
  - **Jitter**
  - **Throughput**
  - **Availibility**
- *Difficult to predict in IP networks!*



Quality of Service

- The above – mentioned problems are solved in telephone networks
  - e.g. *Time division multiplexing – time slots*
  - `IF` there is not enough capacity for another call `THEN` call is refused
- Packet switching networks can fulfill the requirements by
  - Separating data and voice traffic
  - Classifying and prioritizing voice traffic
  - Providing sufficient link capacity
- …all of previous is called **Quality of Service (QoS)**

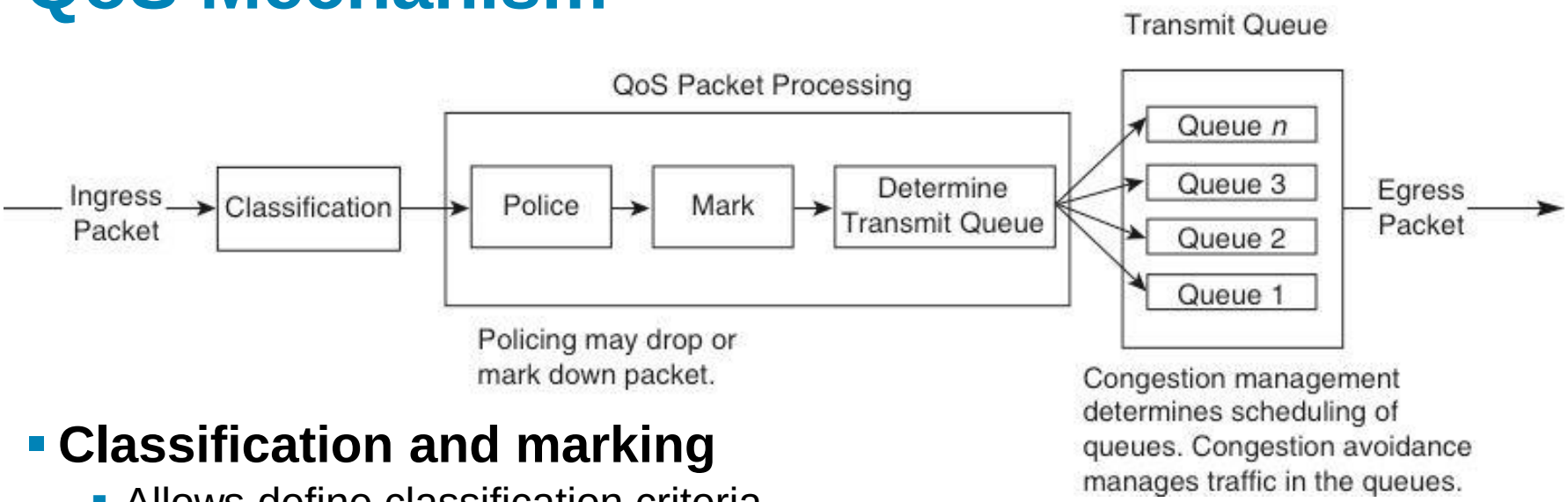
How to Achieve QoS

- Requirements for new mechanisms
  - There is a need for mechanisms to distinguish different data flows
    - …and process them a special/required way
    - *No flat behavior anymore!*
  - There is a need for advanced resource management mechanisms
    - …which allows manage net resources (bandwidth, delay, loss, jitter)
    - …with focus on different data flows requirements

QoS Service Models

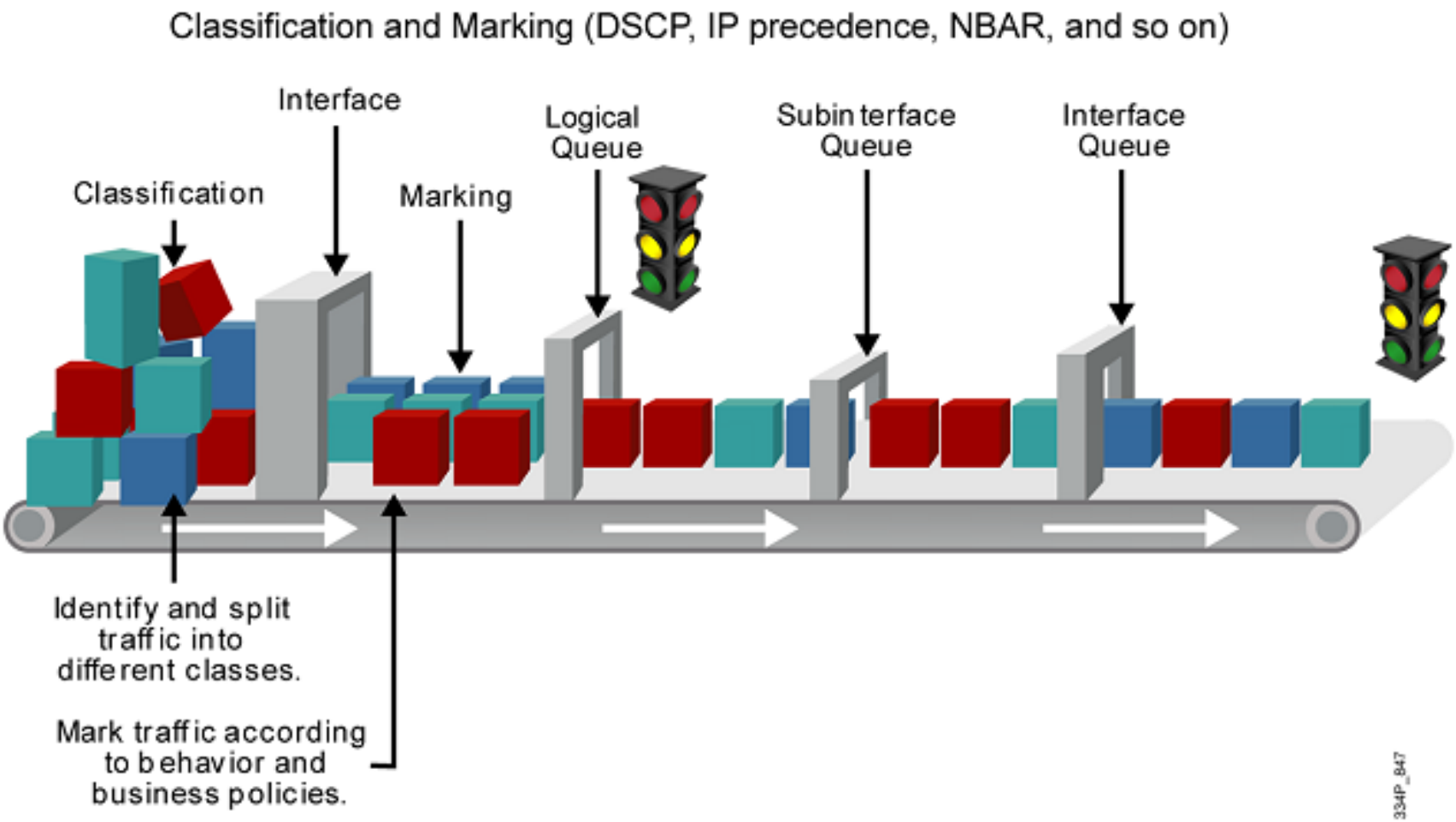
- **Best-effort service**
  - The standard form of connectivity without guarantees
  - This type of service, in reference to Catalyst switches, uses first-in, first-out (FIFO) queues
- **Integrated service (IntServ)**
  - a.k.a. **hard QoS** is a reservation of services
  - The IntServ model implies that traffic flows are reserved explicitly by all intermediate systems and resources
- **Differentiated service (DiffServ)**
  - a.k.a. **soft QoS**, is class-based, in which some classes of traffic receive preferential handling over other traffic classes
  - Differentiated services use statistical preferences, not a hard guarantee such as integrated services
  - DiffServ categorizes traffic and then sorts it into queues of various efficiencies.

QoS Mechanism



- **Classification and marking**
  - Allows define classification criteria
  - *How to find traffic which requires special processing?*
- **Scheduling and policing enforcement**
  - Allows create special processing mechanisms for classified flows and control traffic compliance
- **Policy Control**
  - *Who may requires a special handling for their data?*
- **Admission Control**
  - *Does network has enough resources to provide required resources?*

QoS Operation



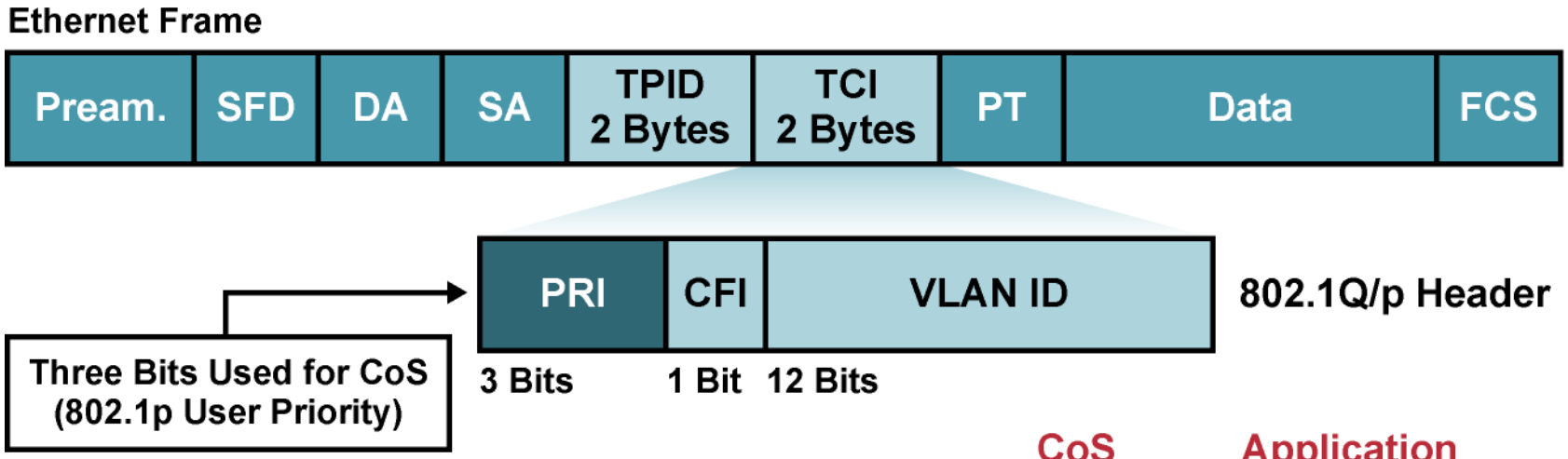
Classification

- **Classification** = process of content determination
- Typically on access or distribution layer
- **Layer 2 parameters**
  - MAC address, 802.1p CoS, Multiprotocol Label Switching (MPLS) TC, ATM Cell Loss Priority (CLP) bit, Frame Relay Discard Eligible (DE) bit, input interface
- **Layer 3 parameters**
  - IP precedence, Differentiated Services Code Point (DSCP), IP address, input interface
- **Layer 4 parameters**
  - TCP/UDP ports, transport protocol
- **Layer 7 parameters**
  - Application signatures

Marking

- **Marking** is a result of classification
  - L2 - 802.1p (part of 802.1q)
  - L3 - IP Precedence (Type of Service field)
  - DSCP (Differentiated Services Code Point)
- Frames with a same mark is processed similarly
  - Input queue scheduling
  - Policing
  - Output queue scheduling

Class of Service Field

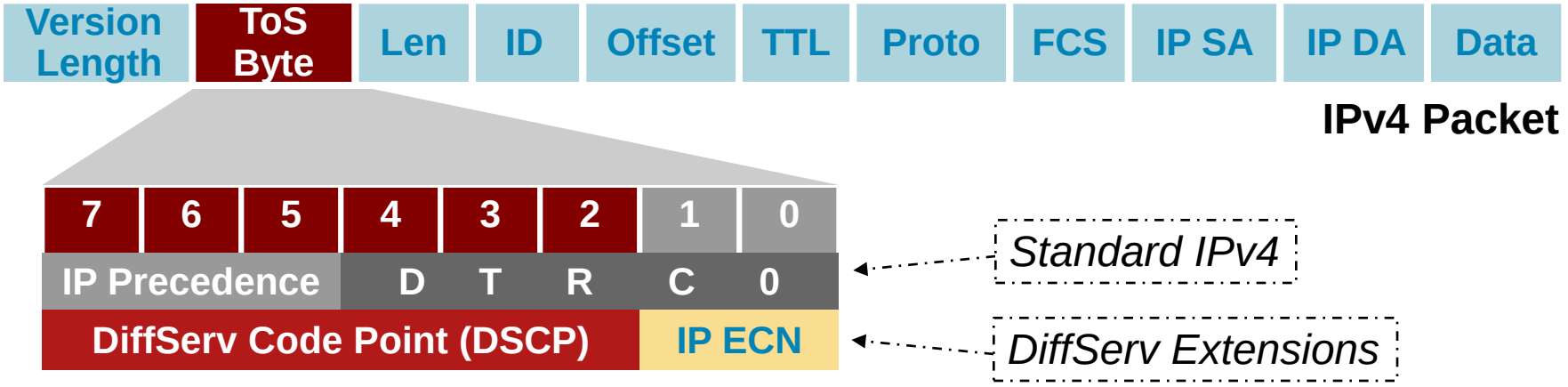


- IEEE 802.1p user priority field is also called **Class of Service (CoS)**
- IEEE 802.1p supports up to eight CoSs
- IEEE 802.1p is preserved through the LAN, not end to end

CoS	Application
7	Reserved
6	Reserved
5	Voice Bearer
4	Videoconferencing
3	Call Signaling
2	High-Priority Data
1	Medium-Priority Data
0	Best-Effort Data

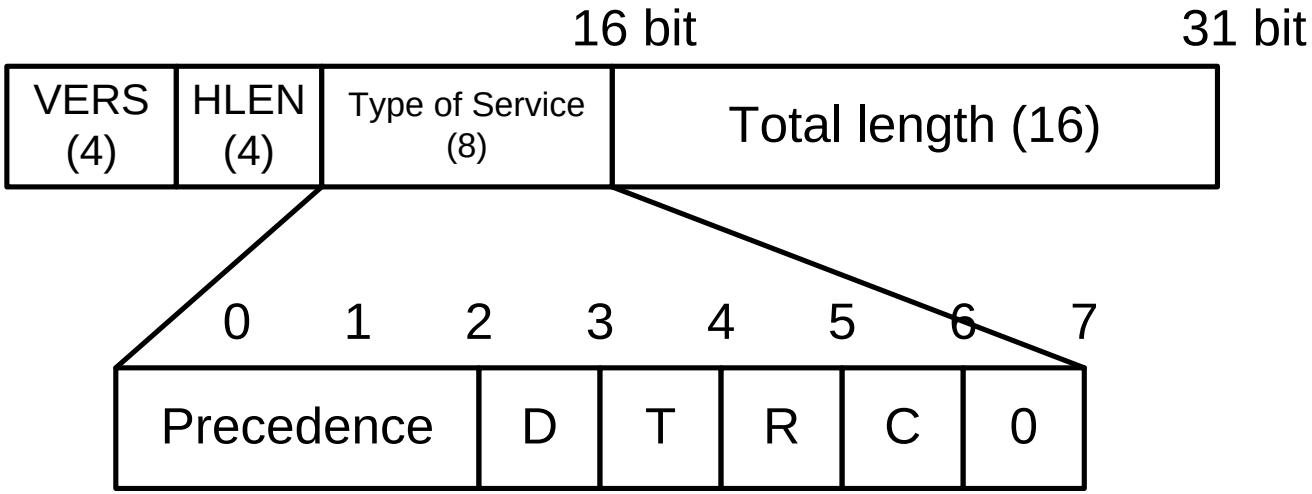
325P_090

ToS vs. DSCP



- **IPv4**: three most significant bits of ToS byte are called **IP Precedence (IPP)**
- **DiffServ**: six most significant bits of ToS byte are called **DiffServ Code Point (DSCP)**—remaining two bits used for flow control
- DSCP is backward-compatible with IP precedence

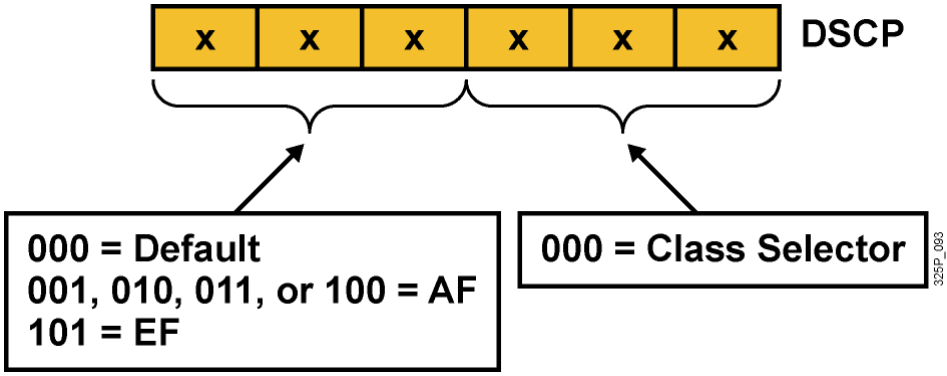
Type of Service Field



- **Precedence**
  - 111 - Network Control
  - 110 - Internetwork Control
  - 101 - CRITIC/ECP
  - 100 - Flash Override
  - 011 - Flash
  - 010 - Immediate
  - 001 - Priority
  - 000 - Routine (BE)
- **D – Delay**
- **T – Throughput**
- **R – Reliability**
- **C – Cost**
  - 0000 – All normal (Default)
  - 1000 – Minimize delay
  - 0100 – Maximize throughput
  - 0010 – Maximize reliability
  - 0001 – Minimize monetary cost

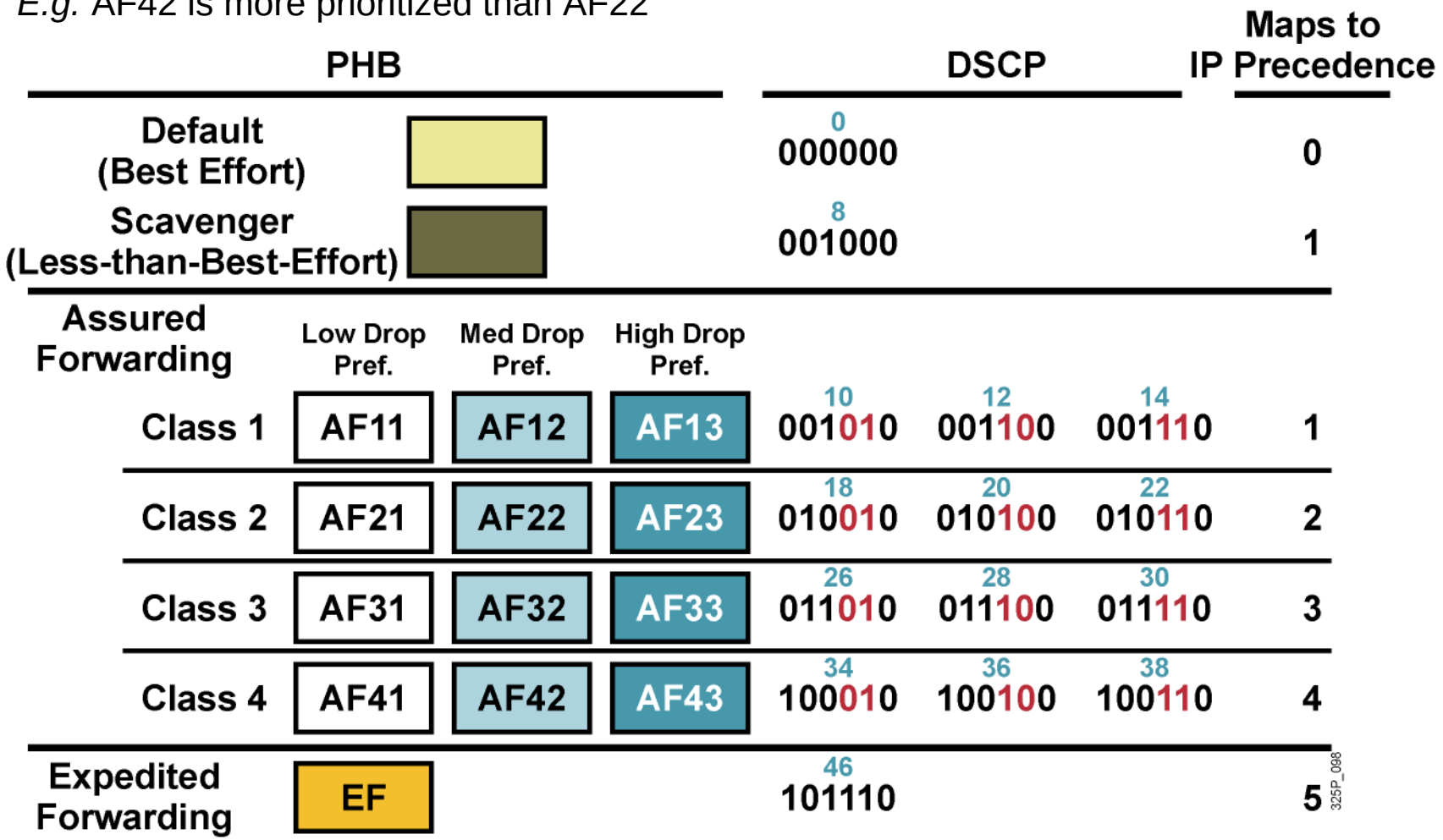
DSCP: Per-Hop Behavior

- **Per-Hop Behavior (PHB)**
  - Influenced by DSCP
  - = the packet scheduling, queuing, policing, or shaping behavior of a node on any given packet with DSCP set
- PHB Groups
  - **Default**
  - **Class-selector**
  - **Expedited Forwarding (EF)**
    - Value ***dd0
    - Ensures minimum departure rate
    - Guarantess and policies bandwidth
  - **Assured Forwarding (AF)**
    - Guarantees bandwidth
    - Value 101110



DSCP: Standard PHB Groups

- *E.g.* AF13 is more eligible for drops than AF11
- *E.g.* AF42 is more prioritized than AF22

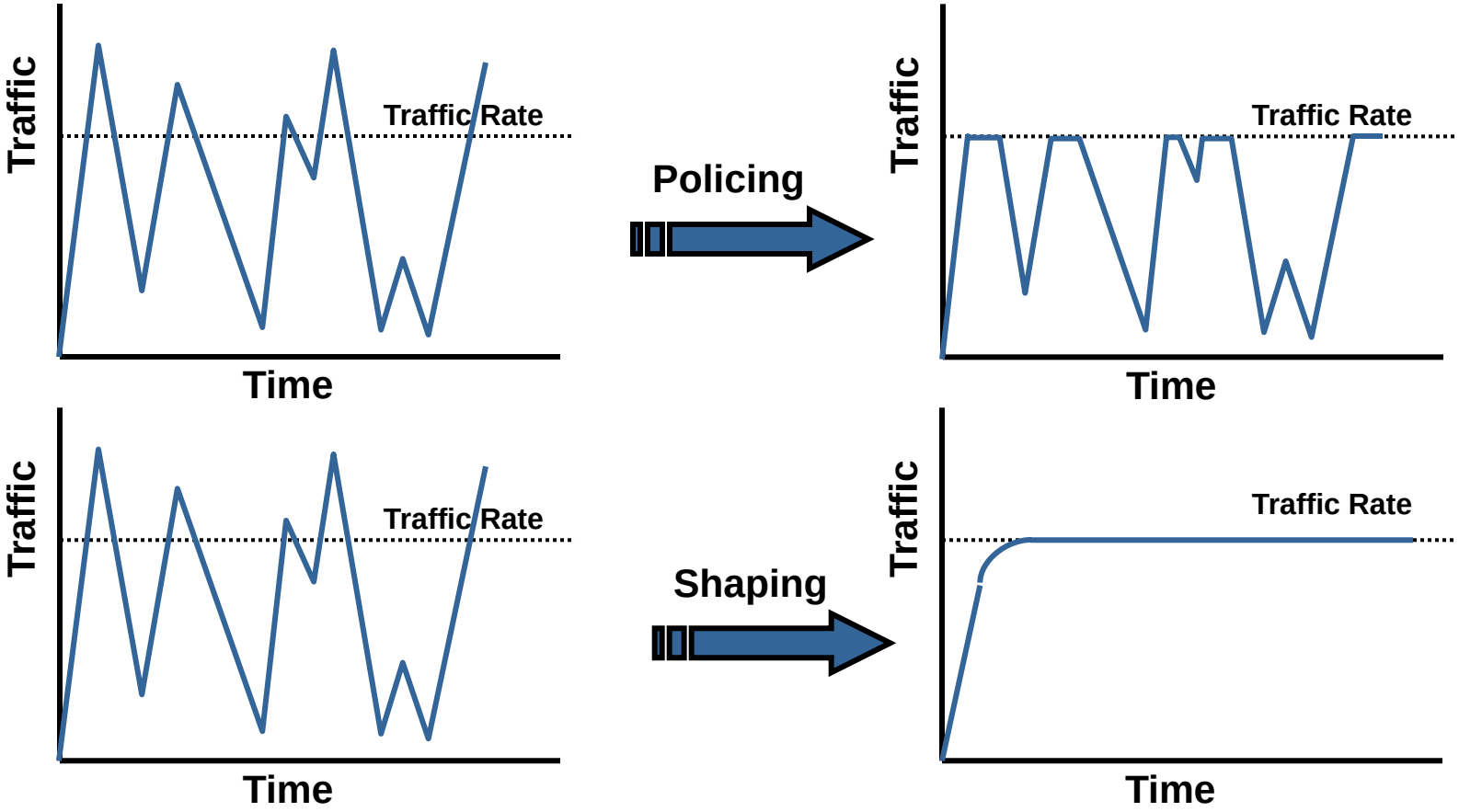


Classification and Marking Best-Practice

Application	L3 Classification			L2
	IPP	PHB	DSCP	CoS
Routing	6	CS6	48	6
Voice	5	EF	46	5
Video Conferencing	4	AF41	34	4
Streaming Video	4	CS4	32	4
Mission-Critical Data	3	AF31*	26	3
Call Signaling	3	CS3*	24	3
Transactional Data	2	AF21	18	2
Network Management	2	CS2	16	2
Bulk Data	1	AF11	10	1
Best Effort	0	0	0	0
Scavenger	1	CS1	8	1

Traffic Policing and Shaping

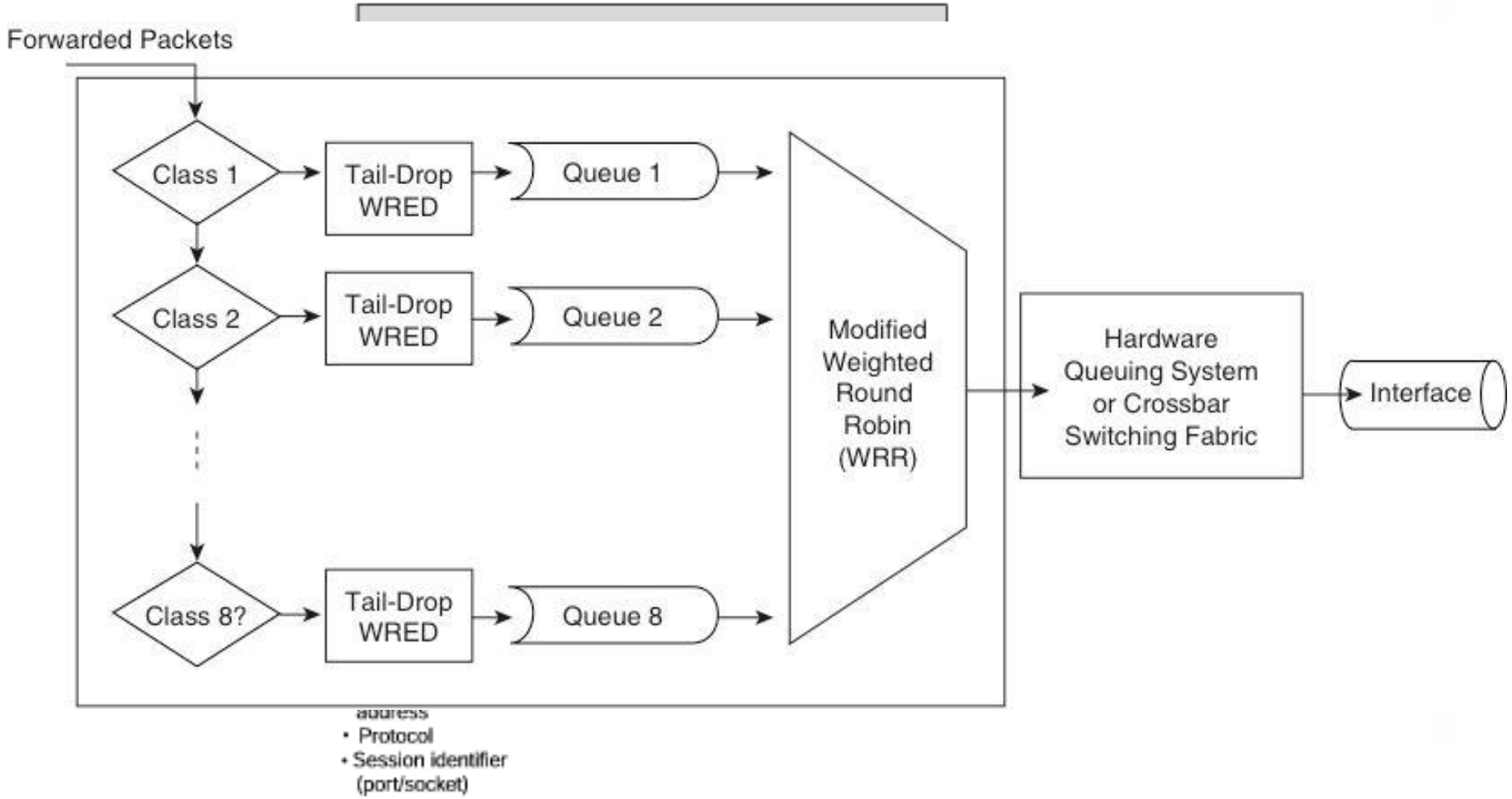
- Admission and policy control is done via **Shaping/Policing**
  - Shaping is done on customer's side
  - Policing is done on provider's side



Congestion Management

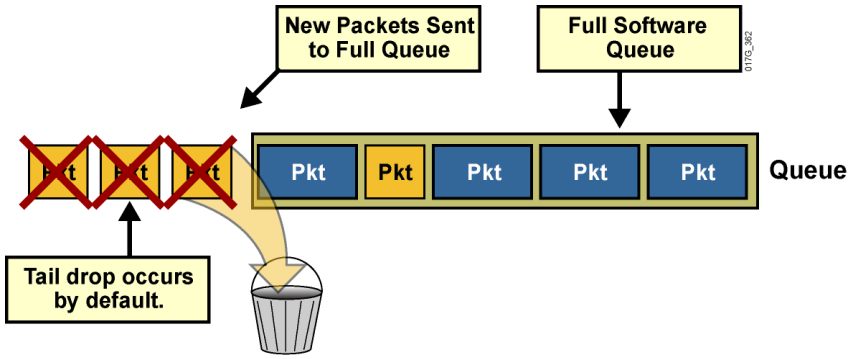
- **FIFO Queuing**
  - Places all egress frames into same queue
- **Weighted Round Robin (WRR) Queuing**
  - Multiple egress queues with different weigths
- **Priority Queuing (PQ)**
  - More prioritized queue is served first
  - Usually 1 PQ that is taking advantage above others
- **Custom Queuing (CQ)**
  - Each traffic type has reserved queue with guaranteed bandwidth
- **Weighted Fair Queuing (WFQ)**
  - Flow-base queues creating bit-wise fairness

Queues Implementation

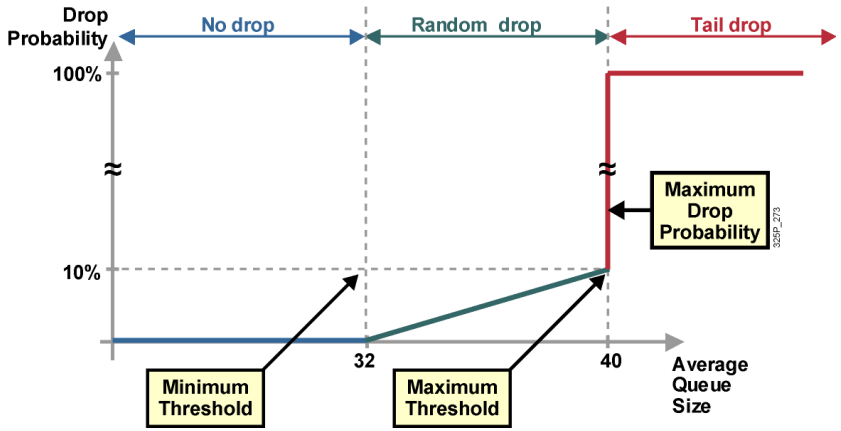


Congestion Avoidance

- **Tail Drop**



- **Random Early Detection (RED)**

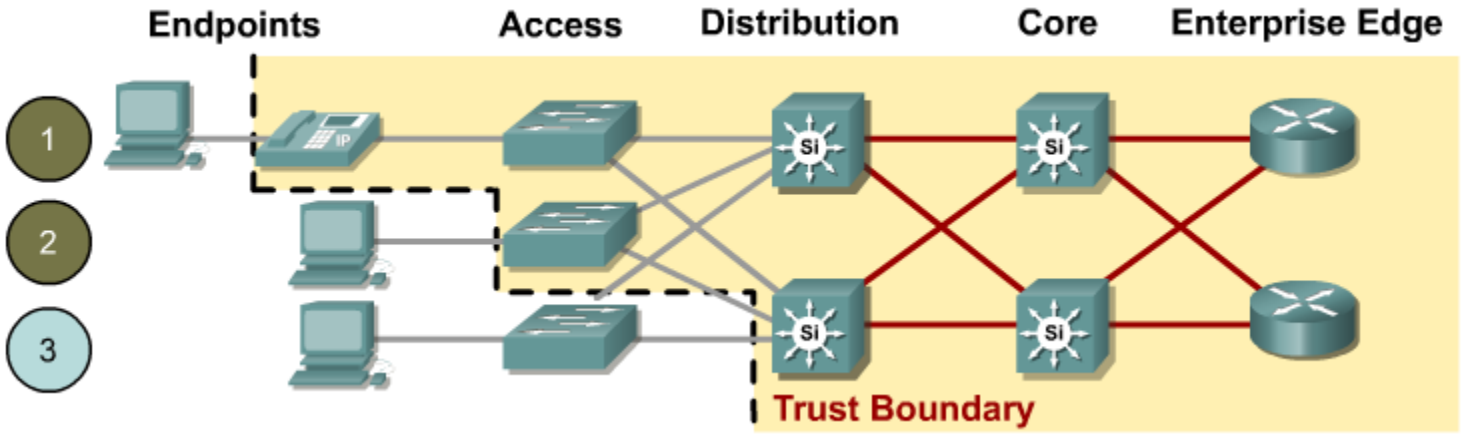


- **Weighted Random Early Detection (WRED)**
  - Multiple RED profiles (according to CoS or DSCP)

VoIP and QoS Configuration

Trust Boundaries

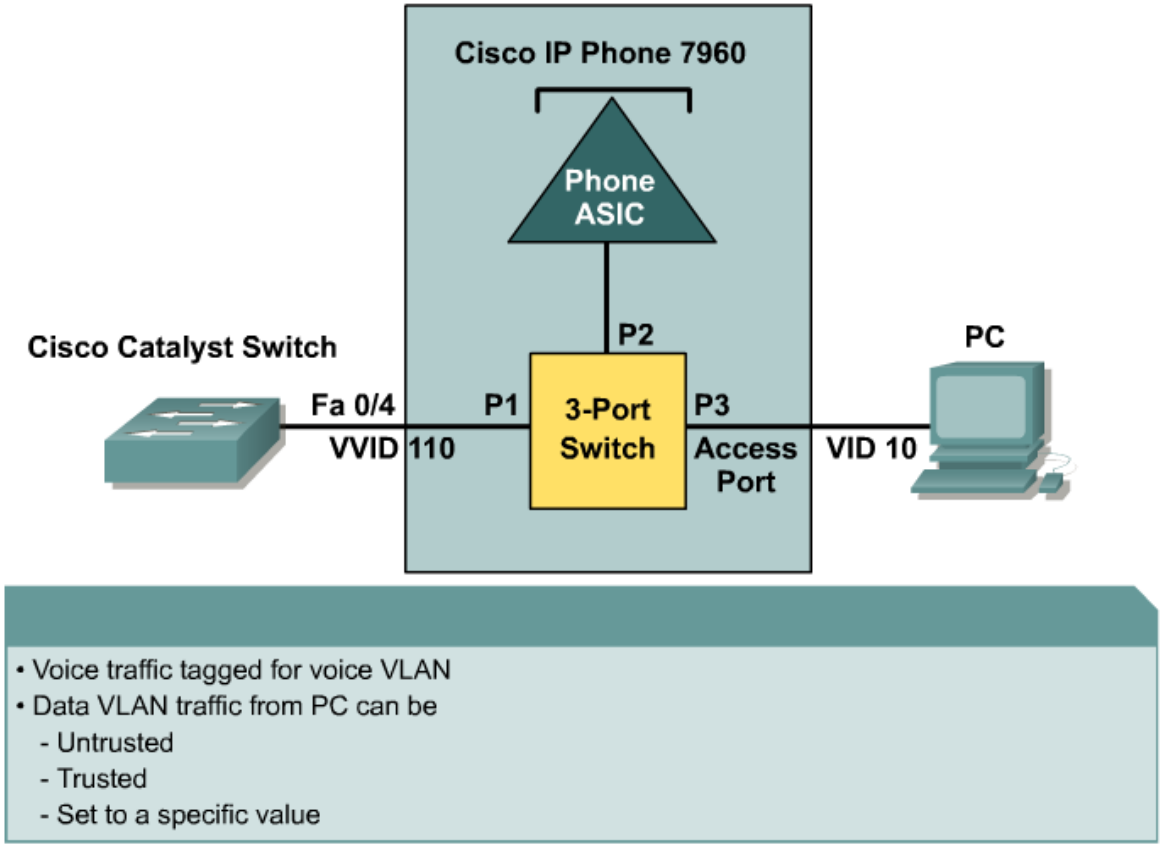
- Boundaries where marking performed by previous active network devices is being trusted
- *Best practices suggest classifying and marking traffic as close to the traffic source as possible!*



Separation of Data and Voice Traffic ①

- Switch cannot distinguish voice and data packets
  - Voice packets cannot be prioritized
- *Solution?*
  - 802.1Q tagging
  - Data packets are transmitted without a tag
  - Voice packet tagged by phone

Separation of Data and Voice Traffic ②



- IP phone has two Ethernet ports
  - Connection to the network
  - Connection to the PC
- IP phone transmits data
  - Voice packets
  - Data packets generated by PC

Voice VLAN (Auxiliary VLAN)

- Cisco switch allows to configure **voice vlan a.k.a. auxiliary VLAN**
- Data traffic DOES NOT use 802.1Q tag
- Voice traffic is tagged according to the configuration
  - Voice Vlan ID = VVID
- Cisco IP phone discover voice VLAN by CDP
  - CDP should be enabled on access ports
  - IP phone tags Voice packets with VVID

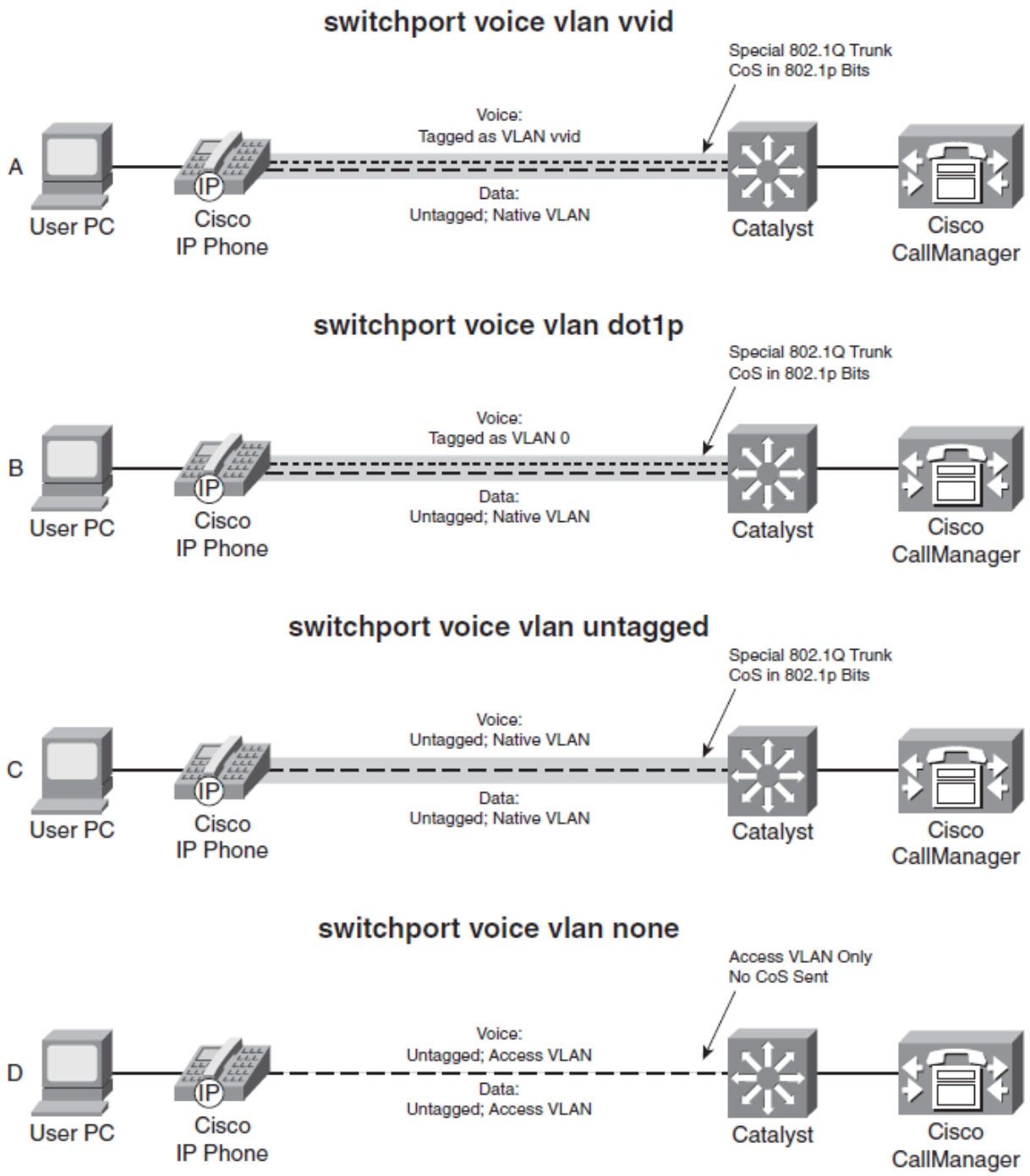
```
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 100
Switch(config-if)# switchport voice vlan 200
```

Class of Service (CoS)

- Voice packets tagged with 802.1Q tag allows:
  - Separation of voice and data traffic
  - Allows to set CoS bits in 802.1Q header

```
Switch(config-if)#
  switchport voice vlan {vlan-id | dot1p | untagged | none}
```

Keyword	In Figure	Native VLAN (untagged)	Voice VLAN	Voice QoS (CoS)
vlan-id	1st	PCdata	VLAN *vlan-id*	802.1p
dot1p	2nd	PCdata	VLAN 0	802.1p
untagged	3rd	PCdata/voice	—	802.1p
none (default)	4th	PCdata/voice	—	—


switchport voice vlan vvid
Special 802.1Q Trunk
CoS in 802.1p Bits
Voice:
Tagged as VLAN vvid
Data:
Untagged; Native VLAN
A
User PC
IP
Cisco
IP Phone
Catalyst
Cisco
CallManager
switchport voice vlan dot1p
Special 802.1Q Trunk
CoS in 802.1p Bits
Voice:
Tagged as VLAN 0
Data:
Untagged; Native VLAN
B
User PC
IP
Cisco
IP Phone
Catalyst
Cisco
CallManager
switchport voice vlan untagged
Special 802.1Q Trunk
CoS in 802.1p Bits
Voice:
Untagged; Native VLAN
Data:
Untagged; Native VLAN
C
User PC
IP
Cisco
IP Phone
Catalyst
Cisco
CallManager
switchport voice vlan none
Access VLAN Only
No CoS Sent
Voice:
Untagged; Access VLAN
Data:
Untagged; Access VLAN
D
User PC
IP
Cisco
IP Phone
Catalyst
Cisco
CallManager

QoS Configuration

- Enabling QoS (disabled by default on some platforms)

```
Switch(config)# mls qos
```

- IF the **mls qos** is enabled THEN switch starts to rewrite CoS field according the configuration

Class of Service

- Packets are sorted to different output queues according the CoS field
  - Length or weight of queue can be set in configuration
  - Recommended value for voice traffic = CoS 5
  - Cisco IP phones automatically mark voice packet with CoS 5 by default
- Switch DOES NOT believe received CoS priorities by default
  - Trust for CoS field can be set on a interface:

```
Switch(config-if)# mls qos trust cos
```

  - IFF Cisco phone is connected on the interface THEN trust the CoS field :

```
Switch(config-if)# mls qos trust cos
Switch(config-if)# mls qos trust device cisco-phone
```

CoS for Marked Data Frames

- Attacker can mark own data packets with high priority
  - IP phone could be configured to check data packets
    - IF the priority is set
      THEN phone rewrites the priority to predefined value
  - CDP is used to inform the phone about the priority

```
Switch(config-if)# switchport priority extend cos 2
```

- IF the PC can be trusted THEN trust boundaries can be extended to the PC:

```
Switch(config-if)# switchport priority extend trust
```

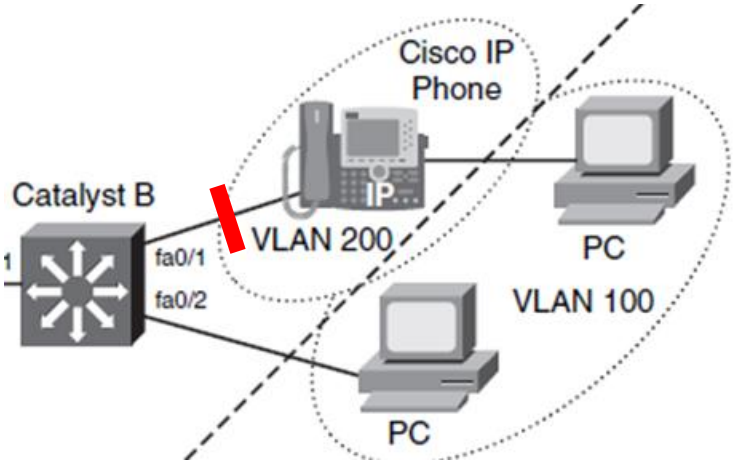
CoS for Unmarked Data Frames

- The CoS can be set to predefined value for data frames without CoS set

```
Switch(config-if)# mls qos cos 1
```

Port Configuration for Hardware IP Phone

```
Switch(config)# mls qos
Switch(config)# interface Fa0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 100
Switch(config-if)# switchport voice vlan 200
Switch(config-if)# switchport priority extend cos 2
Switch(config-if)# mls qos cos 1
Switch(config-if)# mls qos trust cos
Switch(config-if)# mls qos trust device cisco-phone
```



Port Configuration for Software IP Phone

- PC cannot use Voice VLAN
- Cisco IP Communicator does not sent marked frames
- Cisco IP Communicator is also using and benefiting from CDP
- Trust must be set to DSCP field in IP packet

```
Switch(config)# mls qos
Switch(config)# interface Fa0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 100
Switch(config-if)# mls qos trust dscp
Switch(config-if)# mls qos trust device cisco-phone
```

Verify the QoS

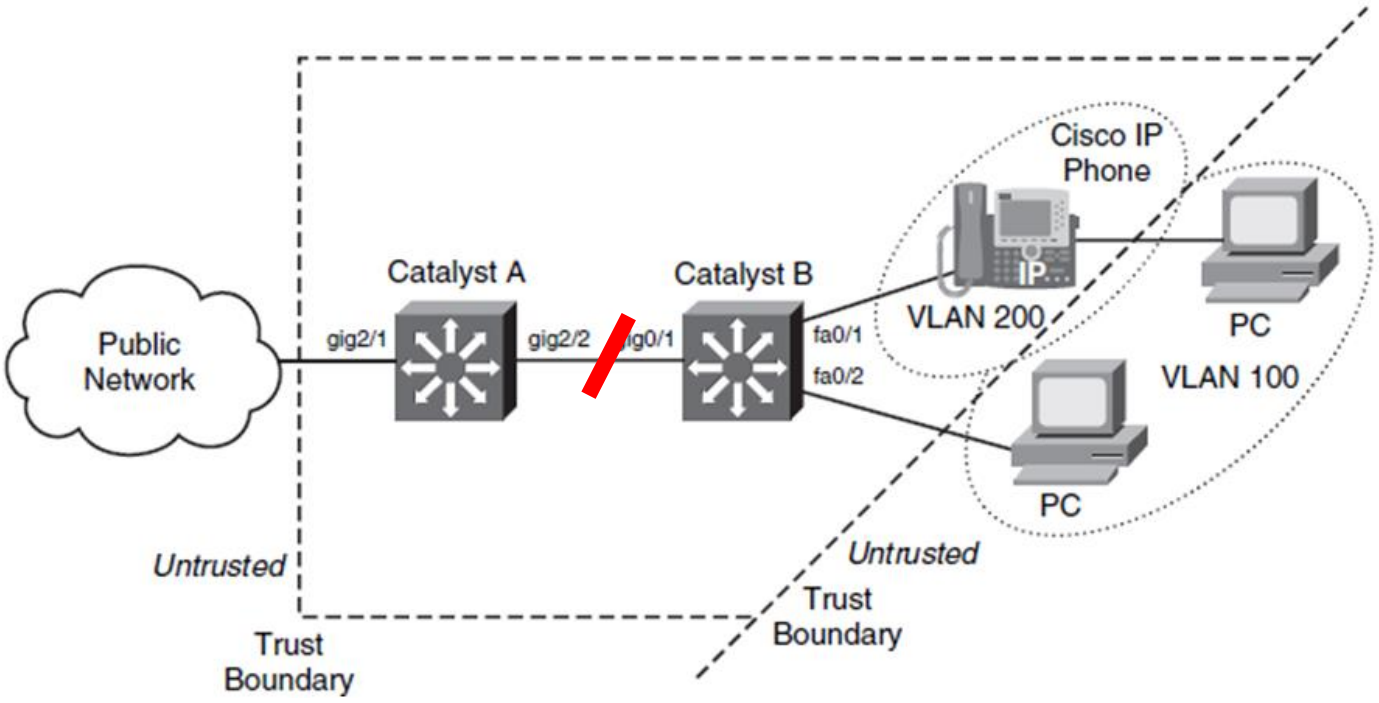
```
show mls qos interface
```

```
Switch# show mls qos interface fastethernet 0/1
FastEthernet0/1
trust state: trust cos
trust mode: trust cos
trust enabled flag: ena
COS override: dis
default COS: 0
DSCP Mutation Map: Default DSCP Mutation Map
Trust device: none
```

Connection Between Switches

- Trust for CoS MUST be enabled between switches

```
Switch(config-if)# switchport mode trust
Switch(config-if)# mls qos trust cos
```



Connection Between Router and Switch

- CoS can be used only on trunk ports
  - Ethernet frame DOES NOT contain priority bits
- CoS is valid only in one VLAN (broadcast domain)
  - Router encapsulates packet into a new frame, hence, CoS field is not copied
- Trust is set to DSCP bits in IP header

```
Switch(config)# mls qos
Switch(config)# interface Fa0/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# mls qos trust dscp
```

CoS/DSCP Trust Notes ①

- CoS is valid only between neighbors
- DSCP is valid between end stations (end-to-end range)
- **`mls qos trust`** creates trust boundary
  - Interface between trusted and untrusted network
  - Untrusted network can use CoS/DSCP marks
  - Trusted network use CoS/DSCP
  - Edge switch for the trust boundary rewrites CoS/DSCP fields
- *Once again trust boundary should be as close to the source as possible*
  - Usually on access switch
  - **`switchport priority extend`** extends the boundary to an IP phone

CoS/DSCP Trust Notes ②

- Catalyst switches CAN NOT trust CoS and DSCP values simultaneously
  - `IF` a switch trust to CoS `THEN` it DOES NOT trust DSCP and vice versa
- `IF` trust is set to CoS `THEN`
  - DSCP bits are rewritten according to „cos-dscp map“ table
- `IF` trust is set to DSCP `THEN`
  - CoS bits are rewritten according to „dscp-cos map“ table

Default Mappings

Default CoS ↔ DSCP Mapping								
CoS	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

Default IP Precedence ↔ DSCP Mapping								
IP Precedence	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

- Displays the maps that are used to generate rewrites:

```
switch# show mls qos maps [cos-dscp | dscp-cos]
```

```
switch#show mls qos maps dscp-cos

Dscp-cos map:
   dscp: 0 8 10 16 18 24 26 32 34 40 46 48 56
         ----------------------------------------
    cos: 0 1  1  2  2  3  7  4  4  5  5  7  7
```

Auto-QoS

- Setting the QoS parameters is non-trivial
- Macro **auto qos** generates QoS configuration automatically
- IFF HW phone is connected to switch THEN trust CoS:

```
Switch(config-if)# auto qos voip cisco-phone
```

- IFF SW phone is connected THEN trust DSCP

```
Switch(config-if)# auto qos voip cisco-softphone
```

- Trusted PC

```
Switch(config-if)# auto qos voip trust
```

- Uplink from switch port to the router

```
Switch(config-if)# auto qos voip trust
```

Verifying Cisco Auto-QoS

- Generated configuration can be changed by administrator
- **`show auto qos`** command displays the original configuration
  - *However, it does not display any additional changes by network administrator ☹*

```
switch# show auto qos
Initial configuration applied by AutoQoS:
wrr-queue bandwidth 20 1 80 0
no wrr-queue cos-map
wrr-queue cos 1 0 1 2 4
wrr-queue cos 3 3 6 7
wrr-queue cos 4 5
mls qos map cos-dscp 0 8 16 26 32 46 48 56
!
interface FastEthernet0/3
mls qos trust device cisco-phone
mls qos trust cos
…
```

Power Over Ethernet (PoE)

Power over Ethernet

- High availability
- Cisco Inline Power (ILP)
  - Cisco proprietary, before 802.3af
- IEEE 802.3af – 15.4W per port
- IEEE 802.3at – 25.5W per port
- Power
  - 48V DC
  - Pins 1-3, 2-6 (ILP, IEEE)
  - Pins 4,5 a 7,8 (IEEE)

Device Detection

- Switch is constantly checking presence of a PoE device
- Cisco Inline Power (CIP)
  - Catalyst switch is sending 340 kHz tone on Tx pair
  - Cisco phone connects Rx and Tx pair by low-pass filter
  - Switch „hear“ own tone if a device supports PoE
- IEEE 802.3af, 802.3at
  - Power is connected to Tx and Rx pair
  - Measures impedance

IEEE802.3af PoE Classes

- IEEE 802.3af allows to assign only necessary power for PoE device

Power Class	Maximum Power Offered at 48V DC	Notes
0	15.4W	Default class
1	4.0W	Optional class
2	7.0W	Optional class
3	15.4W	Optional class
4	—	Reserved for future use

Debug PoE

```
Switch# debug ilpower controller
Switch# debug cdp packets
```

```
00:58:46: ILP uses AC Disconnect(Fa1/0/47): state= ILP_DETECTING_S, event=
PHY_CSCO_DETECTED_EV
00:58:46: %ILPOWER-7-DETECT: Interface Fa1/0/47: Power Device detected: Cisco PD
00:58:46: Ilpower PD device 1 class 2 from interface (Fa1/0/47)
00:58:46: ilpower new power from pd discovery Fa1/0/47, power_status ok
00:58:46: Ilpower interface (Fa1/0/47) power status change, allocated power 15400
00:58:46: ILP Power apply to ( Fa1/0/47 ) Okay
00:58:46: ILP Start PHY Cisco IP phone detection ( Fa1/0/47 ) Okay
00:58:46: %ILPOWER-5-POWER_GRANTED: Interface Fa1/0/47: Power granted
00:58:46: ILP uses AC Disconnect(Fa1/0/47): state= ILP_CSCO_PD_DETECTED_S, event=
IEEE_PWR_GOOD_EV
00:58:48: ILP State_Machine ( Fa1/0/47 ): State= ILP_PWR_GOOD_USE_IEEE_DISC_S, Event=
PHY_LINK_UP_EV
```

PoE Configuration

- Enabled by default

```
Switch(config)# interface IFACE
Switch(config-if)#  power inline {auto [max milli-watts]    |
                                 static [max milli-watts] | never}
```

- Verify

```
Switch# show power inline [ type mod/num ]
```

Cisco CallManager Express

QoS on Routers

Slides adapted by Matěj Grégr and tuned by Vladimír Veselý
partially from official course materials
but most of credit goes to CCIE#23527 Ing. Peter Palúch, Ph.D.

The last update: 2013-08-01