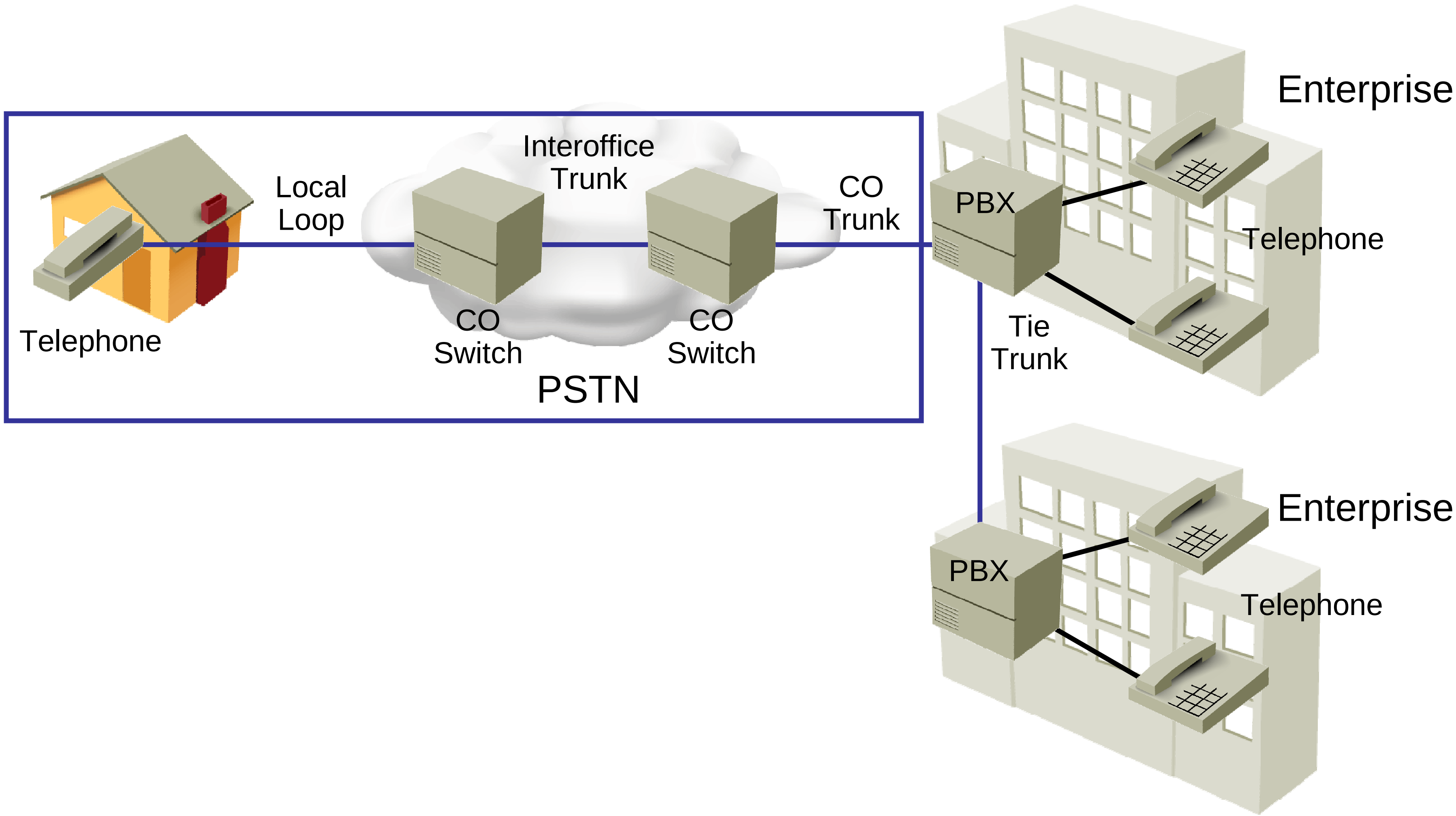
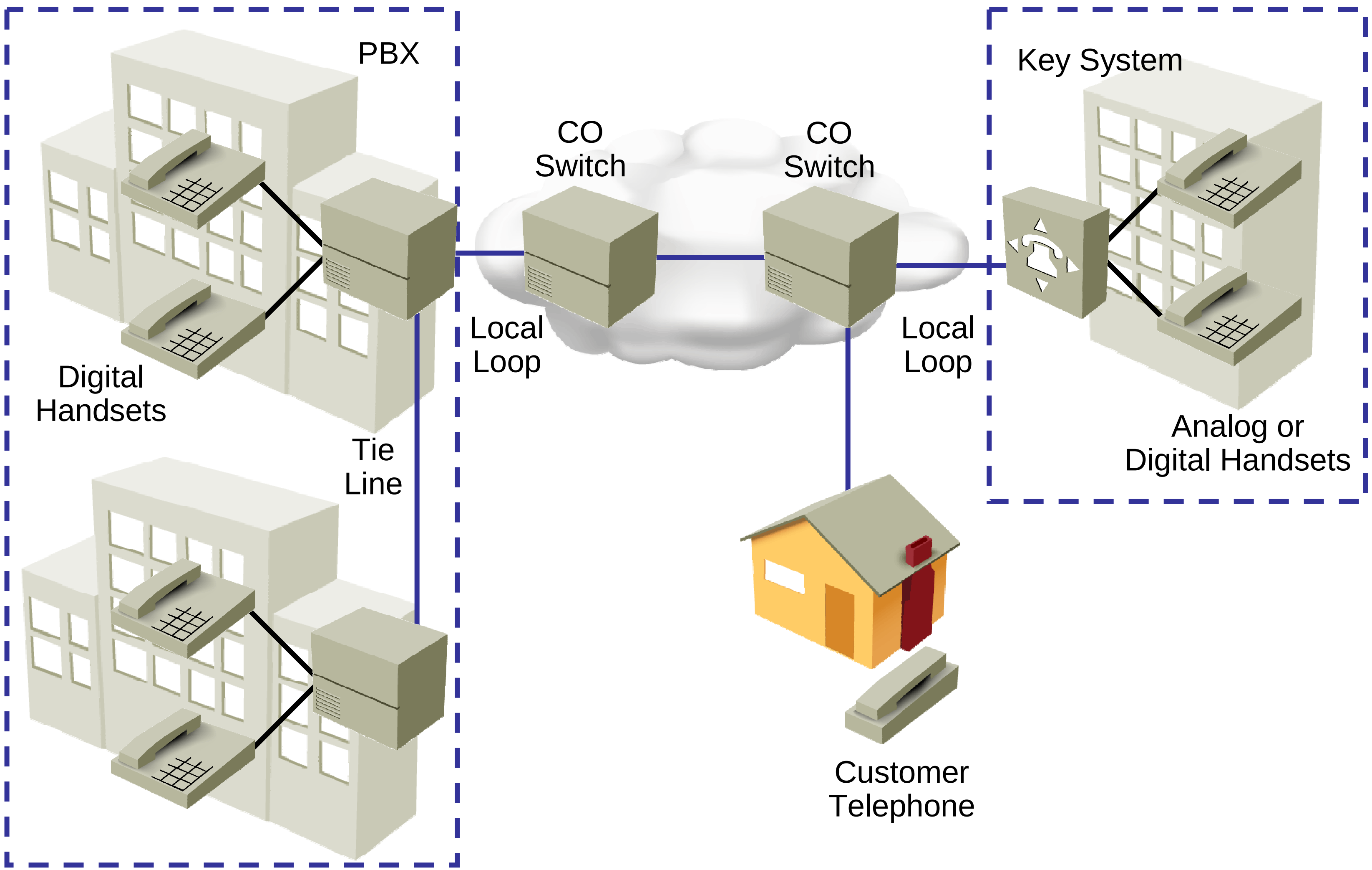
TRADITIONAL TELEPHONY

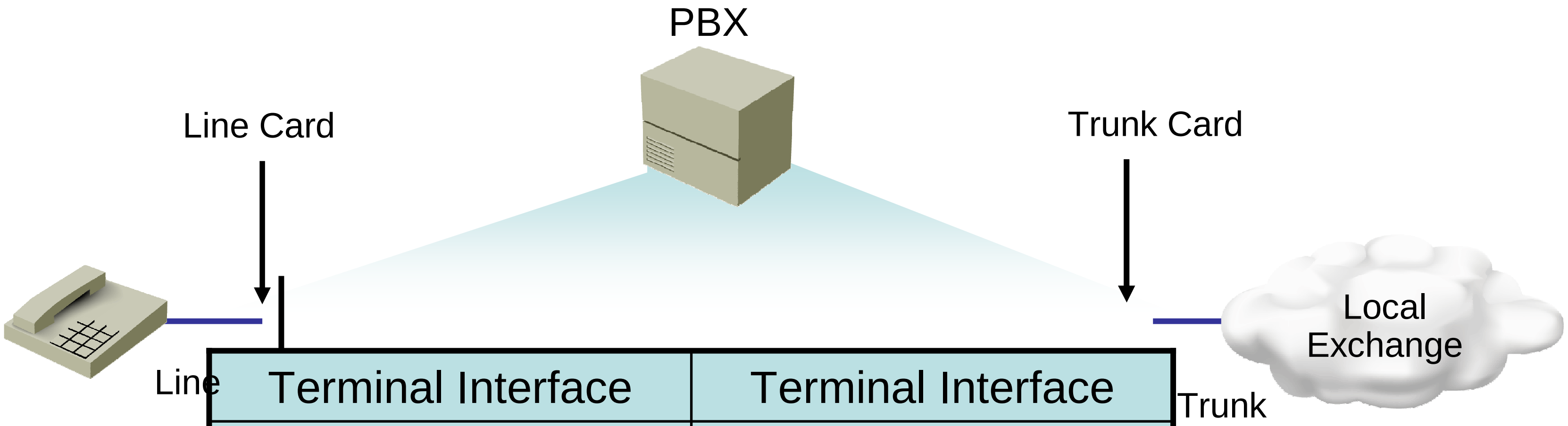
Public Switched Telephony Network



Traditional Business Phone System

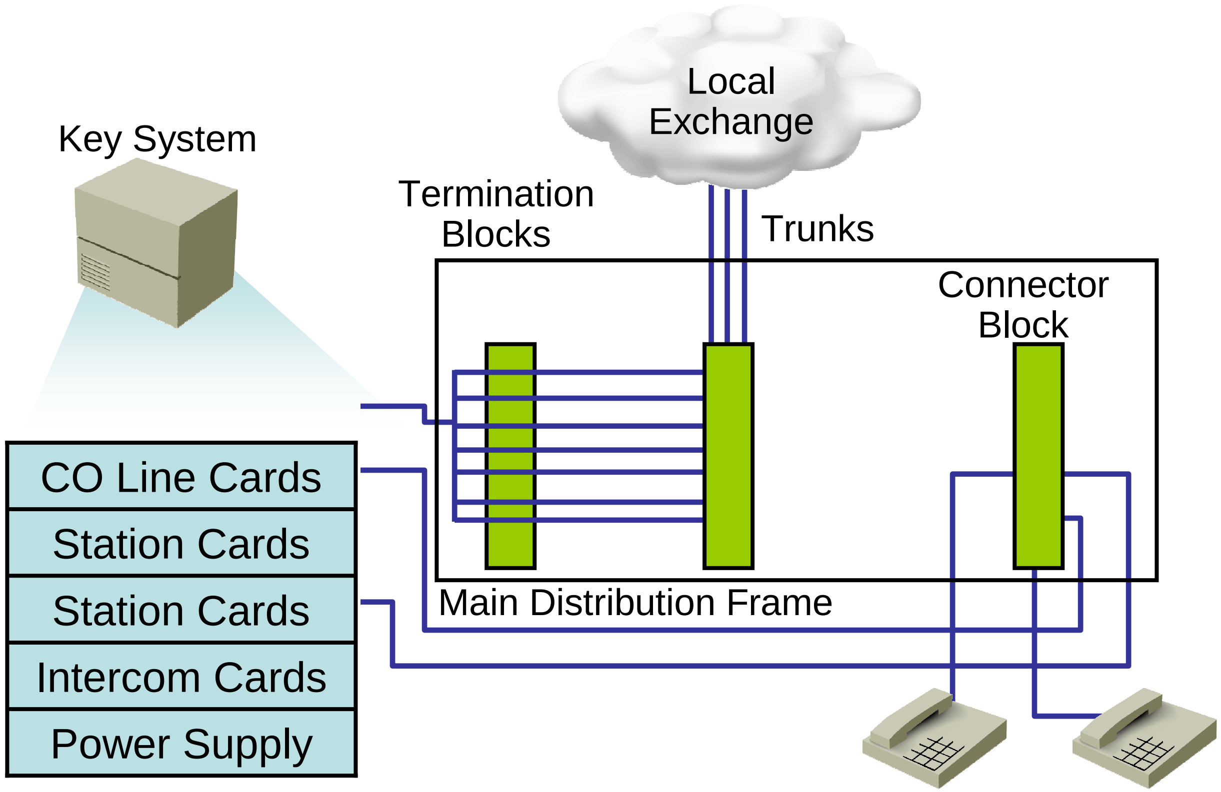


What Is a PBX?



Terminal Interface	Terminal Interface
Switching Network	Terminal Interface
Control Complex	Terminal Interface
Power Supply & Fans	Terminal Interface

What Is a Key System?



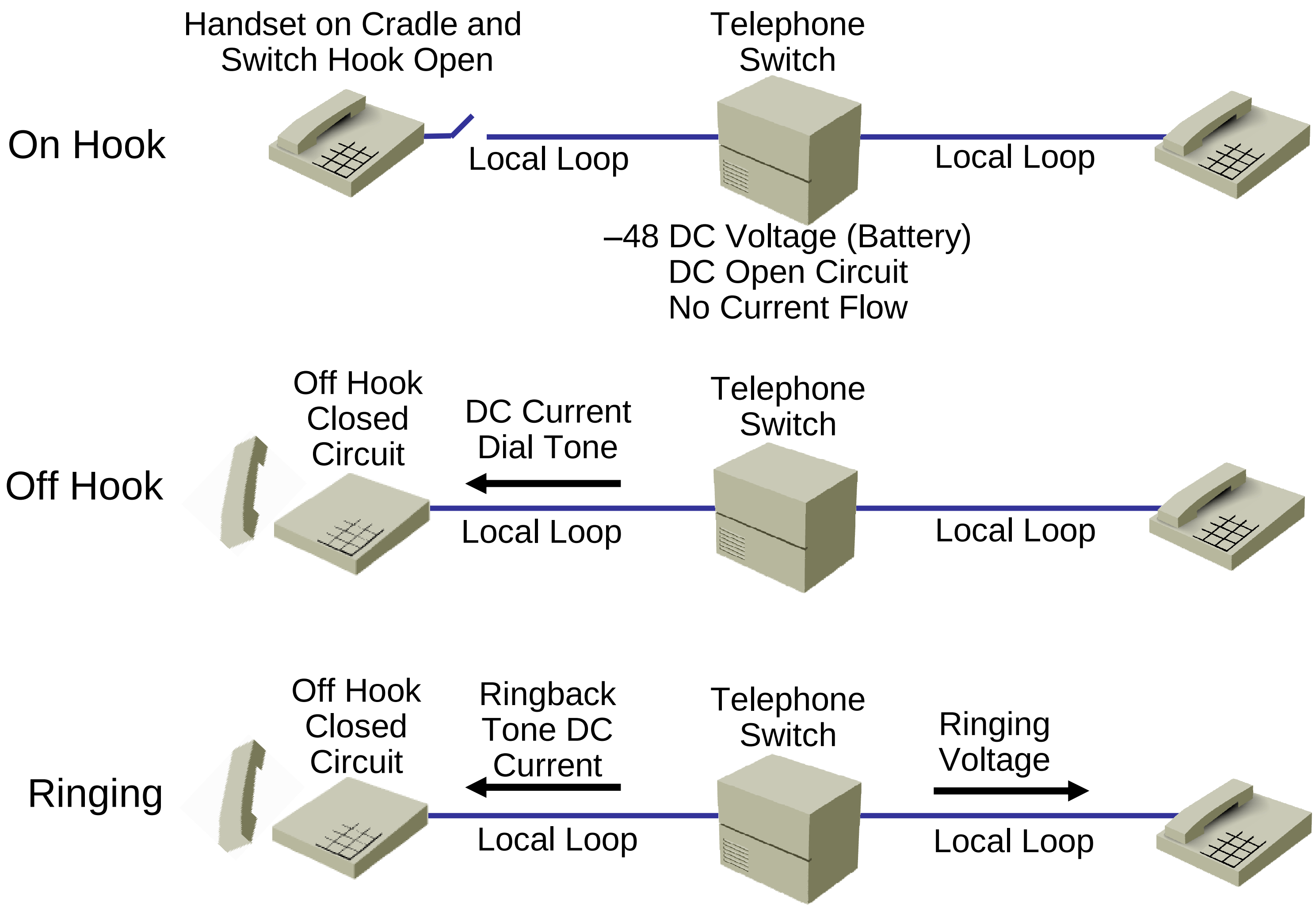
Comparing Key Systems to PBXs

	PBX	Key System
Technology	Primarily digital	Analog or digital
Switch Functionality	Similar to the CO switch	Not a switch
Typical Installation	Large company site (typically more than 50 users)	Small company or branch office (typically 50 or fewer users)
Method for Accessing Outside Trunks	Dial 9 or other access number to access outside line	Press a button to access outside line

Signaling Types

- There are three types of signaling used in a telephony network:
  - **Supervisory** signaling communicates the state of a telephony device.
  - **Address** signaling sends information about the digits dialed.
  - **Informational** signaling communicates the current state of the call.
- Signaling can be sent either **in-band** or **out-of-band.**
  - In-band signaling sends the signaling in the same communications channel as the voice.
  - Out-of-band signaling sends the signaling in a separate communications channel from the voice.

Supervisory Signaling



Address Signaling

008G_277

- Tone telephone
  - DTMF dialing

008G_276

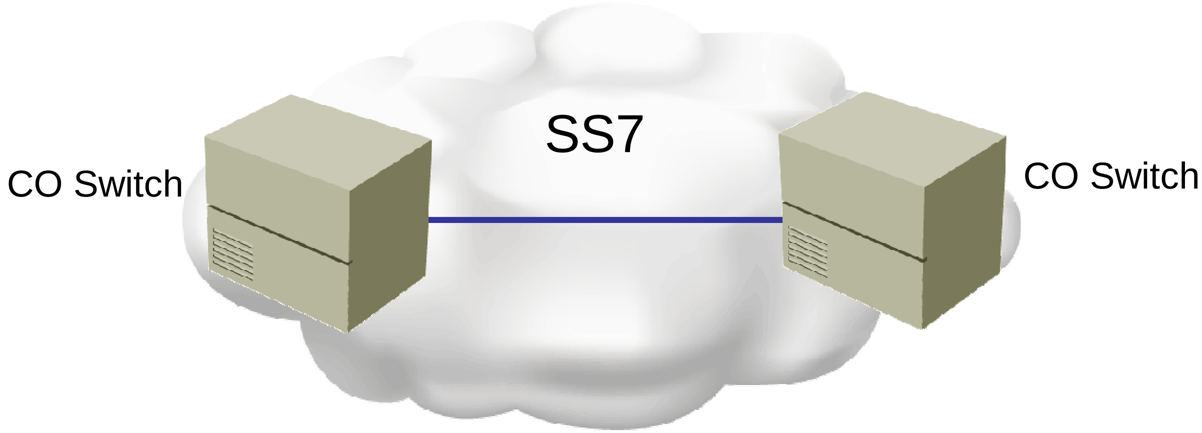
- Rotary telephone
  - Pulse dialing

Informational Signaling Example

Tone	Frequency (Hz)	On Time (Sec)	Off Time (Sec)
Dial	350 + 440	Continuous	Continuous
Busy	480 + 620	0.5	0.5
Ringback, line	440 + 480	2	4
Ringback, PBX	440 + 480	1	3
Congestion (toll)	480 + 620	0.2	0.3
Reorder (local)	480 + 620	0.3	0.2
Receiver off hook	(1400 + 2060 + 2450 + 2600)	0.1	0.1
No such number	200 to 400	Continuous	Continuous
Confirmation tone		Frequency modulation 1 kHz	Frequency modulation 1 kHz

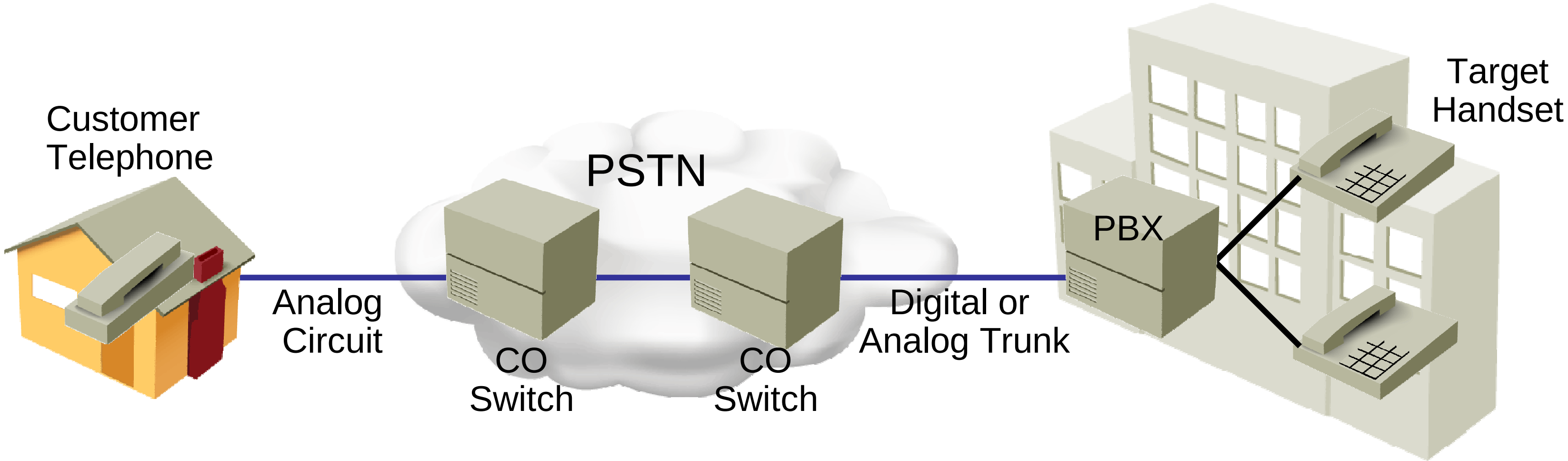
This information will vary based on the country.

Signaling System 7



- SS7 functions:
  - Informational signaling
  - Call setup
  - Call routing
  - Call billing
  - Toll-free number resolution
  - Used out-of-band signaling

PSTN Call Setup



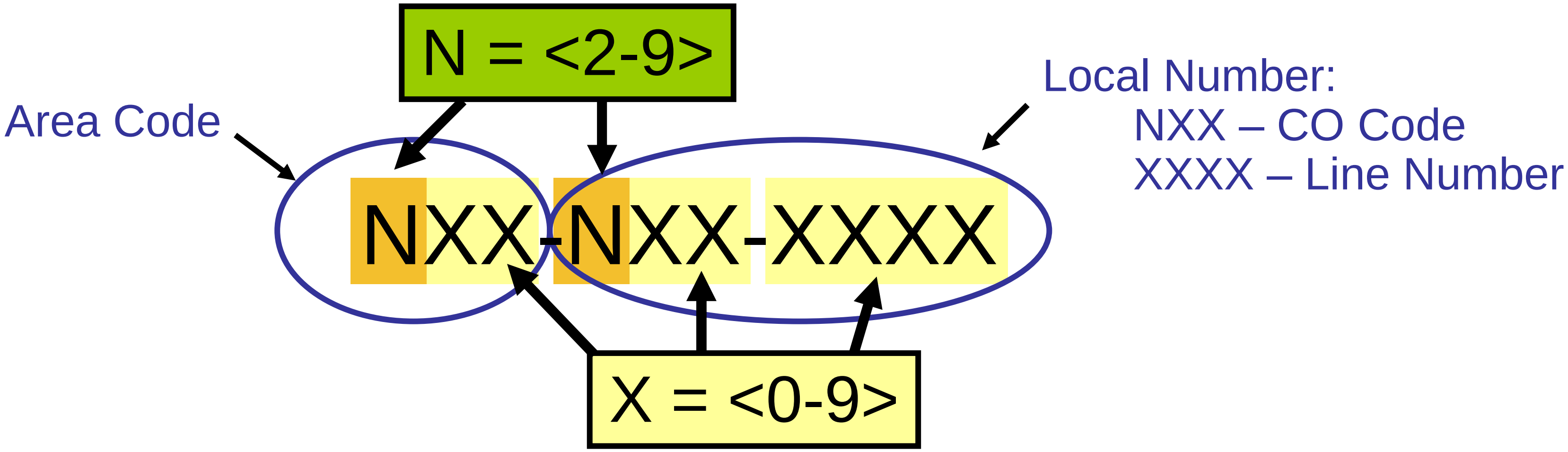
1. Customer phone goes off hook creating a closed circuit.
2. The customer's CO switch detects that current is flowing and generates dial tone to the customer phone.
3. Either DTMF or pulse digits are dialed by the customer.
4. The CO switch collects the digits and performs an SS7 lookup to determine the destination CO switch.
5. Supervisory signaling indicates to the far-end analog or digital trunk that an inbound call has arrived.
6. The PBX determines which internal extension the call should go to and causes the target handset with that extension to ring.
7. Ringback is generated to the customer phone by their local CO switch.
8. The target handset goes off hook and a circuit is built end-to-end.

Numbering Plans

- A numbering plan is a numbering scheme with the following characteristics:
  - Defines a set of rules to allocate numbers used in telecommunications
  - Is based on international telecommunications standards
  - Is established by numbering plan authorities, which regulate the distribution of numbers and codes in their territory
- Many regional and national numbering plans exist:
  - NANP
  - U.K. National Numbering Scheme
  - ETNS
  - Hong Kong
  - Many countries have their own numbering plans

North American Numbering Plan

- NANP is the numbering plan for the United States and its territories, Canada, Bermuda, and many Caribbean nations.
- It is administered by the NANPA.
- NANP numbers are 10-digit numbers.



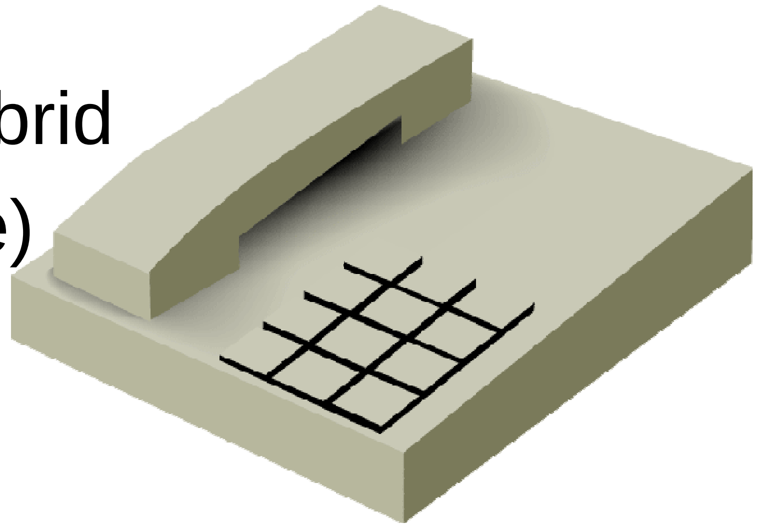
E.164 Addressing

- E.164 is an international numbering plan for public telephony systems:
  - A valid number contains the following components:
    - Country code
    - National destination code
    - Subscriber number
  - Each number can be up to 15 digits long.
  - The E.164 plan was developed by the ITU.

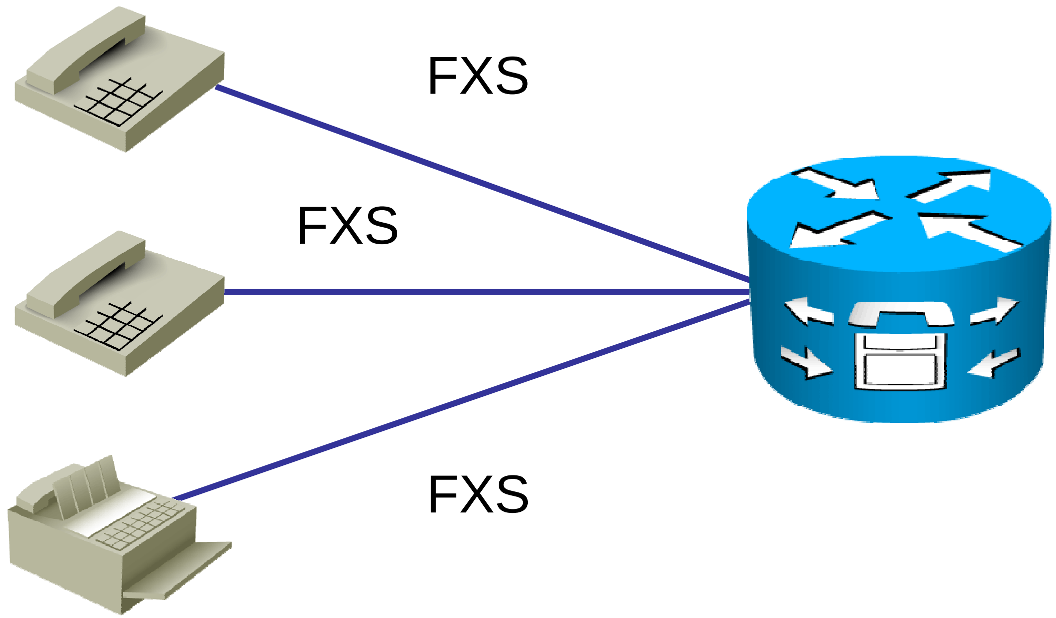
ANALOG TELEPHONY

Components of an Analog Telephone

- Receiver
- Transmitter
- Two-wire/four-wire hybrid
- Dialer (DTMF or pulse)
- Switch hook
- Ringer

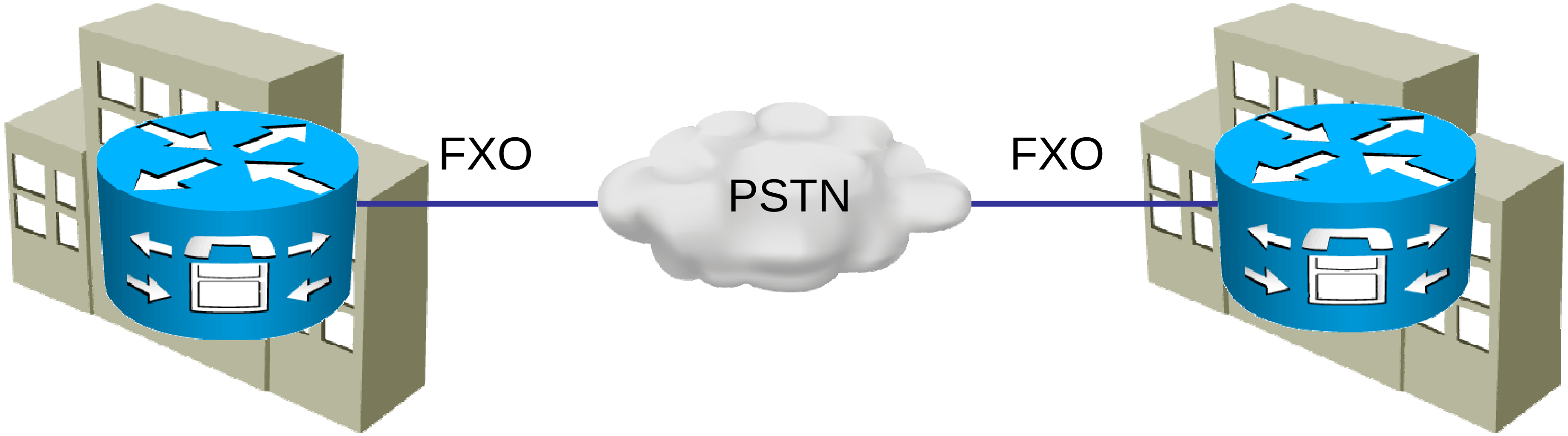


FXS Interface



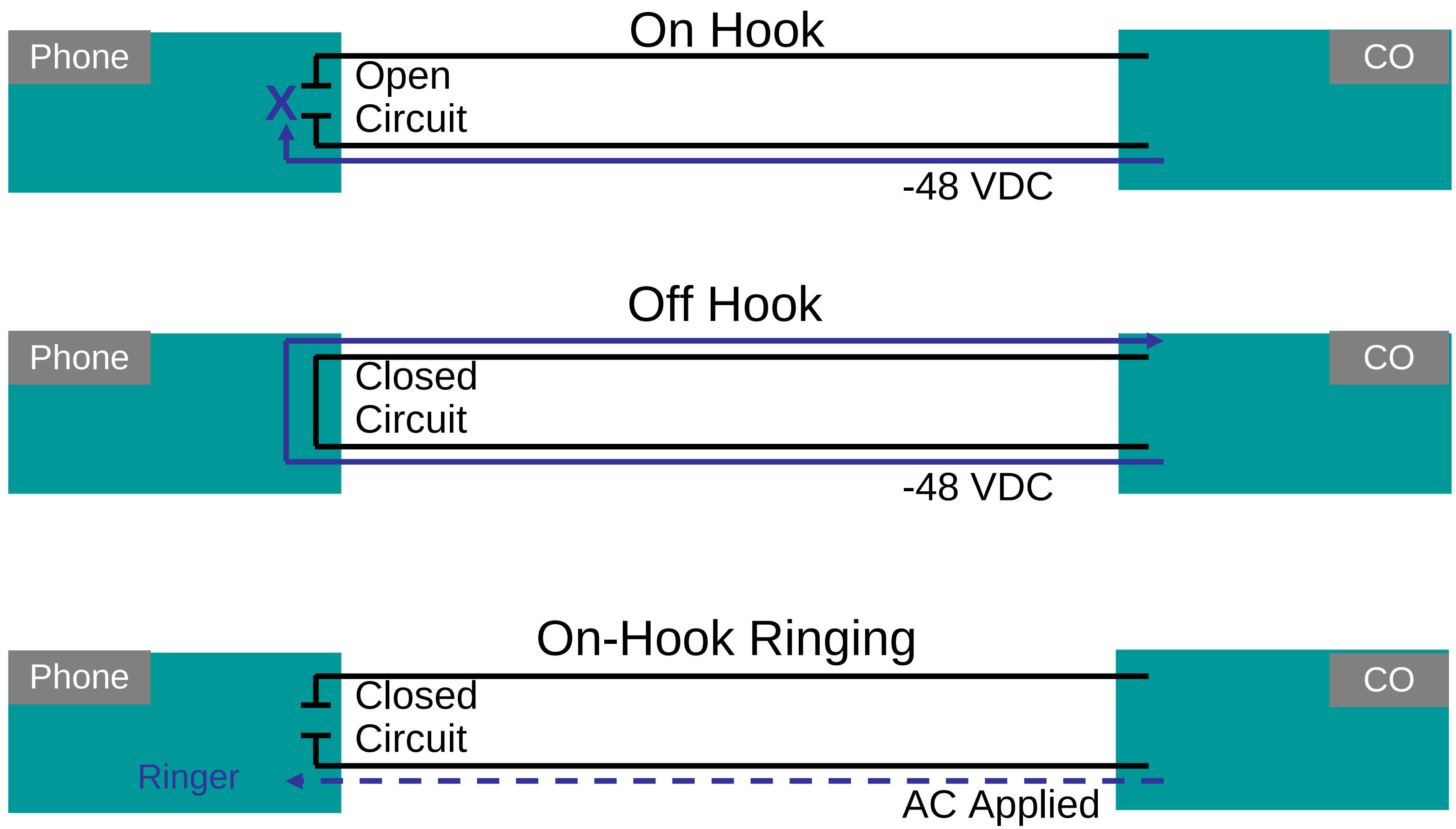
- Connects directly to analog phones or faxes
- Provisions local service
- Emulates the CO to the attached devices
- Provides power, call progress tones, and dial tone

FXO Interface



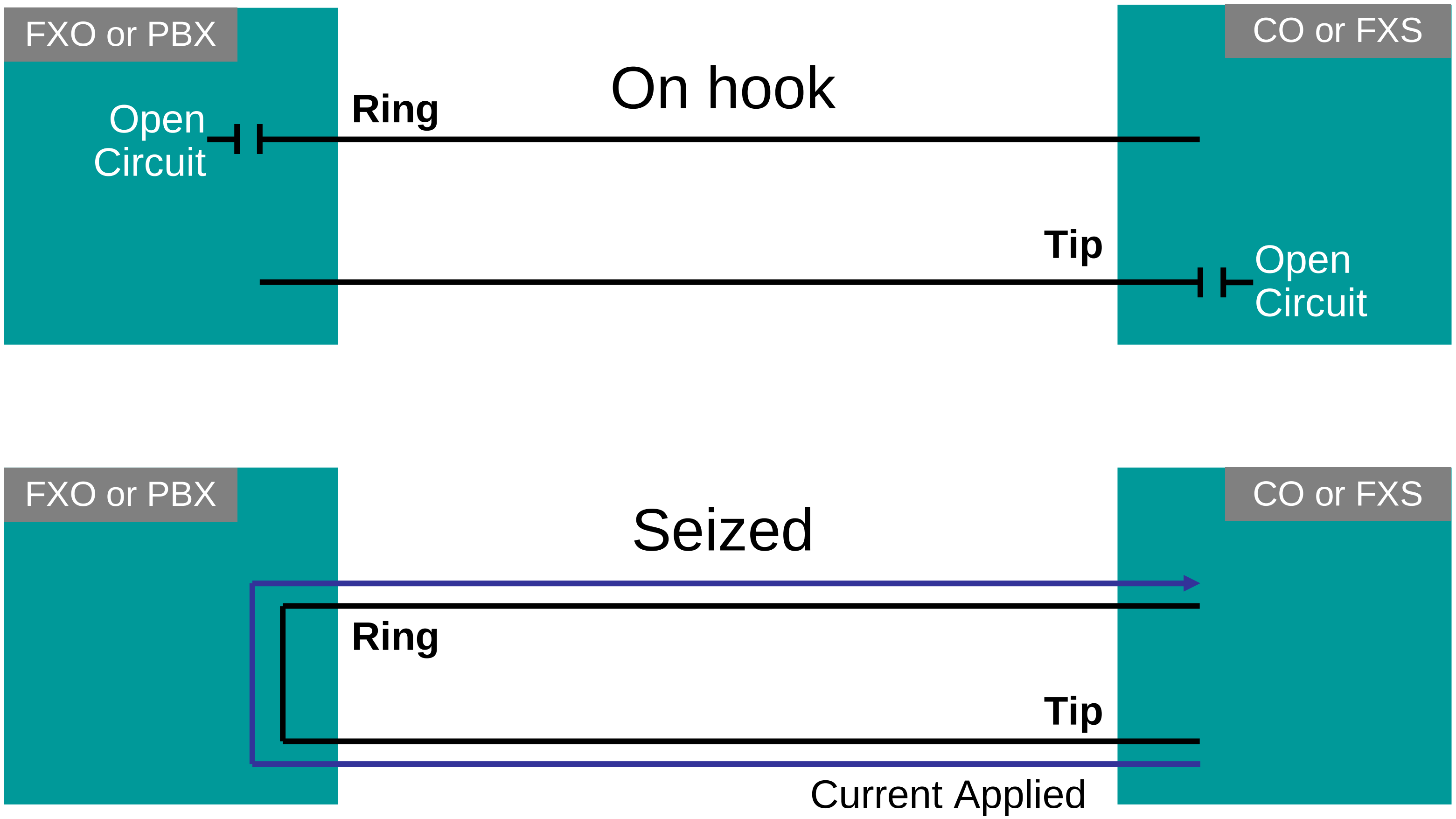
- Connects directly to office equipment
- Used to make and receive calls from the PSTN
- Can be used to connect through the PSTN to another site
- Answers inbound calls

Loop-Start Signaling



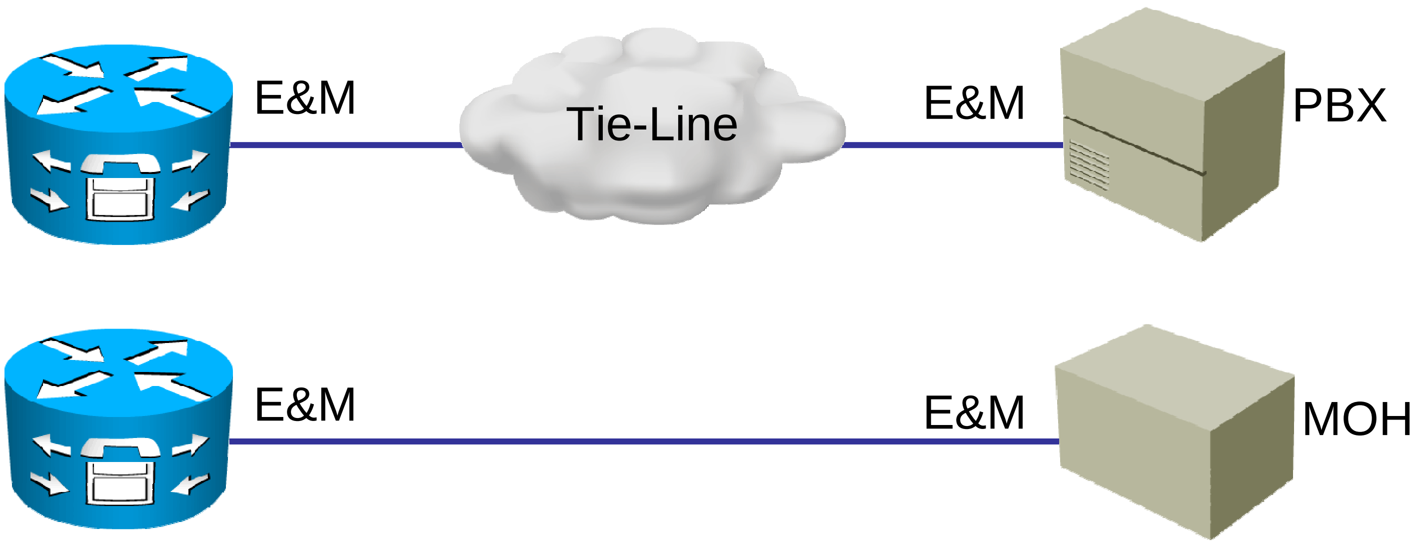
Loop-start signaling is typically used in residential environments.

Ground-Start Signaling



Ground-start signaling is typically used in business environments

E&M Interface



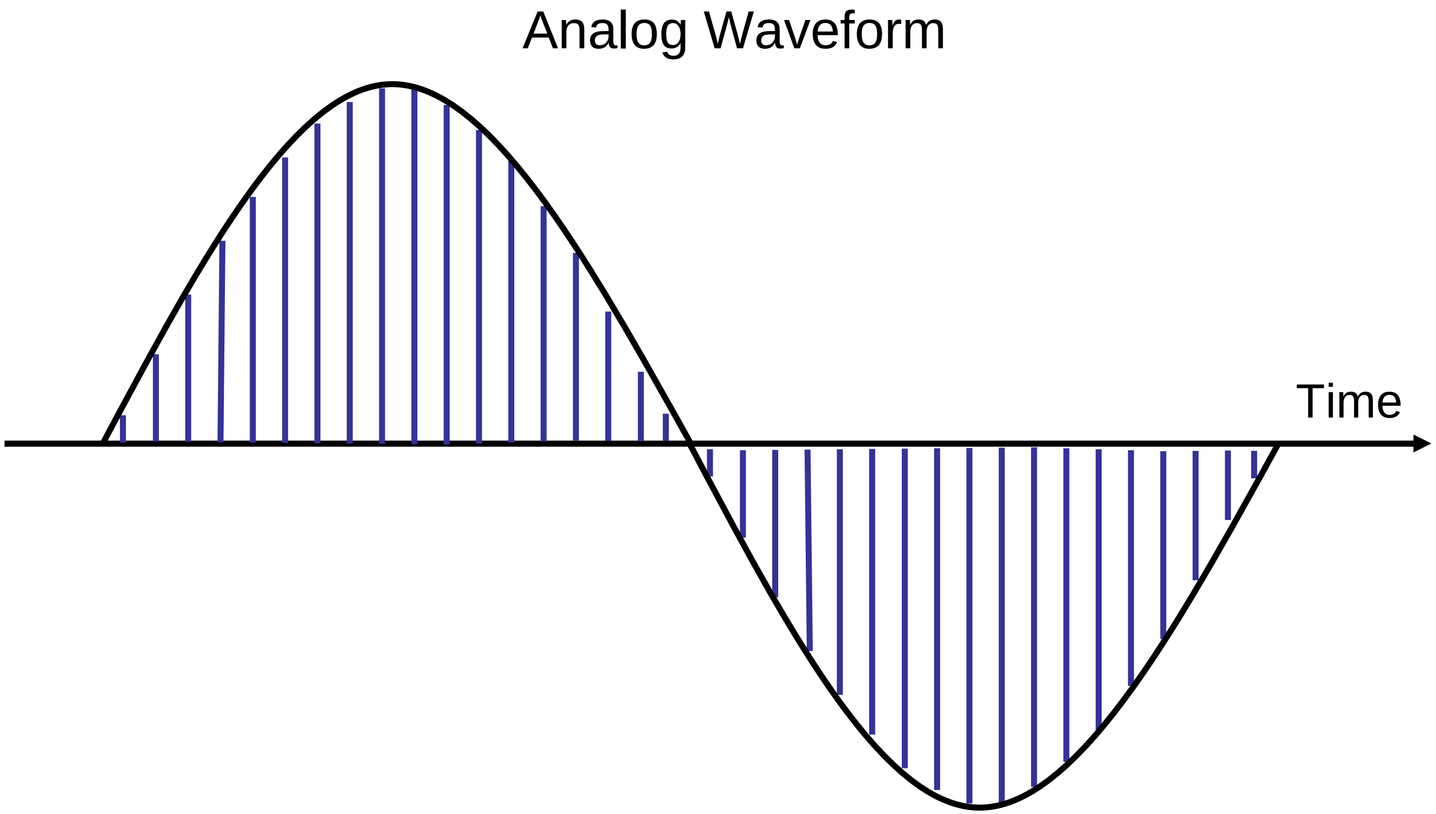
- Connects two sites with a leased connection
- Allows for the use of non-PSTN numbers
- Used to create tie-lines
- Commonly used to connect to external MOH sources

DIGITAL TELEPHONY

Digitizing Analog Signals

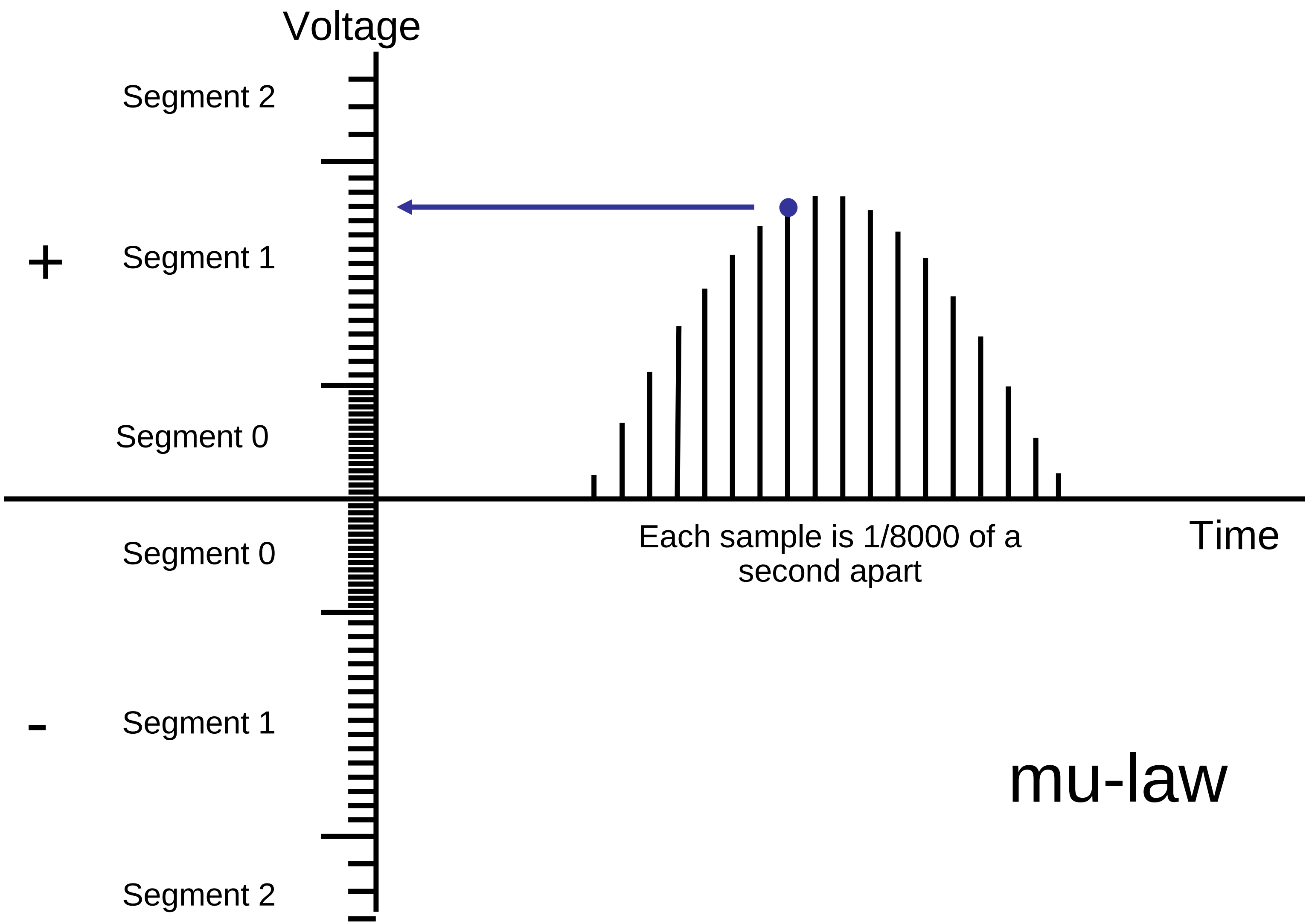
1. Sample the analog signal regularly.
2. Quantize the sample.
3. Encode the value into a binary expression.
4. Compress the samples to reduce bandwidth (optional).

Step 1—Sample the Signal



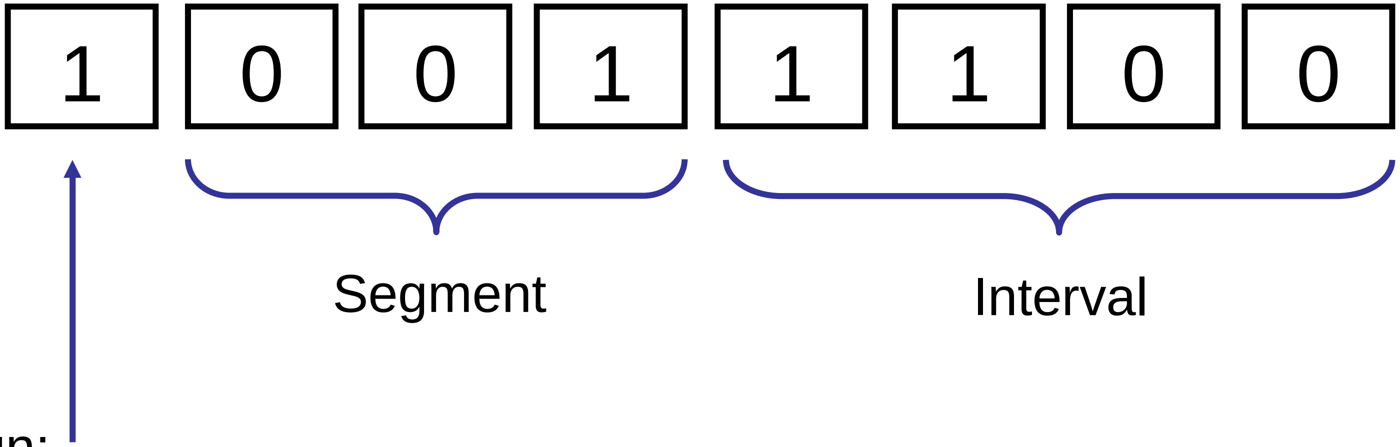
Each sample is 1/8000 of a second apart.

Step 2—Quantize the Signal



mu-law

Step 3—Encode the Signal in Binary



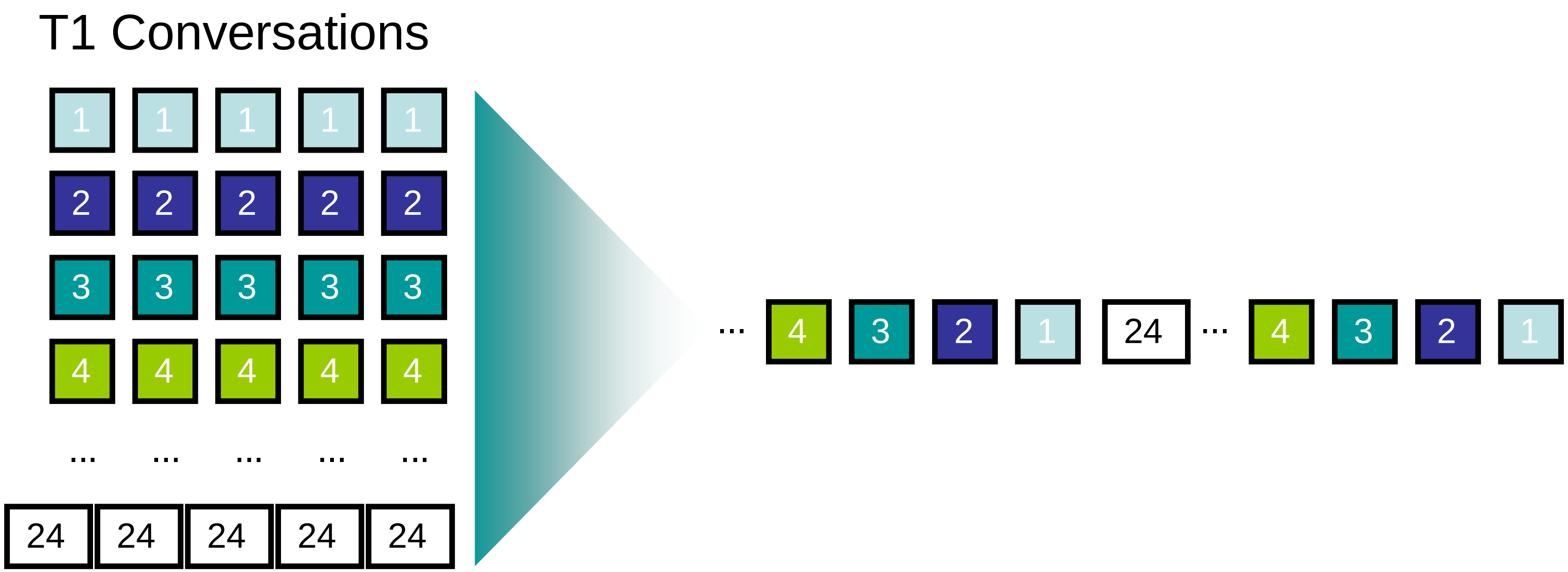
Sign:

- 1 = Positive
- 0 = Negative

Step 4—Compress the Samples (Optional)

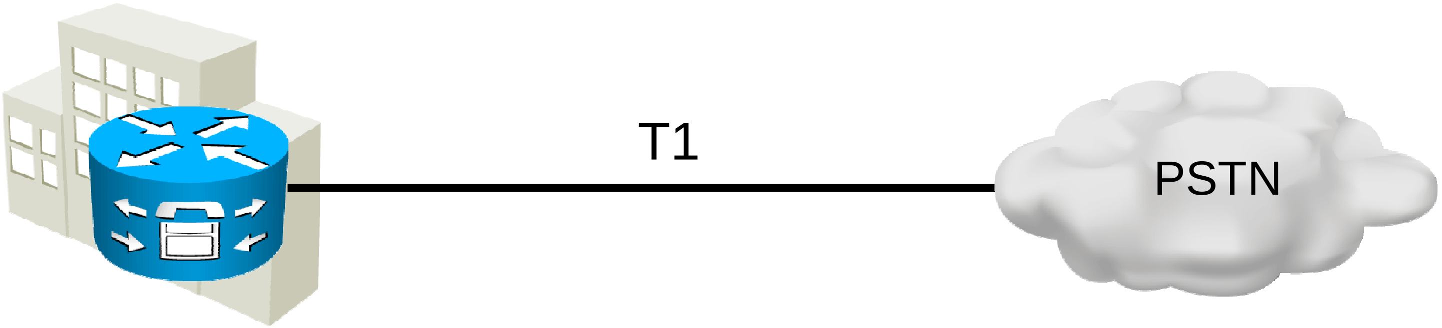
- ADPCM
  - Sends only the differential between the current and last sample
  - Uses G.726 variants
  - Allows encoding PCM data rates of 16 kb/s, 24 kb/s, or 32 kb/s per call
  - Has lower quality than G.729
  - Is not commonly used today
- CS-ACELP
  - Is based on the human vocal system
  - Matches sounds to a codebook of possible sounds
  - Uses G.729 variants
  - Is the most common compression method used today
  - Has a data rate of 8 kb/s per call
  - Provides high quality

Time-Division Multiplexing



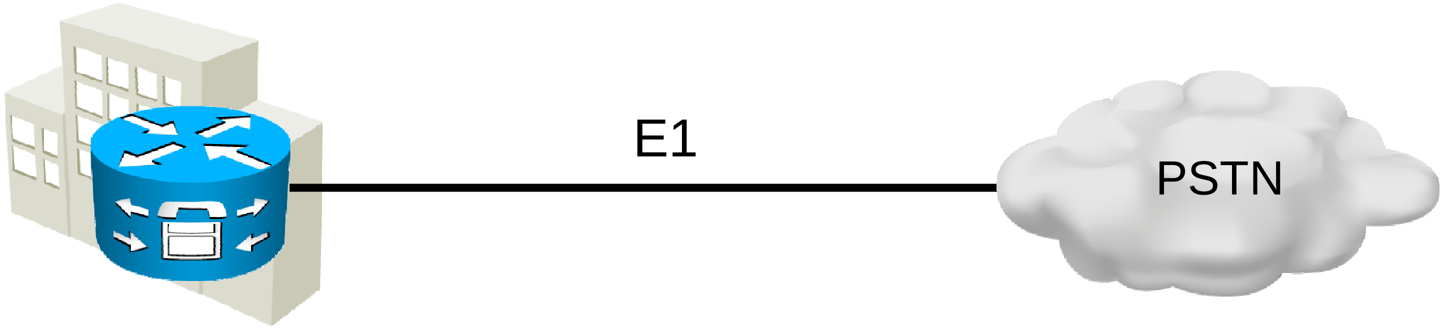
For E1, the conversations would be 1 through 30.

T1 Circuits



- Up to 24 channels for voice
- Each channel is a DS0
- Each DS0 is 64 kb/s
- 8000 samples per second
- One byte per sample
- One sample per channel, per frame
- SF groups together 12 frames
- ESF groups together 24 frames
- Typically used in the United States, Canada and Japan (called J1)

E1 Circuits



- Up to 30 channels for voice
- One channel for signaling
- One channel for framing
- Each channel is a DS0
- Each DS0 is 64 kb/s
- 8000 samples per second in voice DS0s
- One byte per sample
- One sample per channel, per frame
- 16 frames are grouped together to make a multiframe

Channel Associated Signaling

	CAS T1	CAS E1
Number of Voice Channels	24	30
Signaling Method	RBS in-band	Out-of-band signaling in time slot 17
Speed	1.544 Mb/s	2.048 Mb/s
Where Predominately Used	United States, Canada, Japan	The rest of the world

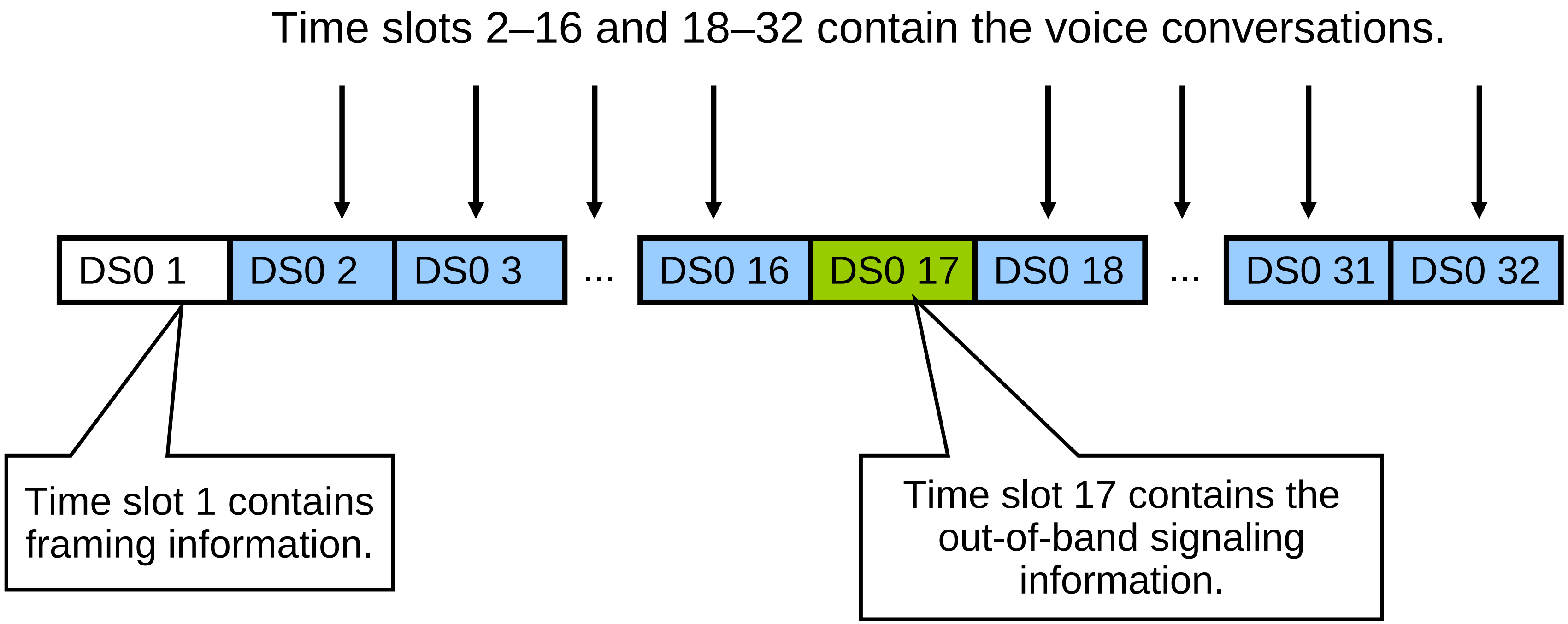
CAS—T1

DS0 = 64 kb/s

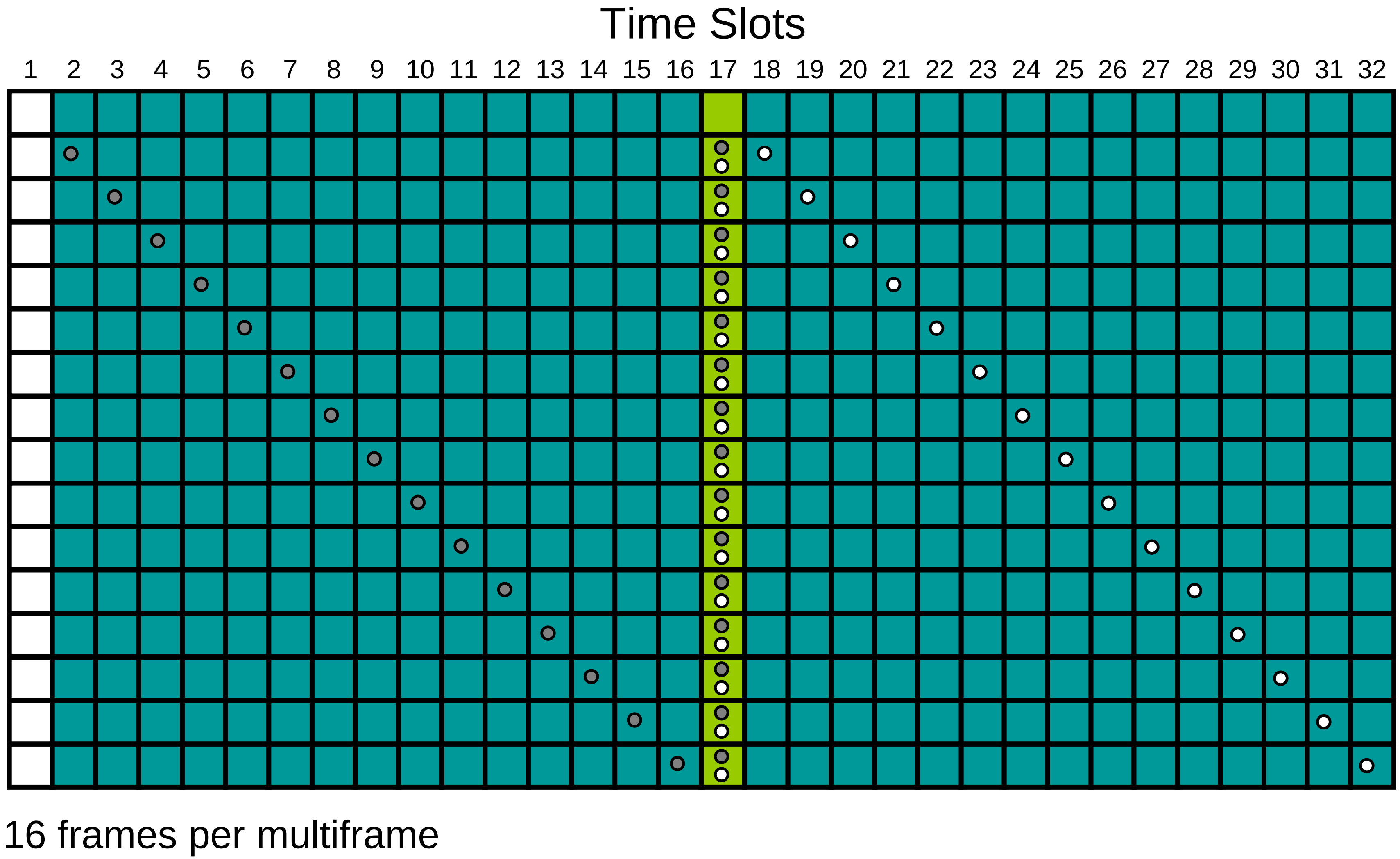
DS0 1	DS0 2	DS0 3	DS0 4	...	DS0 24	F	Frame 1
...	...	...	...		...		
DS0 1	DS0 2	DS0 3	DS0 4	...	DS0 24	F	Frame 5
DS0 1A	DS0 2A	DS0 3A	DS0 4A	...	DS0 24A	F	Frame 6
...	...	...	...		...		
DS0 1	DS0 2	DS0 3	DS0 4	...	DS0 24	F	Frame 11
DS0 1B	DS0 2B	DS0 3B	DS0 4B	...	DS0 24B	F	Frame 12
...	...	...	...		...		
DS0 1	DS0 2	DS0 3	DS0 4	...	DS0 24	F	Frame 17
DS0 1C	DS0 2C	DS0 3C	DS0 4C	...	DS0 24C	F	Frame 18
...	...	...	...		...		
DS0 1	DS0 2	DS0 3	DS0 4	...	DS0 24	F	Frame 23
DS0 1D	DS0 2D	DS0 3D	DS0 4D	...	DS0 24D	F	Frame 24

CAS—E1

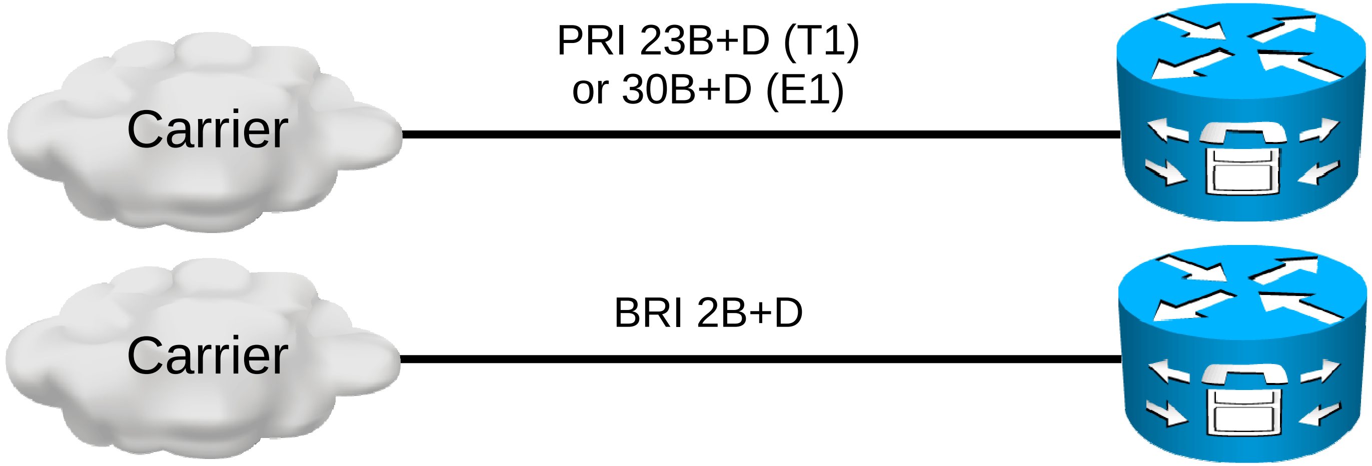
DS0 = 64kb/s



CAS—E1 (Cont.)

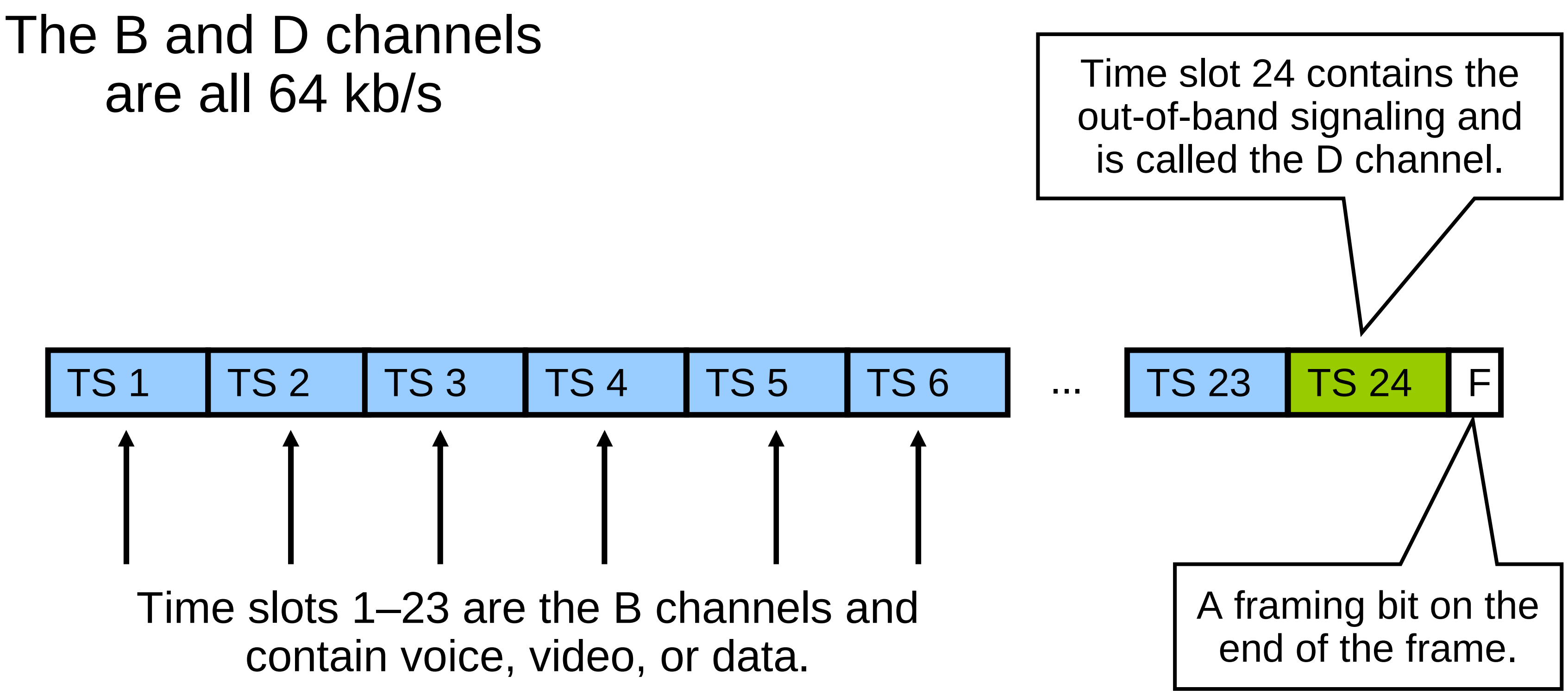

Time Slots
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
16 frames per multiframe

Common Channel Signaling



- Allows for multiple services through one connection
- Is well-adapted for voice
  - 64-kb/s B channels
  - Q.931 protocol used on the D channel
- Supports standards-based functions
- Supports proprietary signaling on the D channel
- Is used internationally

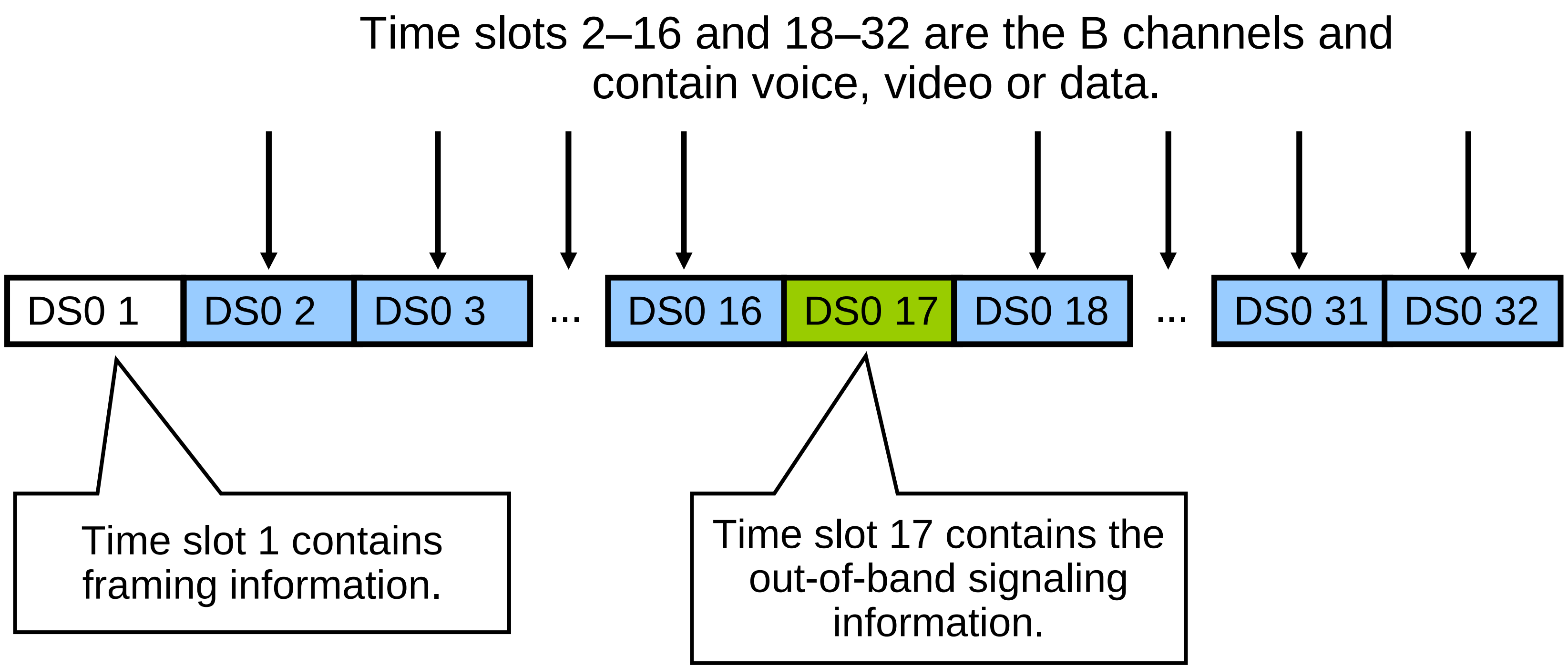
CCS—PRI T1



The B and D channels
are all 64 kb/s
Time slot 24 contains the
out-of-band signaling and
is called the D channel.
TS 1
TS 2
TS 3
TS 4
TS 5
TS 6
...
TS 23
TS 24
F
Time slots 1–23 are the B channels and
contain voice, video, or data.
A framing bit on the
end of the frame.

CCS—PRI E1

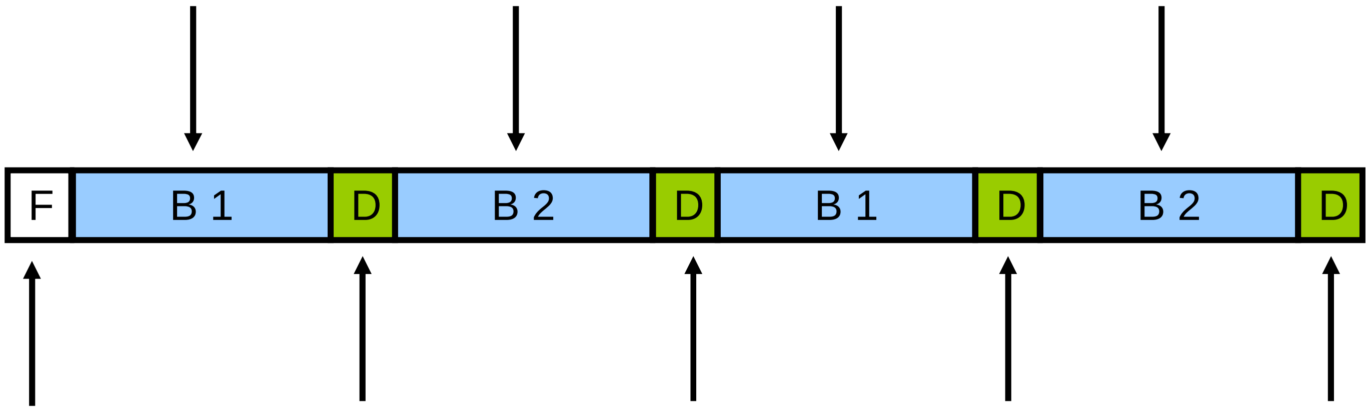
The B and D channels
are all 64 kb/s



CCS—BRI

The two B channels are 64 kb/s;
the D channel is 16 kb/s

The 32 bits total for the two B channels contain the voice, video, or data.

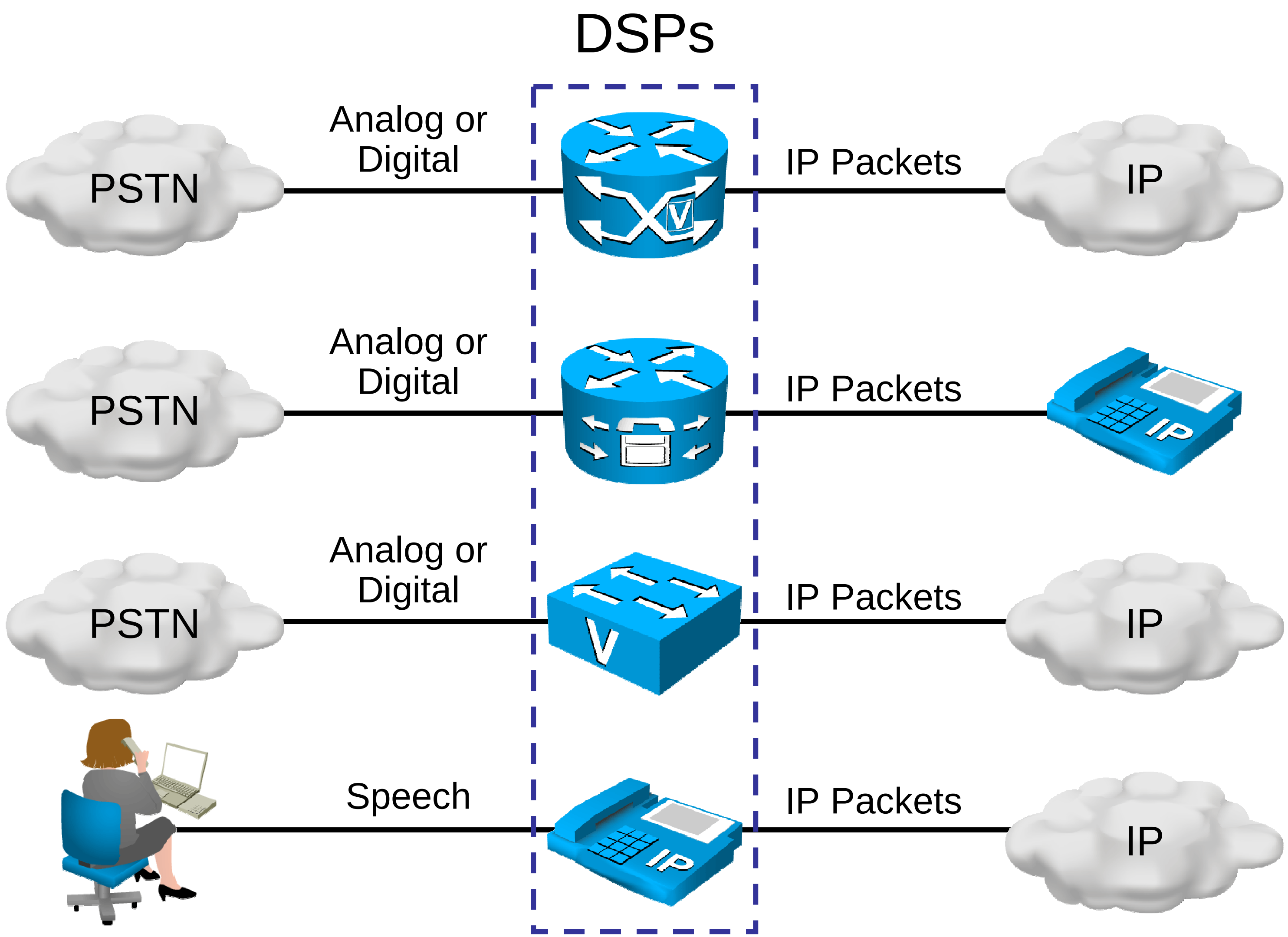


Framing bit

The four total D bits contain the signaling information.

UNDERSTANDING PACKETIZATION

Digital Signal Processors



Digital Signal Processors (Cont.)

– The DSP chip performs the **sampling, quantization, encoding, and optional compression step of digitization**.
– It is used in both directions to convert from a traditional analog or digital voice signal to VoIP; or from VoIP to a traditional analog or digital voice signal.
– The number of simultaneous calls a chip can handle depends on the type of DSP and the codec being used.

Real-Time Transport Protocol

- Provides end-to-end network functions and delivery services for delay-sensitive, real-time data, such as voice and video
- Randomly picks even ports from UDP port range 16384–32767
- Includes the following services:
  - Payload type identification
  - Sequence numbering
  - Time stamping

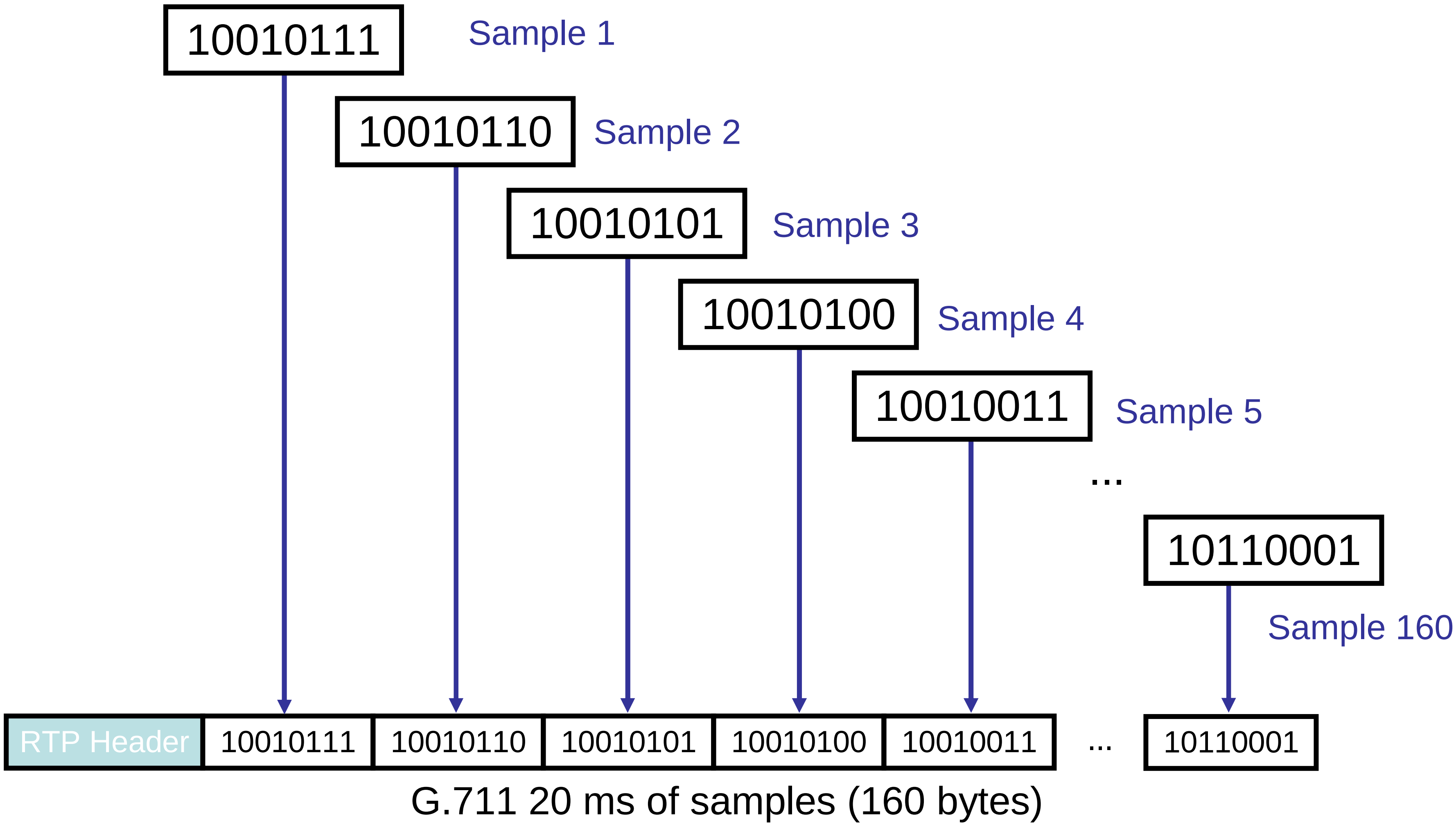
RTP Control Protocol

- Can be used to monitor the quality of the data distribution and provide control information
- Provides feedback on current network conditions
- Allows hosts that are involved in an RTP session to exchange information about monitoring and controlling the session:
  - Packet count
  - Packet delay
  - Octet count
  - Packet loss
  - Jitter (variation in delay)
- Provides a separate flow from RTP for UDP transport use
- Is paired with its RTP stream and uses the same port as the RTP stream plus 1 (odd-numbered port)

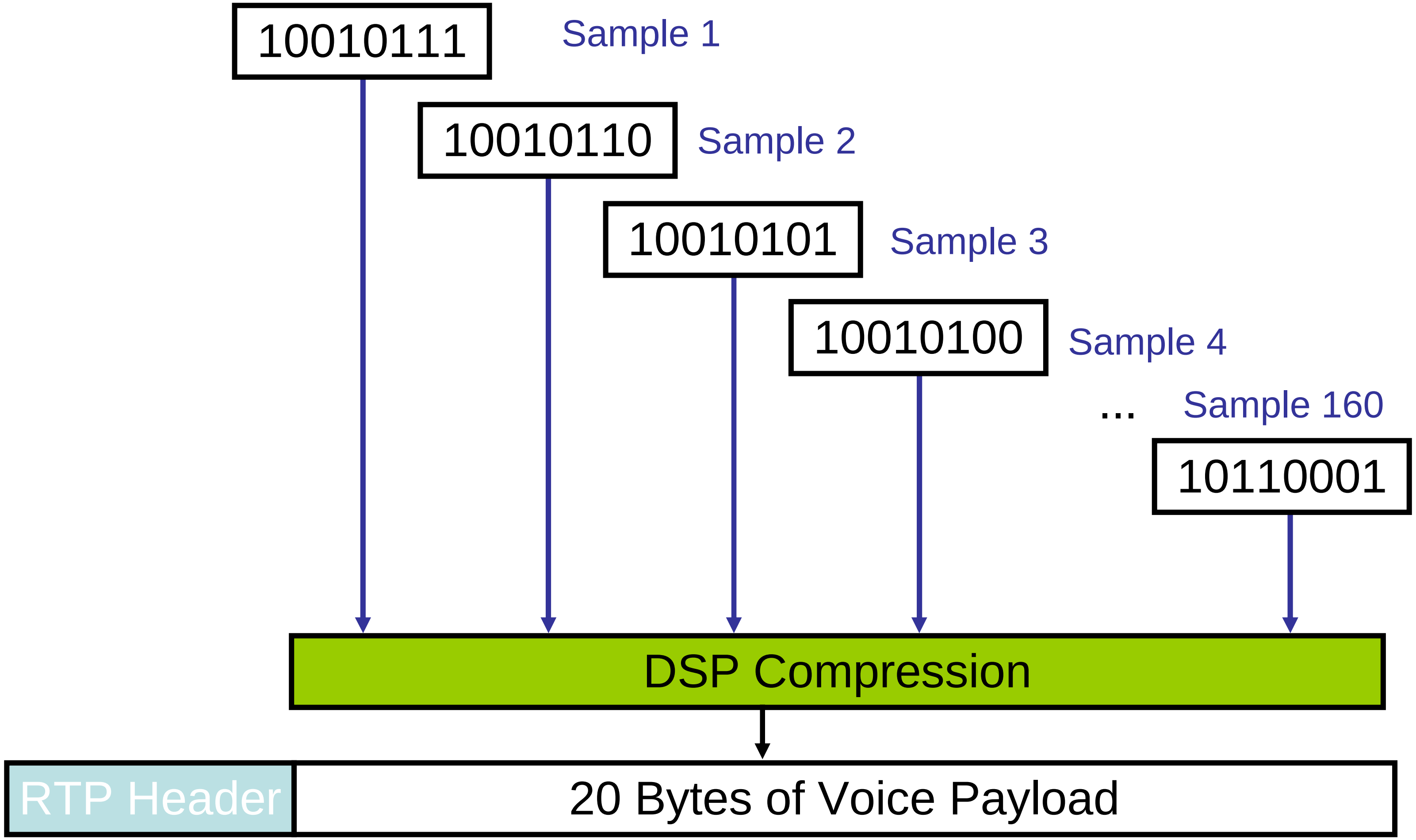
Packetization

- Packetization of voice is performed by DSP resources.
- The DSP packages voice samples or compressed voice into IP packets.
- The voice data is collected until the packet payload is full.
- The voice data is carried in the payload of RTP segments.
- RTP is encapsulated in a UDP segment, which is encapsulated in an IP packet.
- The IP packet is encapsulated into the Layer 2 format.

Packetization—G.711 Example



Packetization—G.729 Example



G.729 20 ms of voice contained in packet

Codecs

- Standardized ways to encode voice for transport across a data network:
  - PCM
    - G.711 rate: 64 kb/s = (2 x 4 kHz) x 8 bits/sample
  - ADPCM
    - G.726 rate: 32 kb/s = (2 x 4 kHz) x 4 bits/sample
    - G.726 rate: 24 kb/s = (2 x 4 kHz) x 3 bits/sample
    - G.726 rate: 16 kb/s = (2 x 4 kHz) x 2 bits/sample
  - LD-CELP
    - G.728 rate: 16 kb/s
  - CS-ACELP
    - G.729: rate 8kb/s
    - Annex A variant—less processor-intensive and allows more voice channels encoded per DSP
    - Annex B variant—VAD and CNG
  - iLBC
    - Rate: 13.3 kb/s

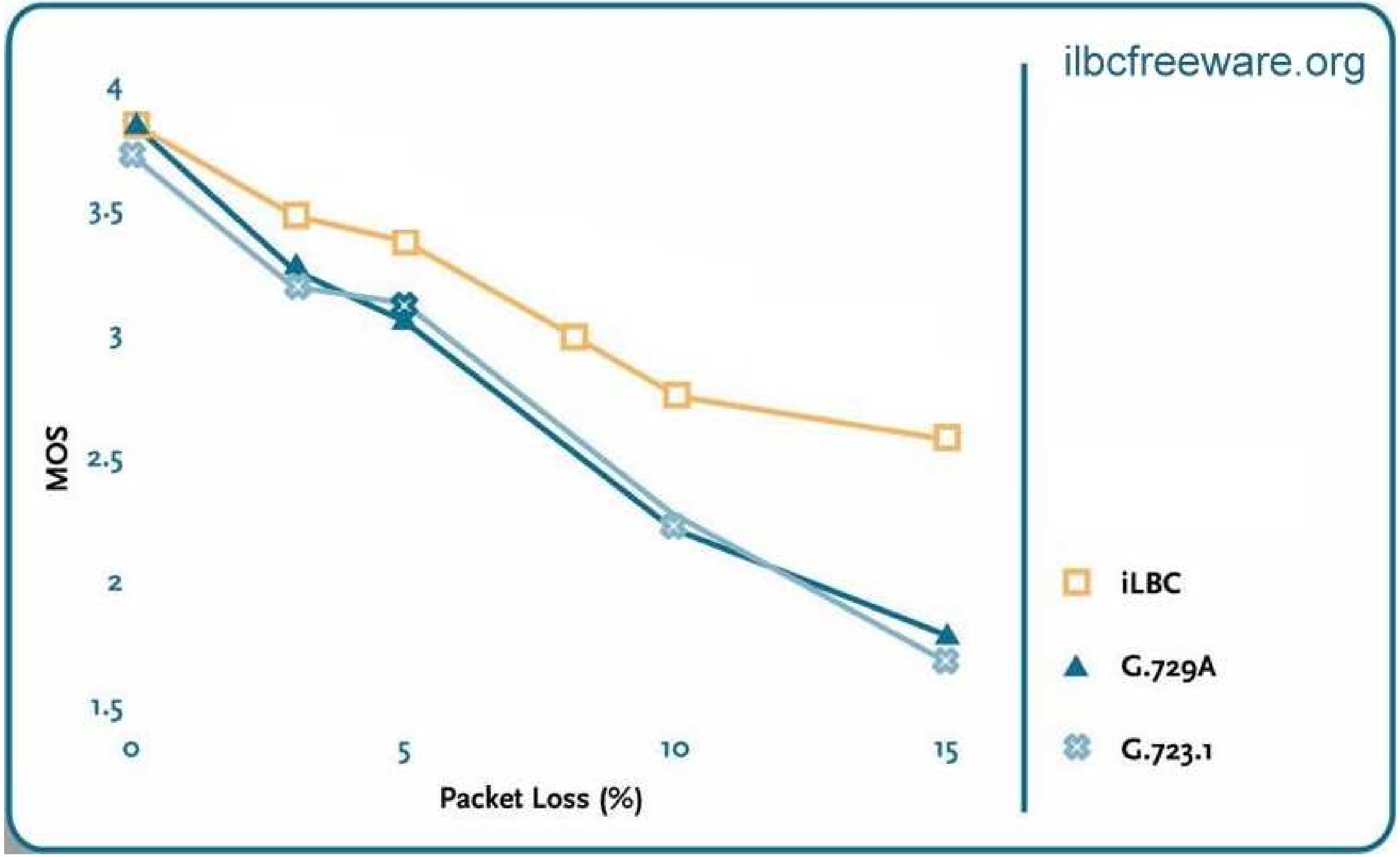
Codecs—G.729 and G.729A Comparison

- Both codecs are ITU standards.
- Both codecs are 8-kb/s CS-ACELP.
- G.729 is more complex and processor-intensive.
- G.729 is slightly higher quality than G.729A.
- The compression delay is the same (10 to 20 ms).
- The Annex B variant can be applied to either codec.
- The Annex B variant adds VAD and CNG.

Internet Low Bitrate Codec

- Was designed for packetized communications
- Is royalty free
- Has better quality than G.729
- Has similar complexity as G.279
- Supports two fixed bit-rate frame lengths:
  - A bit rate of 13.3 kb/s with an encoding frame length of 30 ms
  - A bit rate of 15.2 kb/s with an encoding frame length of 20 ms
- Is supported only on newer Cisco Unified IP Phones:
  - IP Phone 7975G
  - IP Phone 7965G
  - IP Phone 7962G
  - IP Phone 7945G
  - IP Phone 7942G
  - IP Phone 7921G
  - IP Phone 7911G
  - IP Phone 7906G
- Is supported on the VoIP dial peers of Cisco voice gateways using the following protocols:
  - H.323
  - SIP

iLBC—Packet Loss Comparison



Codecs—Bandwidth Implications

Codec	G.711 *	G.726 r32	G.726 r24	G.726 r16	G.728	iLBC *	G.729 *	G.723 r63	G.723 r53
Bandwidth not including overhead	64 kb/s	32 kb/s	24 kb/s	16 kb/s	16 kb/s	13.3 kb/s	8 kb/s	6.3 kb/s	5.3 kb/s

* G.711, G.729, and iLBC are the most common codecs.

Codec—Overhead

- RTP/UDP/IP header overhead
  - 40 bytes of overhead
  - 2 or 4 bytes of overhead if using cRTP
- Data link overhead (Layer 2 header and trailer)
  - Ethernet—18 bytes of overhead
  - MLP—6 bytes of overhead
  - FRF.12—6 bytes of overhead

Codec—Total Bandwidth Required

•Codec	•Codec Speed	•Sample Size	•Frame Relay	•Frame Relay with cRTP	•Ethernet
•G.711	•64,000	•240	•76,267	•66,133	•78,933
•G.711	•64,000	•160	•82,400	•67,200	•86,400
•iLBC	•13,300	•30	•26,100	•16,000	•34,100
•iLBC	•15,200	•20	•34,400	•19,200	•46,400
•G.729	•8000	•40	•17,200	•9600	•19,200
•G.729	•8000	•20	•26,400	•11,200	•30,400

The Effect of VAD

•Codec	•Codec Speed	•Sample Size	•Frame Relay	•Frame Relay with VAD
•G.711	•64,000	•240	•76,267	•49,573
•G.711	•64,000	•160	•82,400	•53,560
•iLBC	•13,300	•30	•26,100	•16,965
•iLBC	•15,200	•20	•34,400	•22,360
•G.729	•8000	•40	•17,200	•11,180
•G.729	•8000	•20	•26,400	•17,160

Additional DSP Functions

– Hardware-based conferencing

– MTP

– Transcoding between two different codecs

– Echo cancellation

INTRODUCING SIGNALING PROTOCOL

VoIP Signaling Protocols

- Signaling generates and monitors the call control information between two endpoints to:
  - Establish the connection
  - Monitor the connection
  - Release the connection
- The signaling protocol must pass **supervisory, informational, and address signaling.**
- Signaling protocols can be peer-to-peer or client/server-based.
  - Peer-to-peer allows the endpoints to contain intelligence to place calls without assistance.
  - Client/server puts the endpoint under the control of a centralized intelligence point.

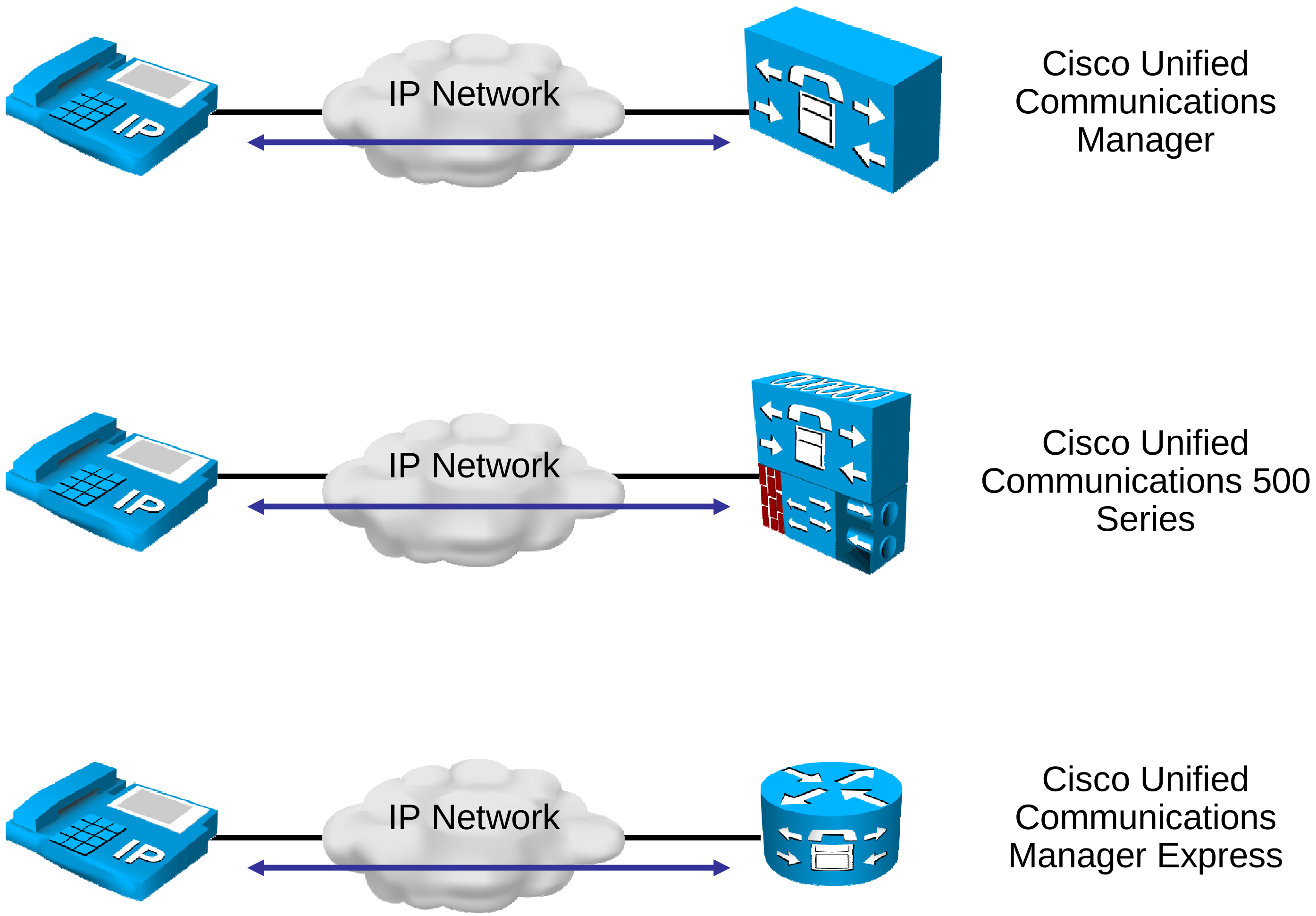
VoIP Signaling Protocols Comparison

	Standards Body	Vendor Neutrality	Used on Gateways	Used on Cisco Unified IP Phones	Architecture
H.323	ITU	Very Good	Yes	No	Peer-to-peer
MGCP	IETF	Good	Yes	Yes, limited	Client/server
SIP	IETF	Basic	Yes	Yes, Cisco Unified IP Phones and third-party phones	Peer-to-peer
SCCP	None	Proprietary	Yes, limited	Yes, Cisco Unified IP Phones only	Client/server

Skinny Client Control Protocol

- Signaling protocol used between Cisco Unified Communications call control platforms and Cisco Unified IP Phones
- Cisco proprietary
- Lightweight protocol
- Client/server protocol
- Used for voice only and video-enabled calls

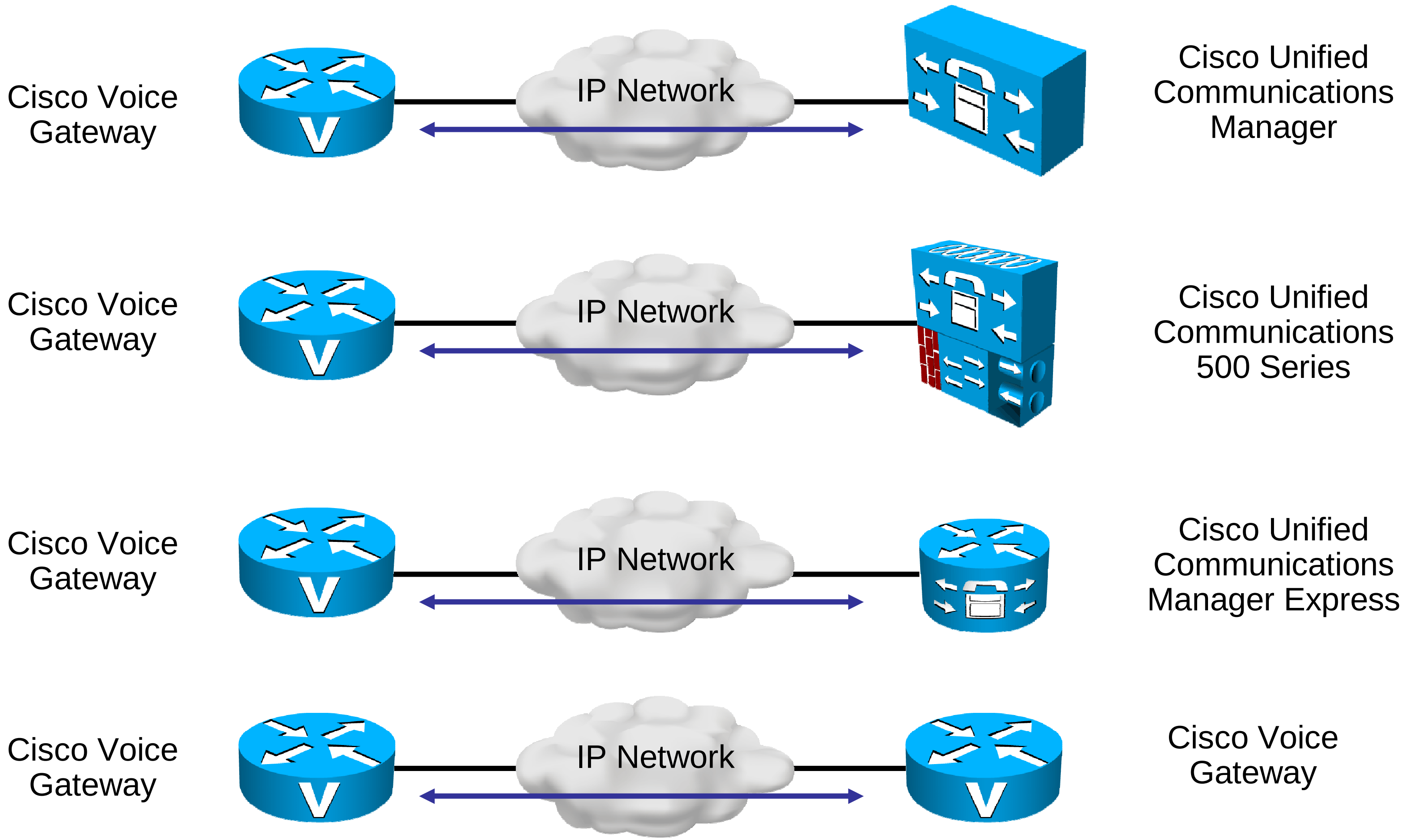
SCCP—Examples



H.323

- H.323 is a suite of protocols for voice, video, and data with the following characteristics:
  - A mature protocol
  - Based on ISDN Q.931
  - Vendor neutral
  - Peer-to-peer architecture
  - Supported on Cisco voice gateways and all Cisco Unified Communications call control platforms
  - Widely deployed
  - ITU standard
  - Encoded into binary messages

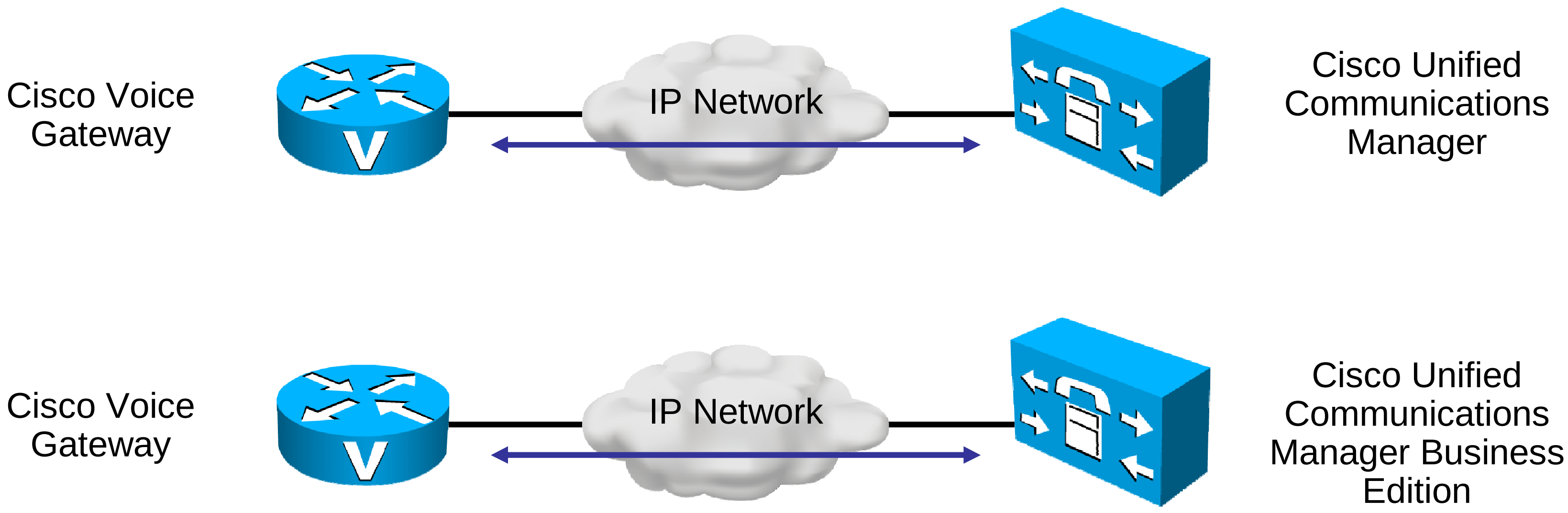
H.323—Examples



Media Gateway Control Protocol

- Is an IETF standard
- Has a client/server architecture
  - Call agent is the Cisco Unified Communications Manager or Cisco Unified Communications Manager Business Edition.
  - The voice gateway is under the control of the call agent.
- Uses plaintext protocol
- Is used on Cisco voice gateways under the control of Cisco Unified Communications Manager or Cisco Unified Communications Manager Business Edition

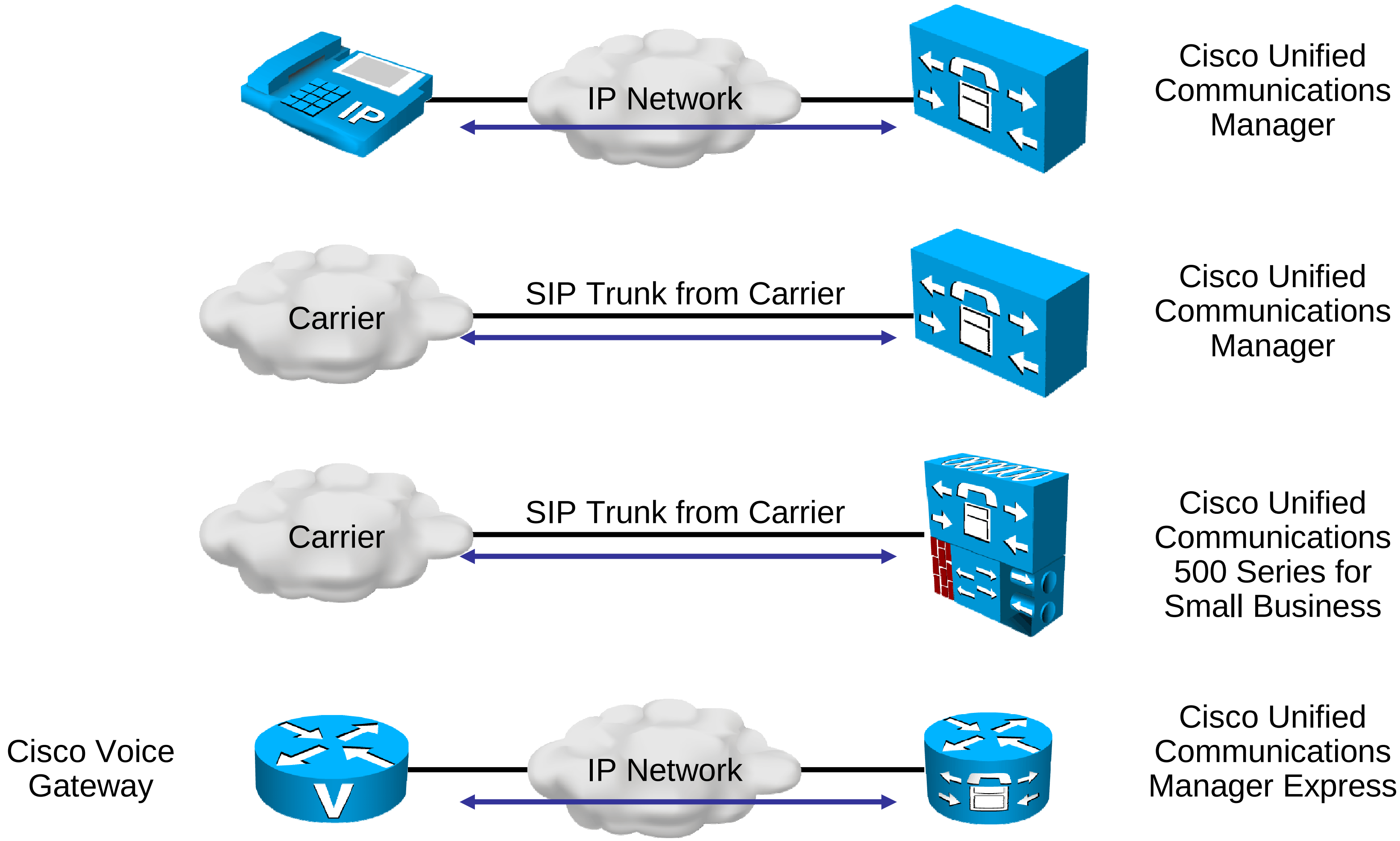
MGCP—Examples



Session Initiation Protocol

- Is an emerging protocol that is still evolving
- Provides basic functionality between different vendors
- Can be used between Cisco Unified Communications call control products and SIP endpoints and SIP trunks
- Is supported on Cisco voice gateways and Cisco Unified IP Phones that have SIP firmware
- Is a peer-to-peer architecture
  - UA initiates the call
  - Phones, gateways, and Cisco call control devices can be UAs
- Is an IETF standard
- Uses ASCII text-based messages

SIP—Examples



OVERVIEW OF PACKET ORIENTED NETWORKS

MOS

The Mean Opinion Score Values

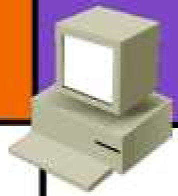
Taken in whole numbers, the numbers are quite easy to grade.

- **5** - Perfect. Like face-to-face conversation or radio reception.
- **4** - Fair. Imperfections can be perceived, but sound still clear. This is (supposedly) the range for cell phones.
- **3** - Annoying.
- **2** - Very annoying. Nearly impossible to communicate.
- **1** - Impossible to communicate

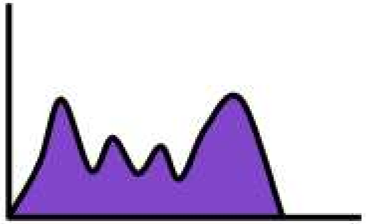
Packet Requirements

Voice

- Smooth
- Benign
- Drop-sensitive
- Delay-sensitive
- UDP priority

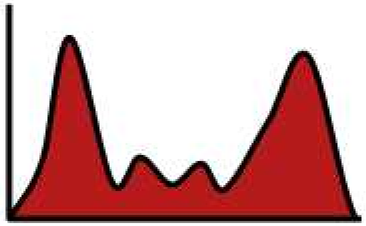


Data



- Smooth or bursty
- Benign or greedy
- Drop-insensitive
- Delay-insensitive
- TCP retransmits

Video



- Bursty
- Greedy
- Drop-sensitive
- Delay-sensitive
- UDP priority

Advantages and Drawbacks of Packet-Oriented Networks

Merging different traffic streams to a single network can lead to a number of service-quality issues:

- Lack of bandwidth: Multiple, simultaneous flows compete for a limited amount of bandwidth.
- Delay issues: End-to-end delay occurs when packets must traverse many network devices and links that add up to the overall delay.
- Jitter: The variability of time that packets need through the network is called "jitter," which occurs as a result of different network load or paths.
- Packet loss: Packets might be dropped when a link is congested.

QoS Recommendations

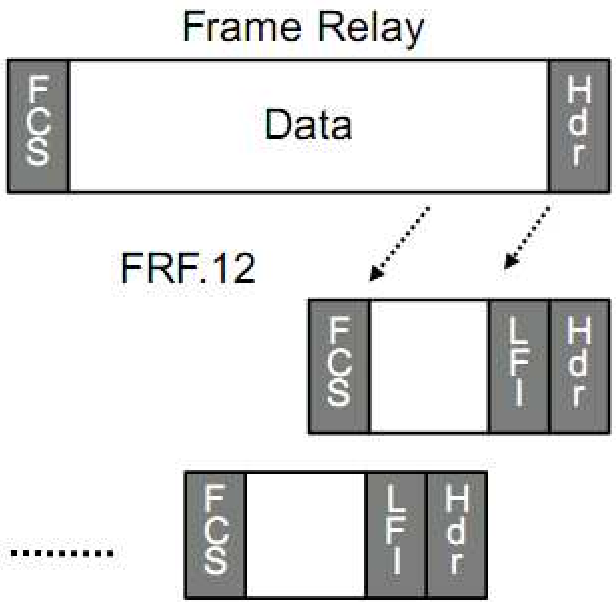
Voice and video traffic has extremely strict QoS requirements:

QoS Issues	Recommendation
Latency	≤ 150 ms
Jitter	≤ 30 ms
Loss	< 1 %

- Bandwidth requirements for voice and video depend on the codec and overhead.
- Video streams need an additional 20 percent bandwidth.

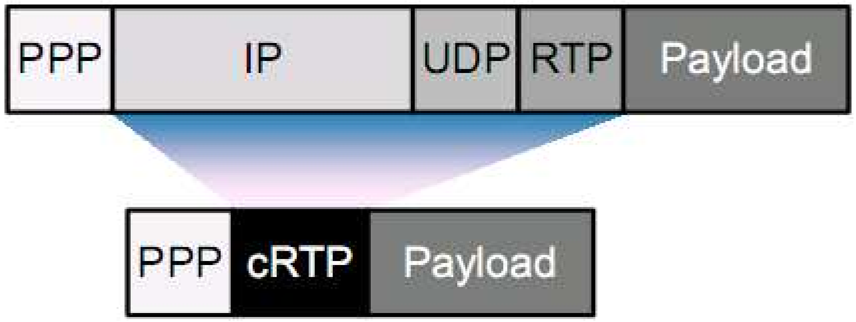
Link Fragmentation and Interleaving

- 1500 bytes need 214 ms to be transmitted on a 56 kb/s link.
- Frames are fragmented into smaller packets.
- Fragmented packets are interleaved to minimize the delay.
- Used for Multilink PPP or Frame Relay.
- Traffic increases due to more frame overhead.



Compression Methods

- Header Compression
  - Used to compress RTP headers for efficient real-time transport of data.
  - Performed on a link-by-link basis.
  - Reduces size of voice packet headers from 40 bytes to 2 or 4 bytes (CRC).
  - G.729 calls over Frame Relay can be reduced from 28 kb/s to 14 kb/s.
- Payload Compression
  - CPU-intensive task that may add per-packet delay.
  - Advantage depends on the complexity of the payload compression algorithm.



Quality of Service Models

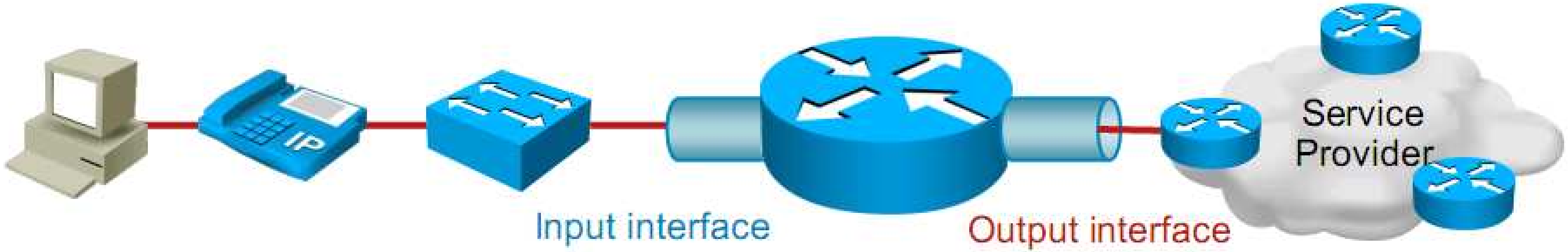
There are three different models for deploying QoS in a network:

- Best-effort model
  - No QoS applied to packets
  - Default model for all traffic
- Integrated Services model (IntServ)
  - Offers absolute QoS guarantees by explicitly reserving bandwidth
  - Uses RSVP to reserve network resources
- Differentiated services model (DiffServ)
  - Allows classification of network traffic
  - QoS policy enforces differentiated treatment of traffic classes
  - Many levels of quality possible
  - Commonly used in enterprise networks

Quality of Service Mechanisms

- Classification: Each class-oriented QoS mechanism must support some type of classification, for example DSCP.
- Marking: Used to mark packets based on classification, metering, or both.
- Congestion management: Each interface must have a queuing mechanism to prioritize transmission of packets.
- Congestion avoidance: Used to drop packets early to avoid congestion later in the network.
- Policing and shaping: Used to enforce a rate limit based on the metering. Excess traffic is either dropped, marked, or delayed.
- Link efficiency: Used to improve bandwidth efficiency through compression, link fragmentation, and interleaving.

Applying Quality of Service to Input and Output Interfaces



	Input interface	Output interface	
(Always)	Classification	Congestion Management	(Always)
(As close to the source as possible)	Marking	Marking	
		Congestion Avoidance	(High-speed to low-speed links or aggregation points)
		Shaping	(Going to lower-speed links or from points of aggregation)
(Coming from a higher-speed link or aggregation)	Policing	Policing	
		Compression	
		Fragmentation and interleaving	(Low-speed WAN links)

Queuing Algorithms

- FIFO
  - First packet in is first packet out; only one queue
- Priority queuing (PQ)
  - Empty queue 1; if queue 1 is empty, then dispatch packets from queue 2, and so on
- Weighted fair queuing (WFQ)
  - Flow-based algorithm that simultaneously schedules interactive traffic to the front of a queue
- Class-based weighted fair queuing (CBWFQ)
  - Extends WFQ functionality to provide support for user-defined traffic classes
- Low-latency queuing (LLQ)
  - Brings strict PQ to CBWFQ; allows delay-sensitive data like voice to be dequeued and transmitted before packets in other queues are dequeued

FACTOR AFFECTING VOICE

VoIP Service Considerations

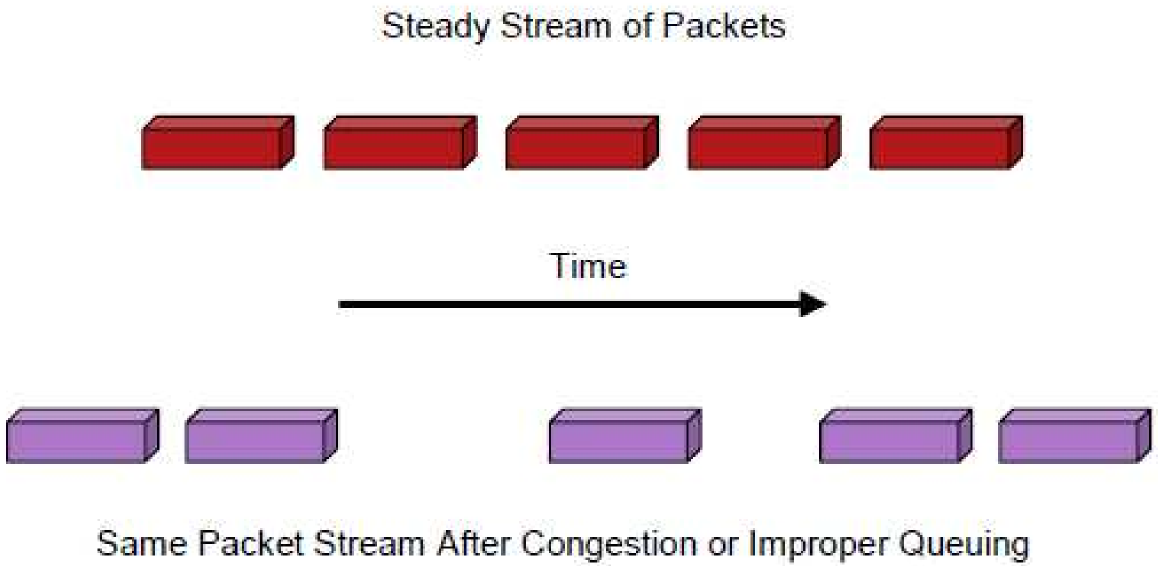
- Latency
- Jitter
- Bandwidth
- Packet loss
- Reliability
- Security

Issue	Solution
Latency	■ Increase bandwidth ■ Choose a different codec type ■ Fragment data packets ■ Prioritize voice packets
Jitter	■ Use dejitter buffers
Bandwidth	■ Calculate bandwidth requirements, including voice payload, overhead, and data
Packet loss	■ Design the network to minimize congestion ■ Prioritize voice packets ■ Use codecs to minimize small amounts of packet loss
Reliability	■ Provide redundancy for these components: — Hardware — Links — Power (uninterruptible power supply [UPS]) ■ Perform proactive network management
Security	■ Secure these components: — Network infrastructure — Call-processing systems

Factors Affecting Audio Clarity

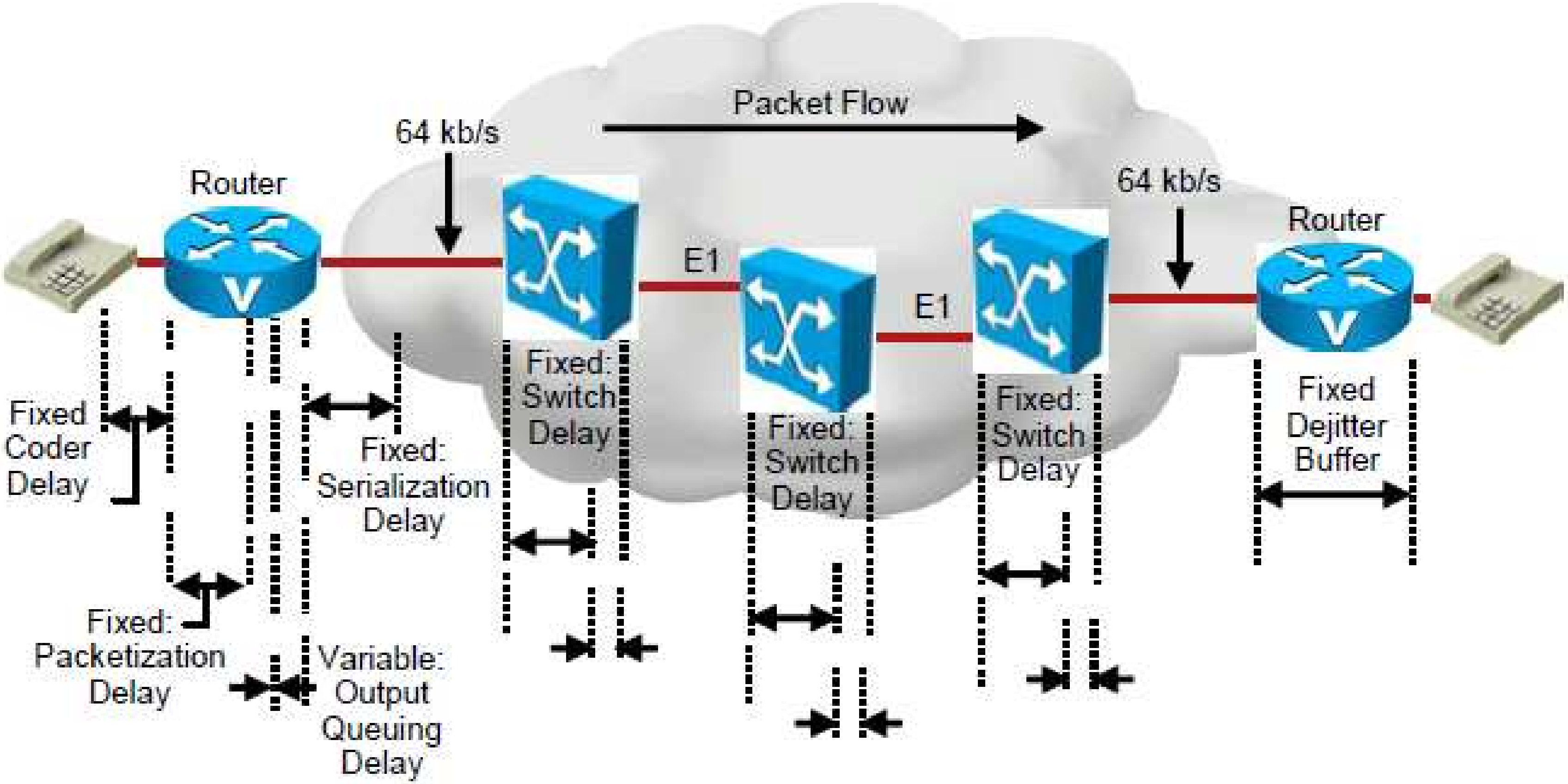
- Fidelity: Audio accuracy or quality
- Echo: Usually due to impedance mismatch
- Jitter: Variation in the arrival of voice packets
- Delay: Time it takes for the signal to propagate from one end to the other end of the conversation
- Packet loss: Loss of packets on the network
- Side tone: Allows speakers to hear their own voice
- Background noise: Low-volume noise heard at the far end of the conversation

Jitter in IP Networks

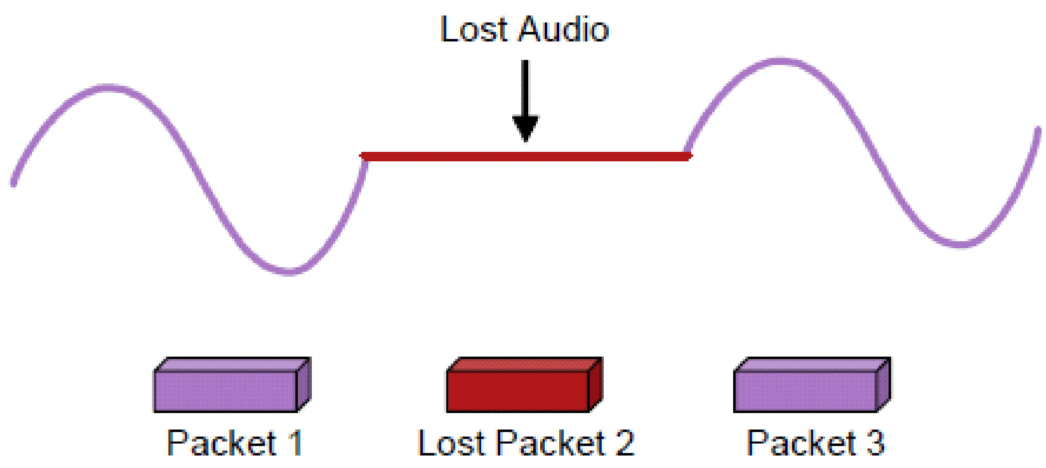


When a conversation is subjected to jitter, the results can be clearly heard. If the talker says, "Watson, come here. I want you," the listener might hear, "Wat….s…on…….come here, I……wa……nt……..y……ou." The variable arrival of the packets at the receiving end causes the speech to be delayed and garbled.

Sources of Delay



Effect of Packet Loss



If a conversation experiences packet loss, the effect is immediately heard. If the talker says, "Watson, come here. I want you," the listener might hear, "Wat----, come here, ------you."

MEDIA TRANSPORT PROTOCOLS

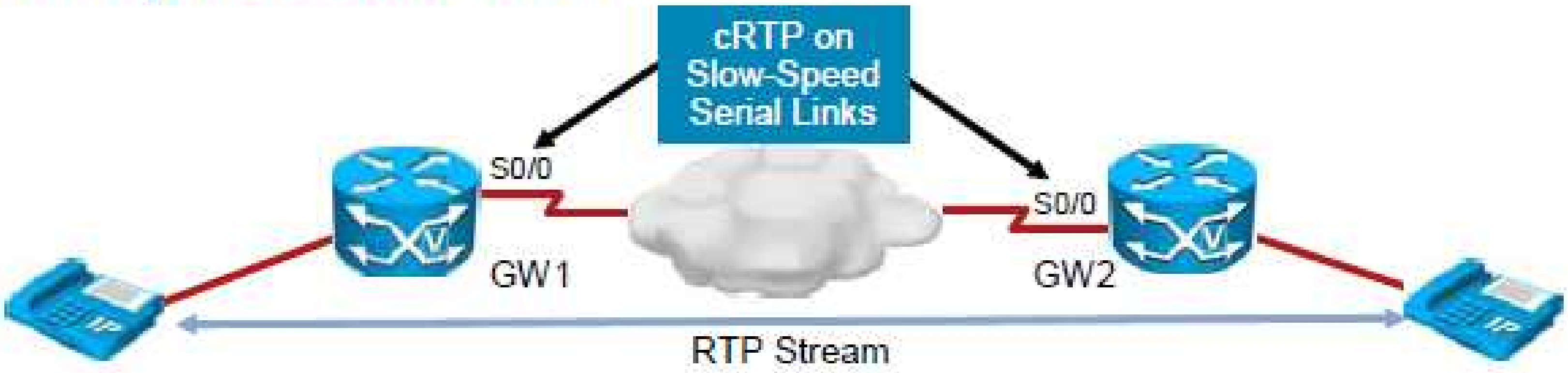
Media Transmission Protocols

- Real-Time Transport Protocol: Delivers the actual audio and video streams over networks
- Real-Time Transport Control Protocol: Provides out-of-band control information for an RTP flow
- cRTP: Compresses IP/UDP/RTP headers on low-speed serial links
- SRTP Provides encryption, message authentication and integrity, and replay protection to the RTP data

Real-Time Transport Control Protocol

- Define in RFCs 1889, 3550
- Provides out-of-band control information for a RTP flow
- Used for QoS reporting
- Monitors the quality of the data distribution and provides control information
- Provides feedback on current network conditions
- Allows hosts involved in an RTP session to exchange information about monitoring and controlling the session
- Provides a separate flow from RTP for UDP transport use

Compressed RTP



- RFCs
  - RFC 2508, *Compressing IP/UDP/RTP Headers for Low-Speed Serial Links*
  - RFC 2509, *IP Header Compression over PPP*
- Enhanced CRTP
  - RFC 3545, *Enhanced Compressed RTP (CRTP) for Links with High Delay, Packet Loss and Reordering*
- Compresses 40-byte header to approximately 2 to 4 bytes

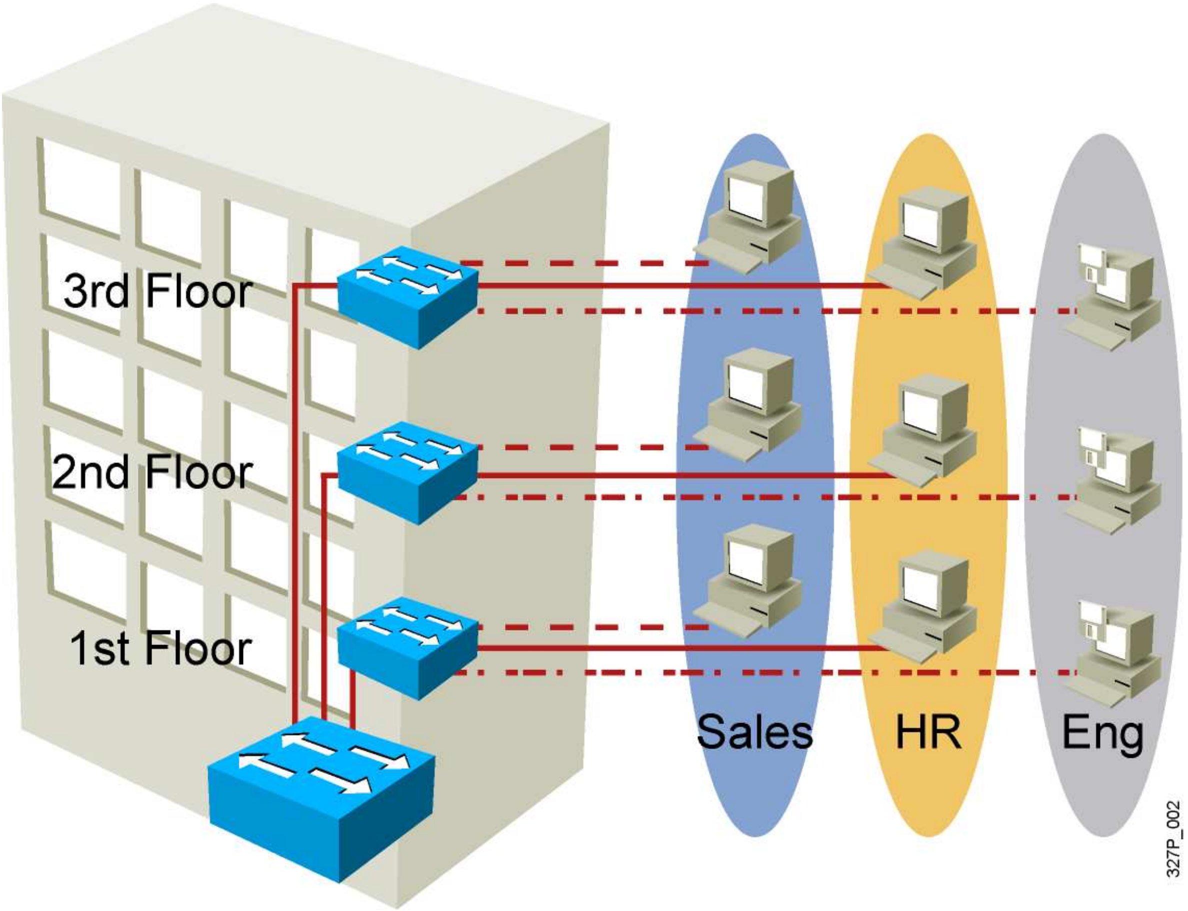
Secure RTP

- RFC 3711
- Provides:
  - Encryption
  - Message authentication and integrity
  - Replay protection

IMPLEMENTING VLANS

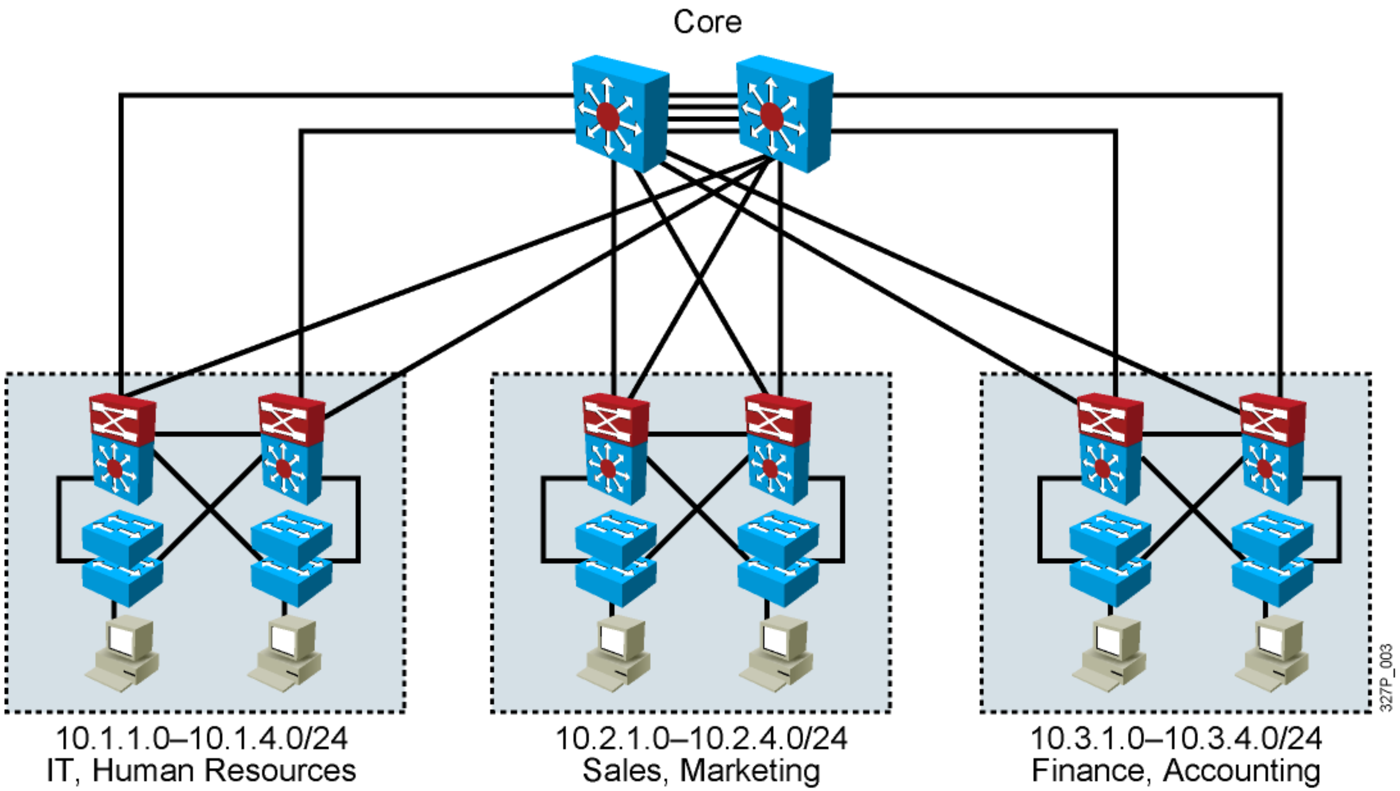
VLAN Overview

- Segmentation
- Flexibility
- Security



VLAN = Broadcast Domain = Logical Network (Subnet)

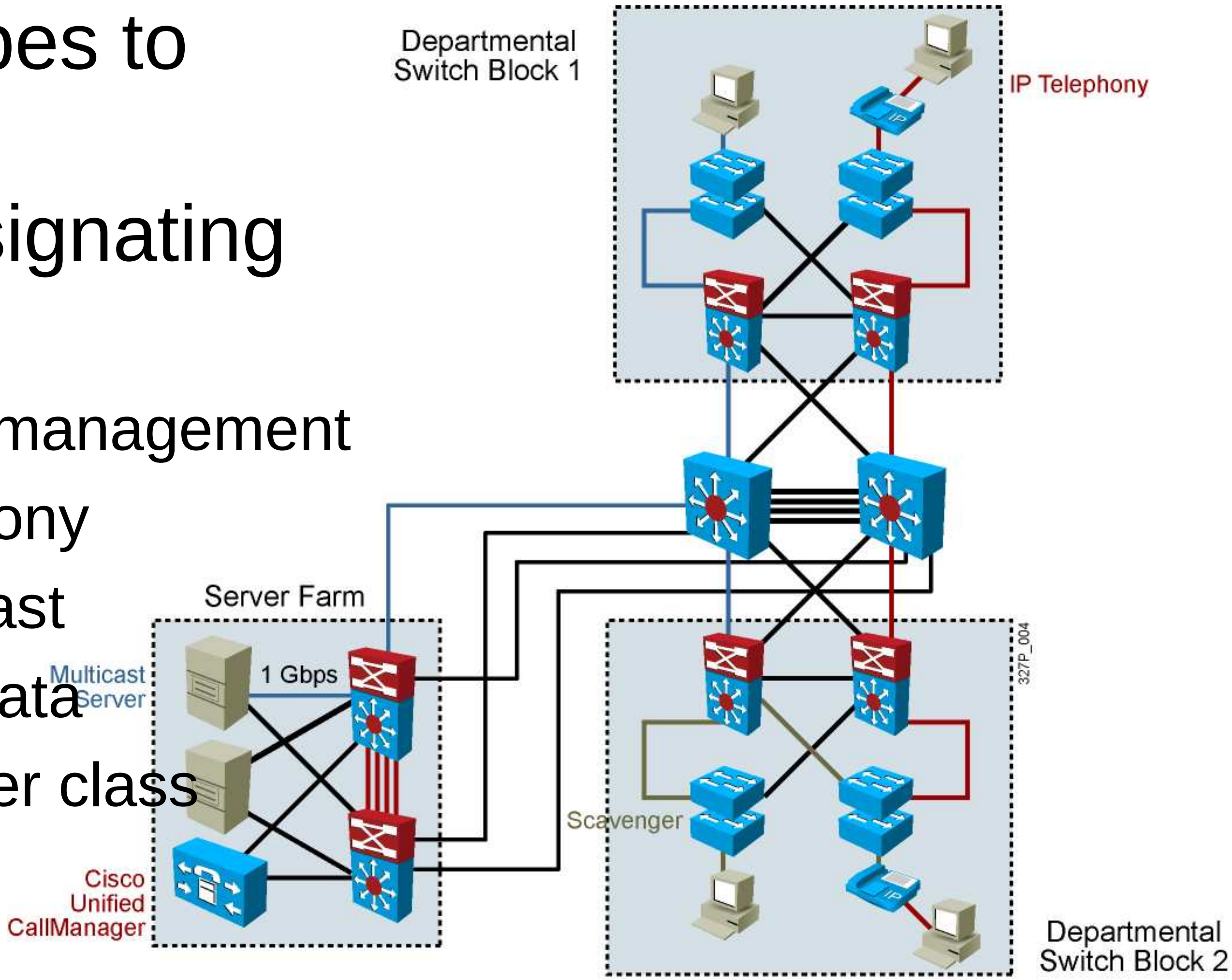
Guidelines for Applying IP Address Space



- Allocate one IP subnet per VLAN.
- Allocate IP address spaces in contiguous blocks.

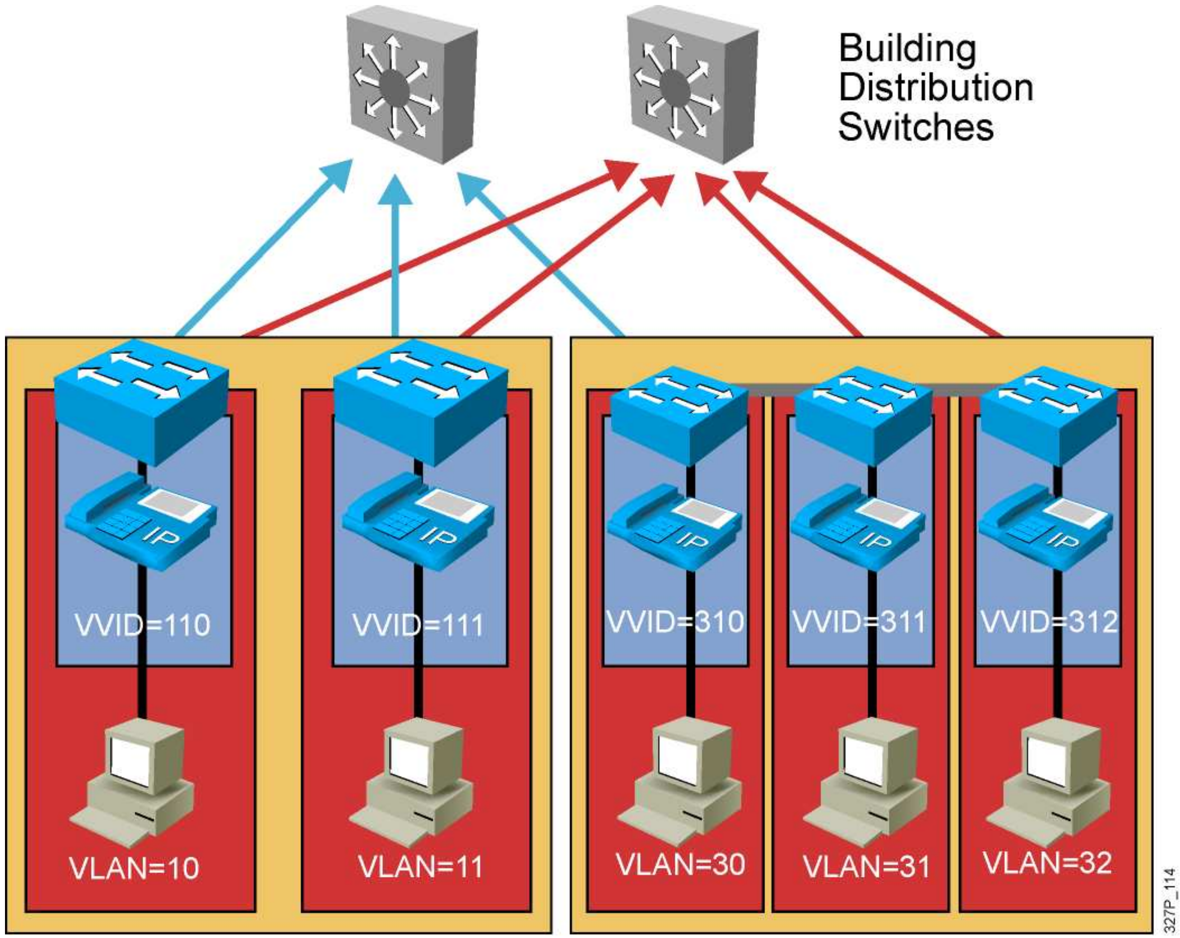
Network Traffic Types

- Traffic types to consider when designating VLANs:
  – Network management
  – IP telephony
  – IP Multicast
  – Normal data
  – Scavenger class

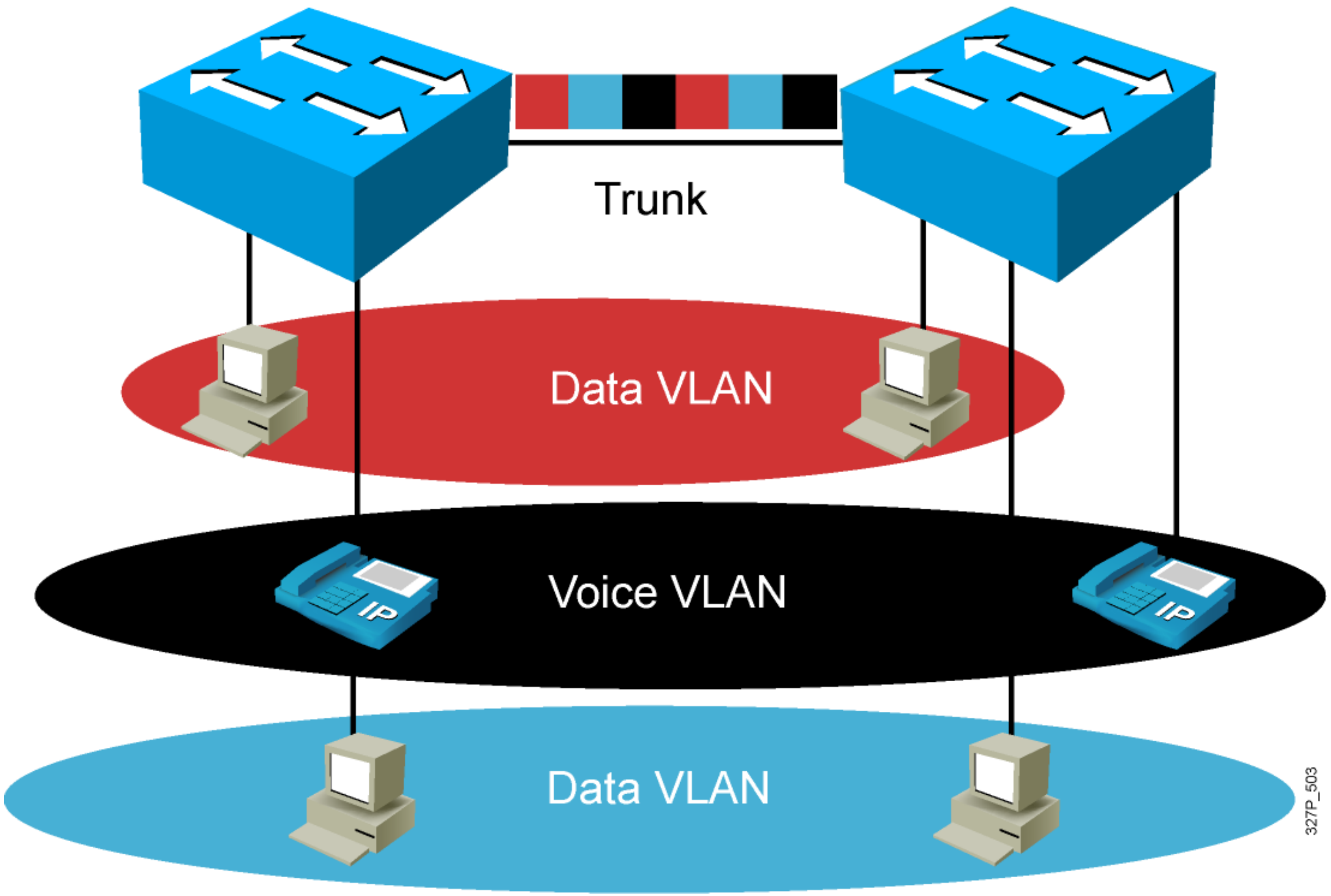


Advantages of Voice VLANs

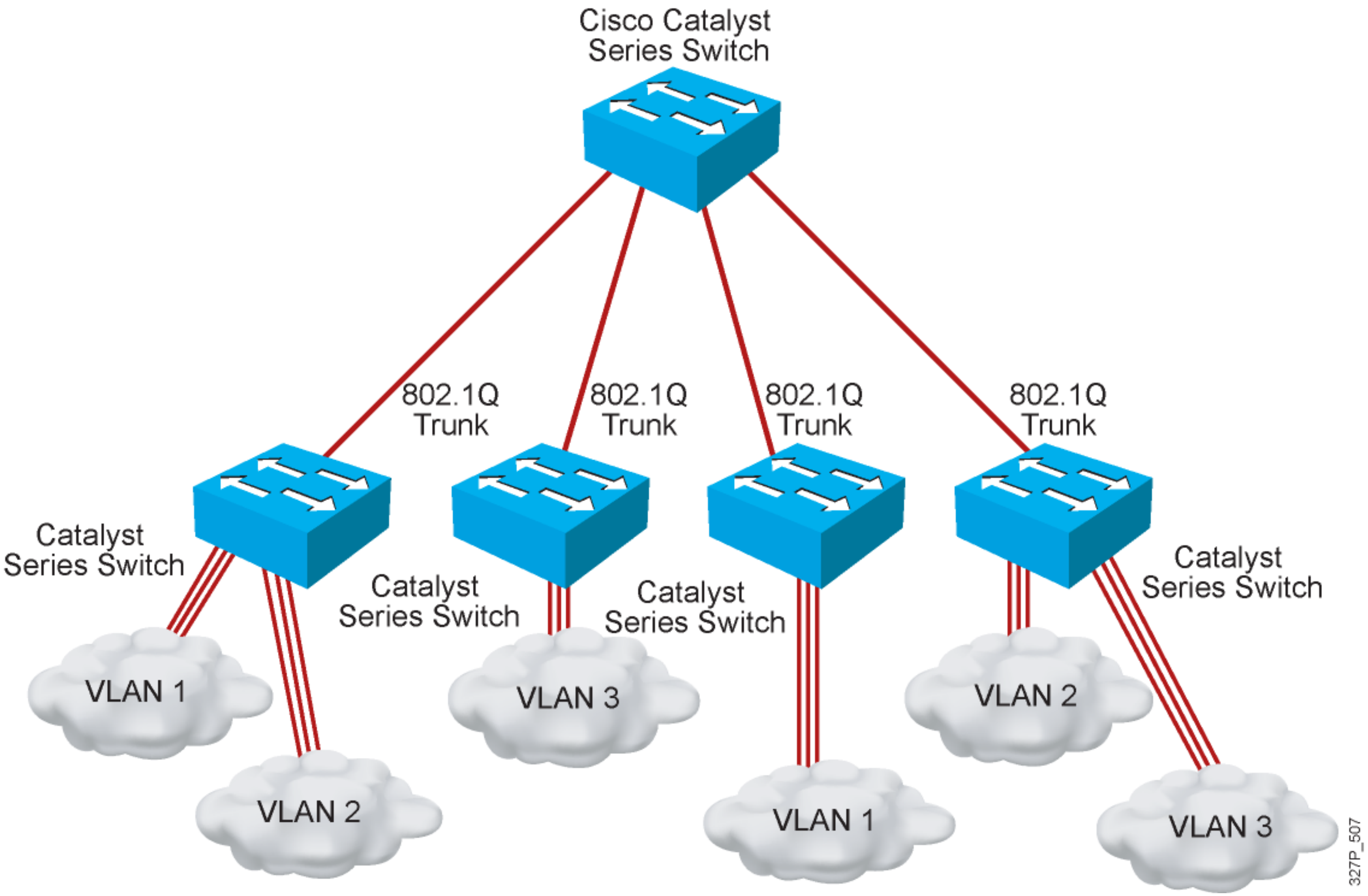
- Phones segmented in separate logical networks
- Provides network segmentation and control
- Allows administrators to create and enforce QoS
- Lets administrators add and enforce security policies



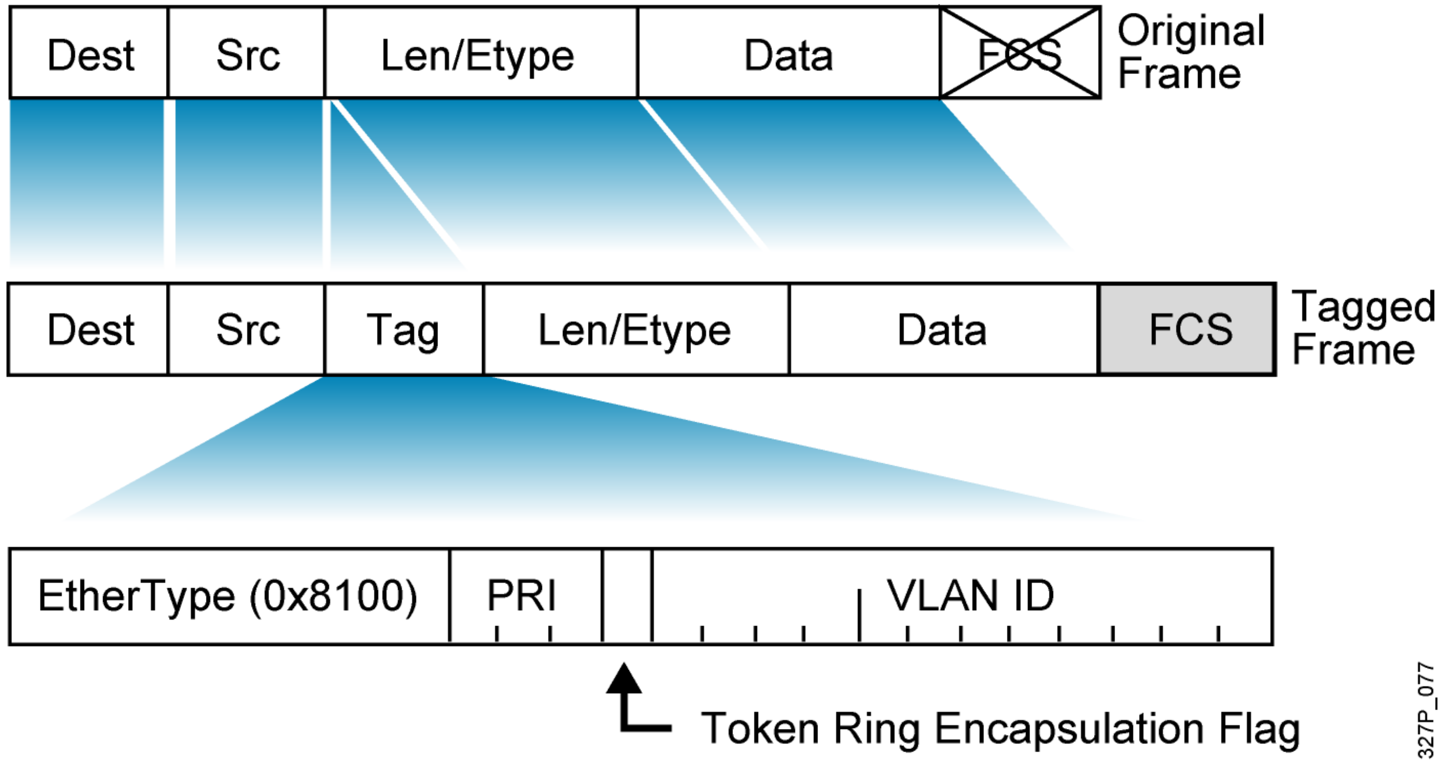
VLAN Operation



802.1Q Trunking

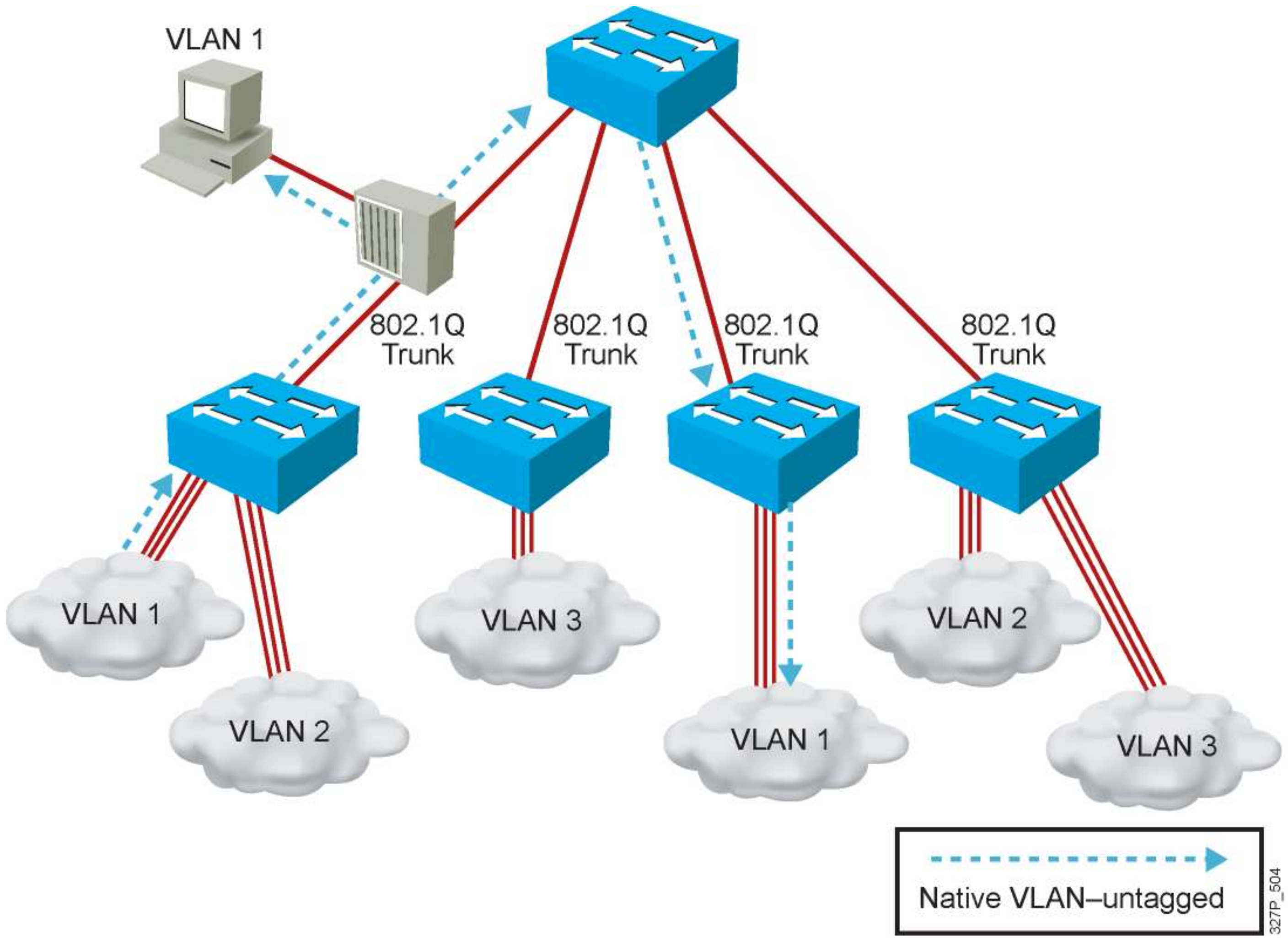


802.1Q Frame

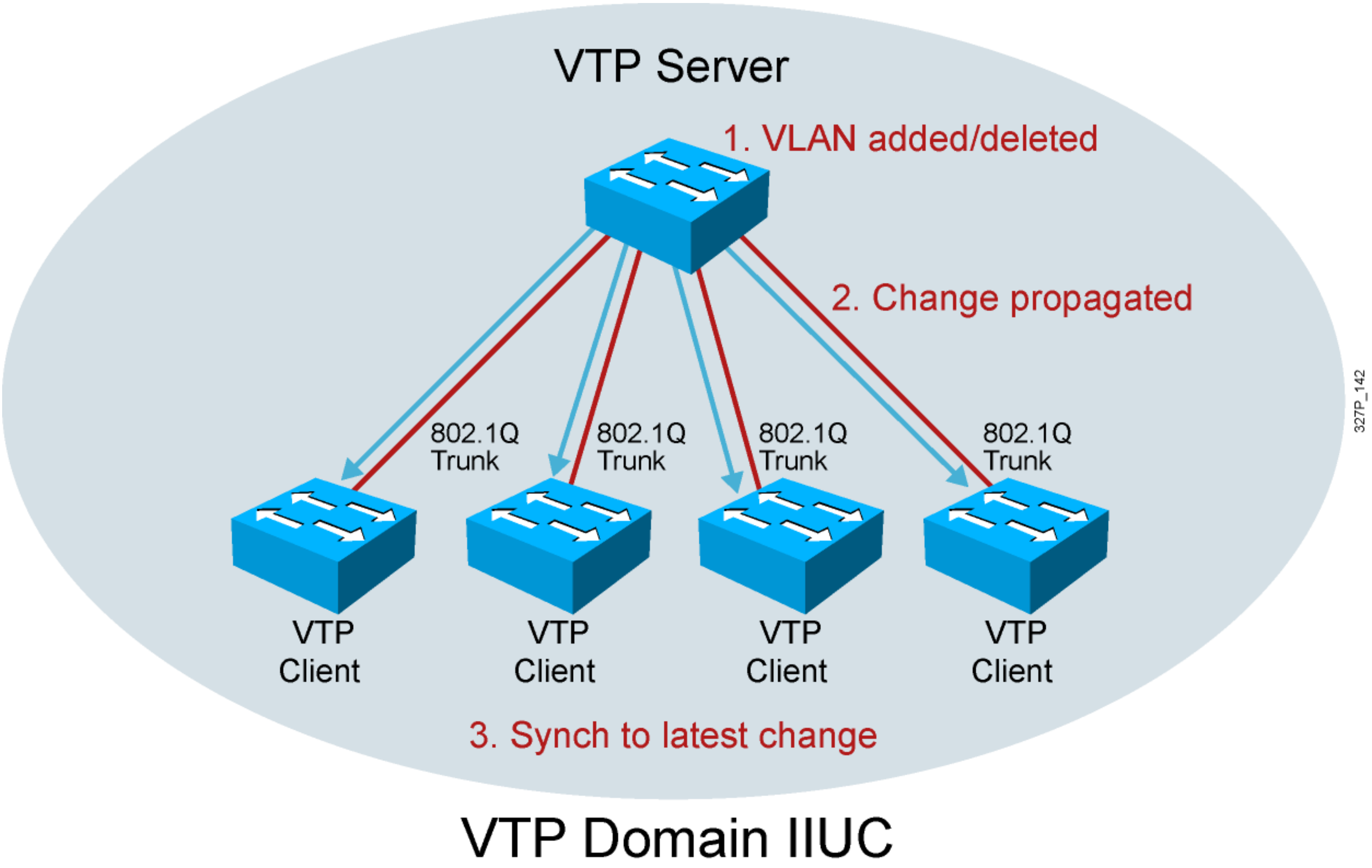


Dest
Src
Len/Etype
Data
FCS
Original Frame
Dest
Src
Tag
Len/Etype
Data
FCS
Tagged Frame
EtherType (0x8100)
PRI
VLAN ID
Token Ring Encapsulation Flag
327P_077

Understanding Native VLANs

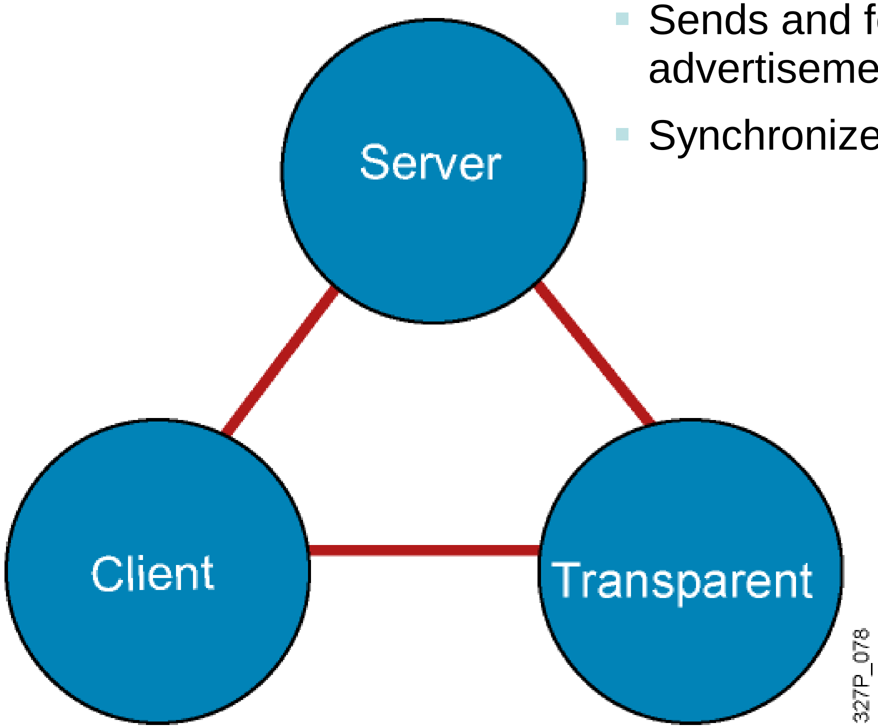


VTP Features



VTP Modes

- Create VLANs
- Modify VLANs
- Delete VLANs
- Sends and forwards advertisements
- Synchronizes



- Cannot create, change, or delete VLANs
- Sends and forwards advertisements
- Synchronizes

- Create local VLANs only
- Modify local VLANs only
- Delete local VLANs only
- Forwards advertisements
- Does not synchronize

Creating a VTP Domain

```
SwitchX# configure terminal
SwitchX(config)# vtp mode [ server | client | transparent ]
SwitchX(config)# vtp domain domain-name
SwitchX(config)# vtp password password
SwitchX(config)# end
```

VTP Configuration and Verification Example

```
SwitchX(config)# vtp domain IIUC
Changing VTP domain name to IIUC
SwitchX(config)# vtp mode transparent
Setting device to VTP TRANSPARENT mode.
SwitchX(config)# end

SwitchX# show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 64
Number of existing VLANs        : 17
VTP Operating Mode              : Transparent
VTP Domain Name                 : IIUC
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x7D 0x6E 0x5E 0x3D 0xAF 0xA0 0x2F 0xAA
Configuration last modified by 10.1.1.4 at 3-3-93 20:08:05
SwitchX#
```

Configuring 802.1Q Trunking

SwitchX(config-if)#

```
switchport mode {access |  dynamic {auto | desirable} | trunk}
```

- Configures the trunking characteristics of the port

SwitchX(config-if)#

```
switchport mode trunk
```

- Configures the port as a VLAN trunk

Verifying a Trunk

```
SwitchX# show interfaces interface [switchport | trunk]
```

```
SwitchX# show interfaces fa0/11 switchport
Name: Fa0/11
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
 . . .
```

```
SwitchX# show interfaces fa0/11 trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/11      desirable    802.1q         trunking      1

Port      Vlans allowed on trunk
Fa0/11      1-4094

Port        Vlans allowed and active in management domain
Fa0/11      1-13
```

Adding a VLAN

```
SwitchX# configure terminal
SwitchX(config)# vlan 2
SwitchX(config-vlan)# name switchlab99
```

Assigning Switch Ports to a VLAN

SwitchX(config-if)#

```
switchport access [vlan vlan# | dynamic]
```

```
SwitchX# configure terminal
SwitchX(config)# interface range fastethernet 0/2 - 4
SwitchX(config-if)# switchport access vlan 2

SwitchX# show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- ---------------------
1    default                           active    Fa0/1
2    switchlab99                       active    Fa0/2, Fa0/3, Fa0/4
```

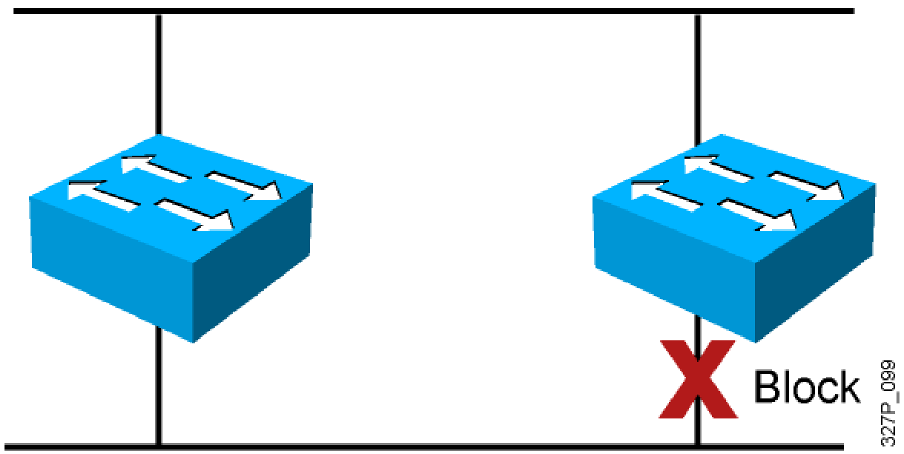
Verifying VLAN Membership (Cont.)

SwitchX(config-if)#

```
show interfaces interface switchport
```

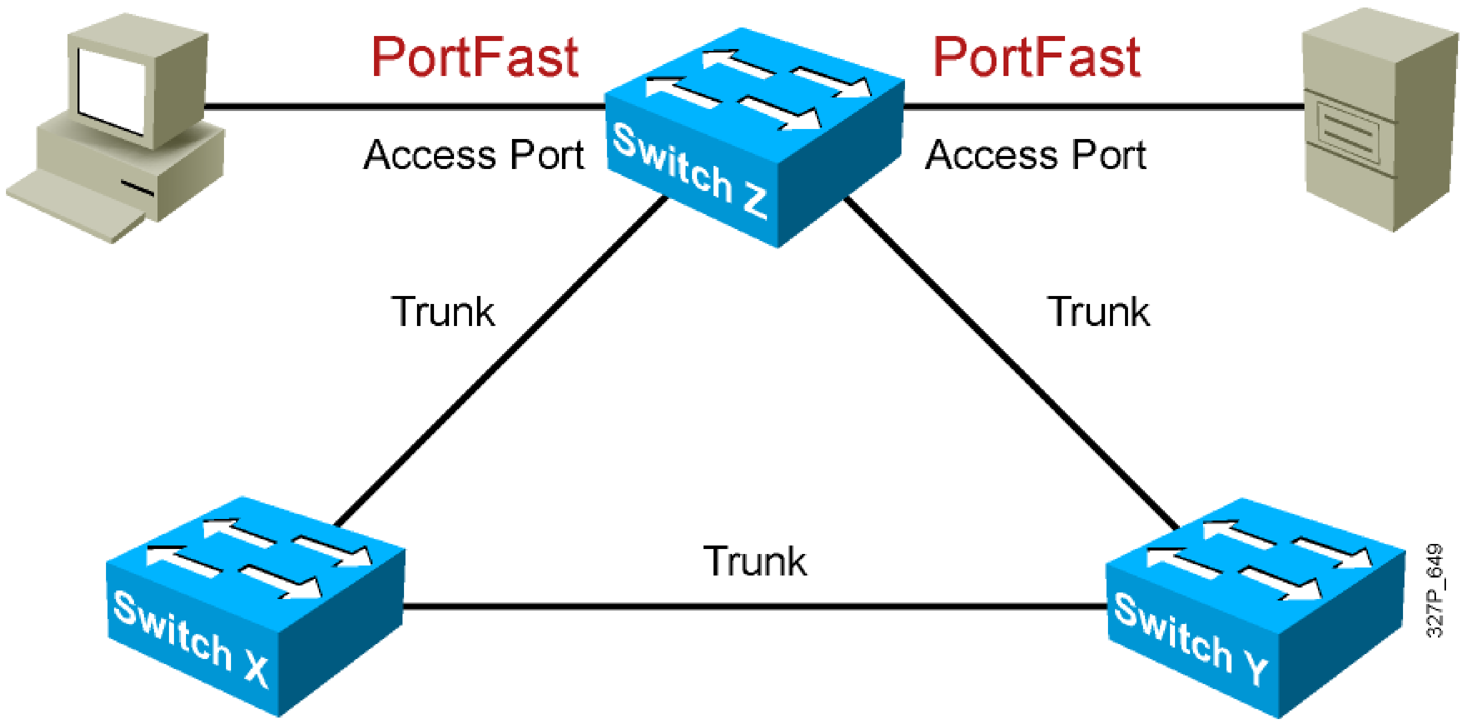
```
SwitchX# show interfaces fa0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 2 (switchlab99)
Trunking Native Mode VLAN: 1 (default)
--- output omitted ----
```

Loop Resolution with STP



- Provides a loop-free redundant network topology by placing certain ports in the blocking state
- Published in the IEEE 802.1D specification
- Enhanced with the Cisco PVST+ implementation

Describing PortFast



- PortFast is configured on access ports, not trunk ports.

Configuring and Verifying PortFast

SwitchX(config-if)#

```
spanning-tree portfast
```

- Configures PortFast on an interface

OR

SwitchX(config)#

```
spanning-tree portfast default
```

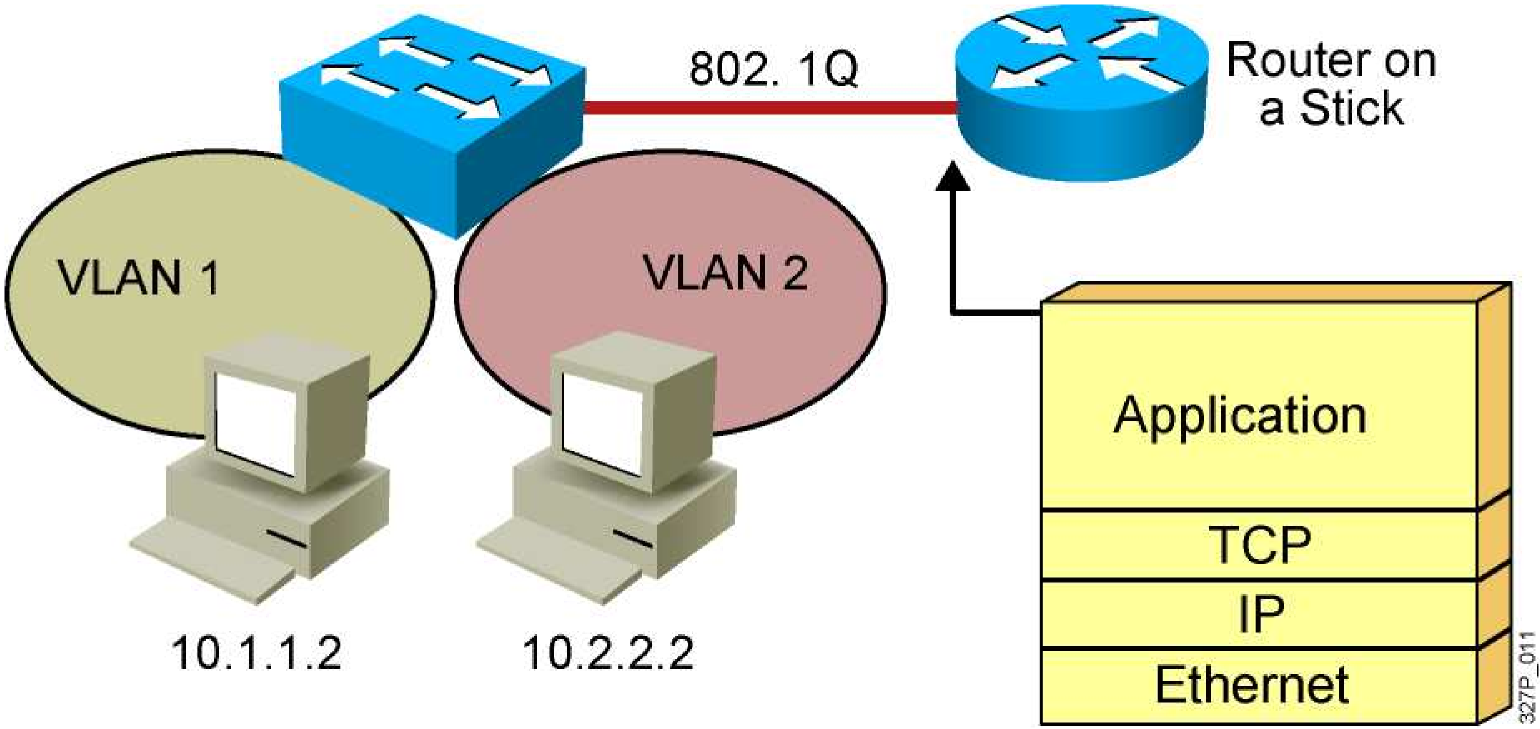
- Enables PortFast on all nontrunking interfaces

SwitchX#

show running-config interface ***interface***

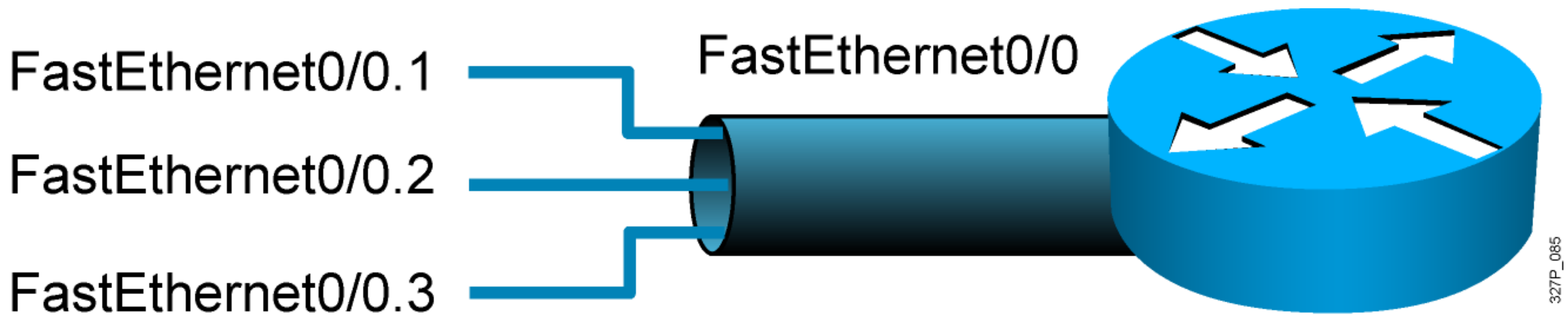
- Verifies that PortFast has been configured on an interface

VLAN-to-VLAN Overview



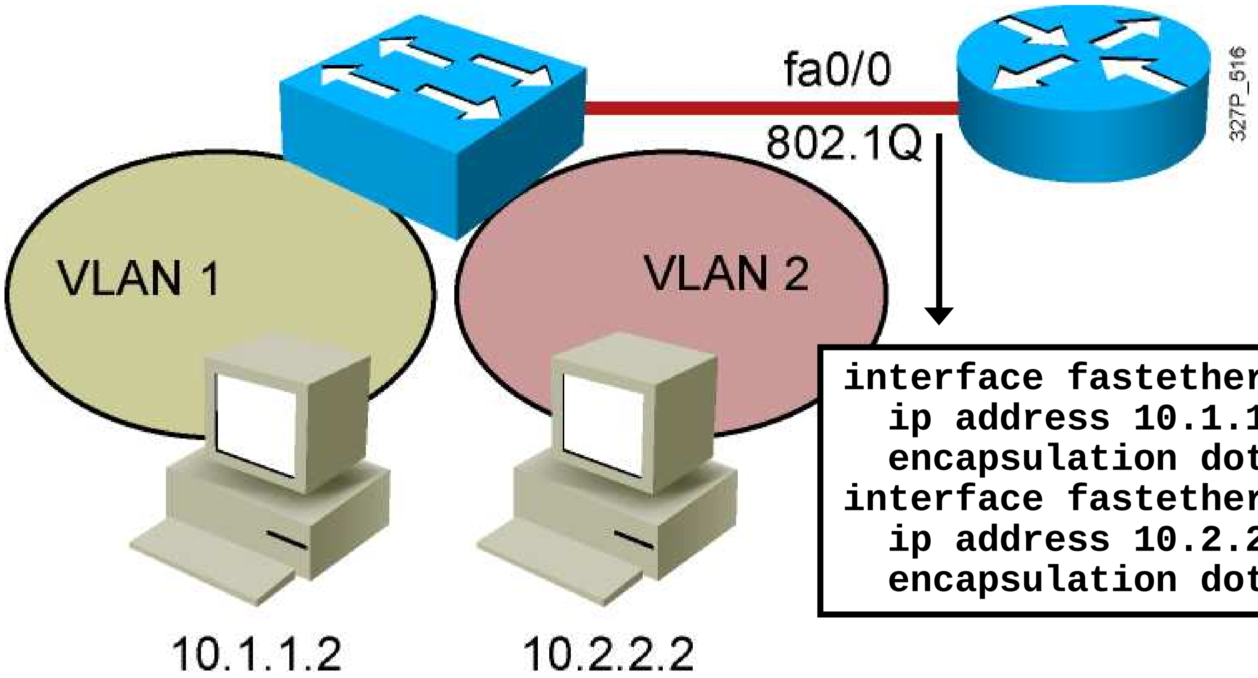
- Network layer devices combine multiple broadcast domains.

Dividing a Physical Interface into Subinterfaces



- Physical interfaces can be divided into multiple subinterfaces.

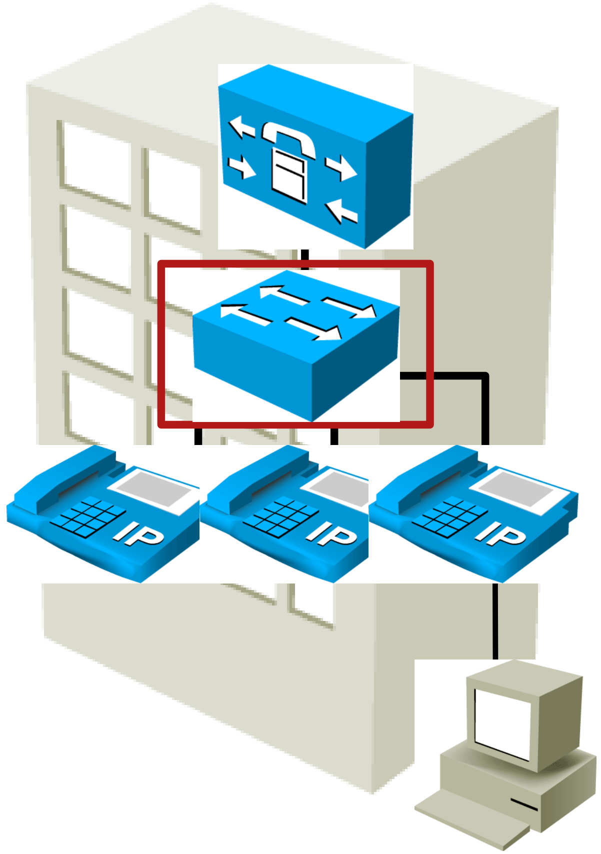
Routing Between VLANs with 802.1Q Trunks




```
interface fastethernet 0/0
  ip address 10.1.1.1 255.255.255.0
  encapsulation dot1q 1 native
interface fastethernet 0/0.2
  ip address 10.2.2.1 255.255.255.0
  encapsulation dot1q 2
```

Cisco Catalyst Switch Role in IP Telephony

- Supplies inline power to IP phones
- Supports voice and data VLANs on a single access port
- Prioritizes voice traffic with CoS or DSCP marking



Applying Switch Features

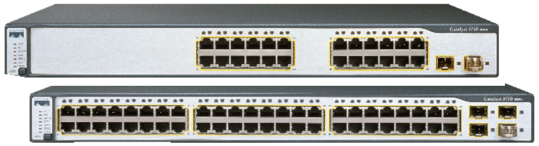
Switch Features	When to Use	How to Use
PoE	When you require the reliability, availability and flexibility of PoE	Identify the PoE type required. PoE is enabled by default.
Voice VLAN	When you want to connect a PC to an IP phone and have both using a single physical port at the switch but with separate VLANs	Configure voice VLAN in addition to access VLAN.
QoS / CoS	When you want to ensure that voice quality is not affected by network traffic congestion	Identify the trust boundary and the applications. Configure the QoS base for your traffic requirements.

Cisco Catalyst Family of Switches

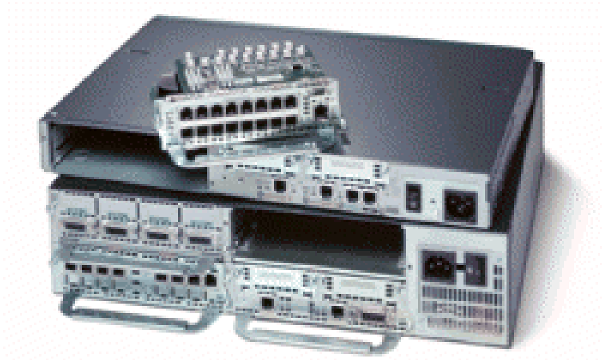
Cisco Catalyst 6500

Cisco Catalyst 4500

Cisco Catalyst 3750



Cisco EtherSwitch Network Module

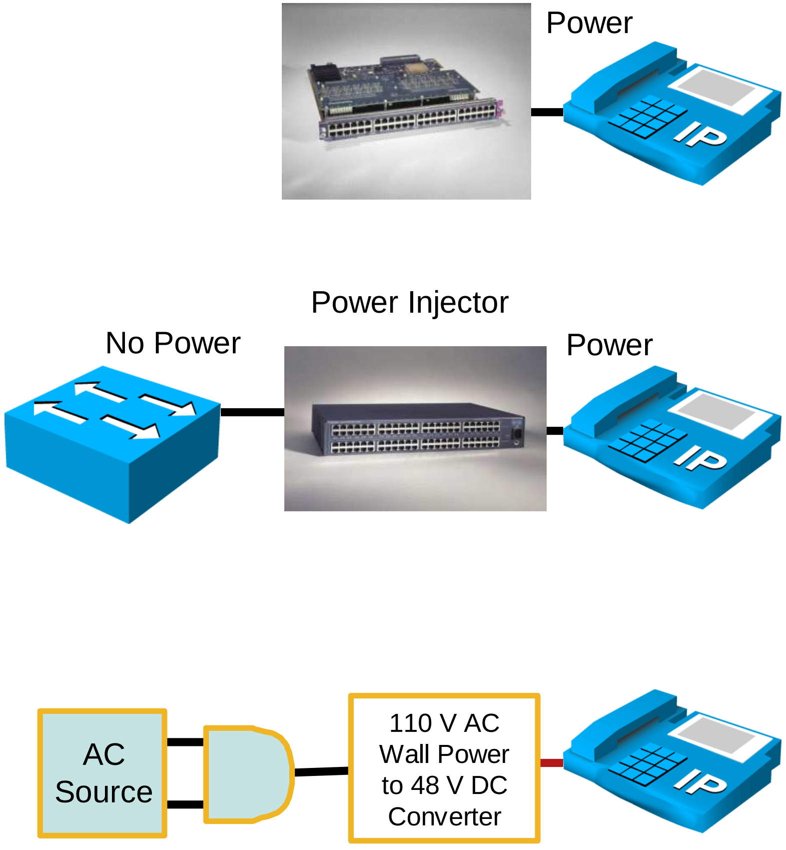


Cisco Catalyst 3560

	Cisco Catalyst 6500	Cisco Catalyst 4500	Cisco Catalyst 3750	Cisco Catalyst 3560	Cisco EtherSwitch Module
PoE Configuration Options	48-, 96-port 10/100 or 48-port 10/100/1000	48-port 10/100 or 10/100/1000	24-, 48-port 10/100	24-, 48-port 10/100	16-, 36-port 10/100
802.3af-Compliant	Yes	Yes	Yes	Yes	No
Cisco Prestandard PoE	Yes	Yes	Yes	Yes	Yes

Three Ways to Power Cisco IP Phones

- Power over Ethernet (PoE):
  - Needs PoE line cards or PoE ports for Cisco Catalyst switches
  - Delivers 48V DC over data pairs (pins 1, 2, 3, and 6) or spare pairs (pins 4, 5, 7, 8)
- Midspan power injection:
  - Needs external power source equipment
  - Delivers 48V DC over spare pairs
- Wall power:
  - Needs DC converter to connect a Cisco IP phone to a wall outlet



Two Types of PoE Delivery

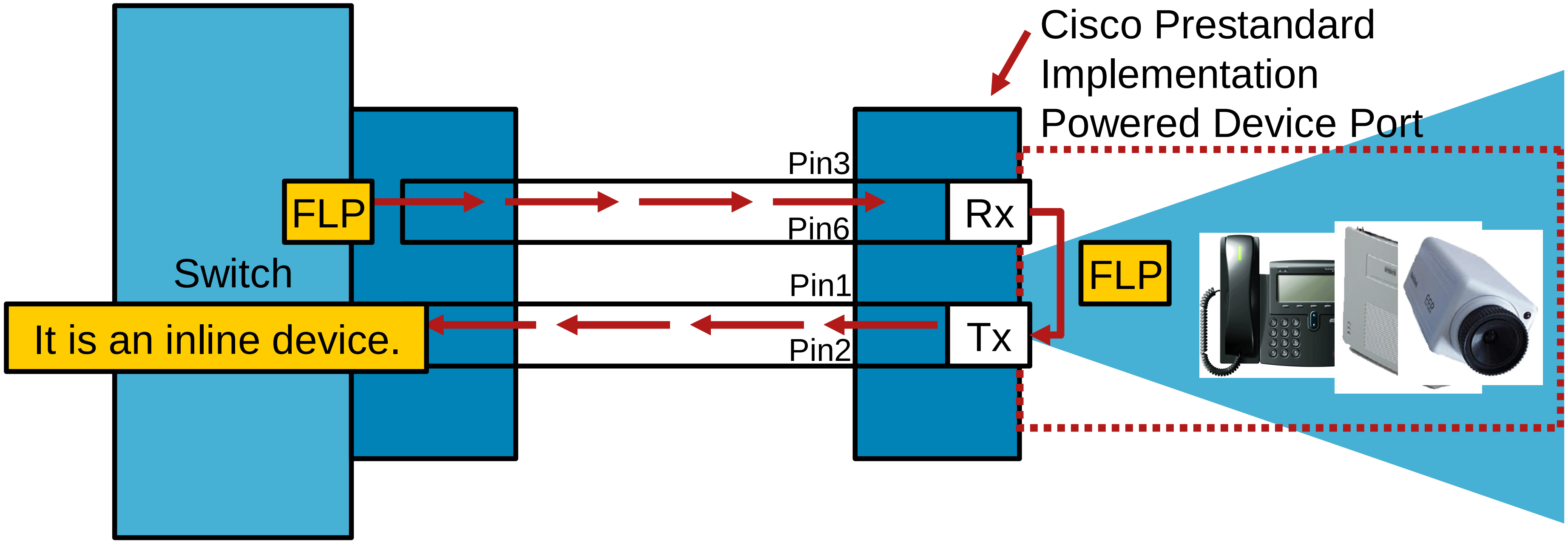
Cisco original implementation:

- Provides -48V DC at up to 6.3 to 7.7 W per port over data pins 1, 2, 3, and 6.
- Supports most Cisco devices (Cisco IP phones and wireless access points).
- Uses a Cisco proprietary method of determining if an attached device requires power. Power is delivered only to devices that require power.

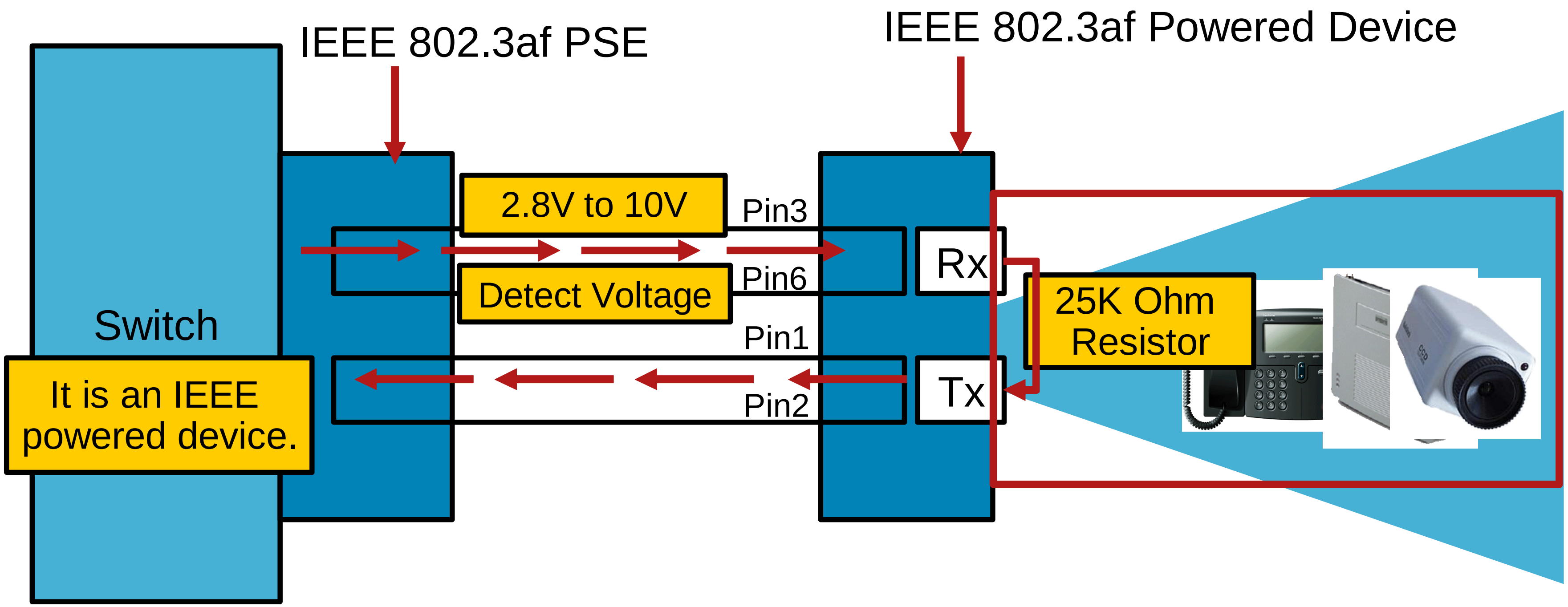
IEEE 802.3af Power over Ethernet:

- Specifies 48V DC at up to 15.4W per port over data pins 1, 2, 3, and 6 or spare pins 4, 5, 7, and 8.
- Enables a new range of Ethernet-powered devices because of increased power.
- Standardizes the method of determining if an attached device requires power. Power is delivered only to devices that require power.
- Has several optional elements, including power classification.

Cisco Prestandard Device Detection



IEEE 802.3af Device Detection



Cisco Catalyst Switch: Configuring PoE

Cisco Catalyst Operating System:

```
CatOS>(enable) set port inlinepower <mod/port> ?
         auto     Port inline power auto mode
         off      Port inline power off mode
```

Native Cisco IOS Software:

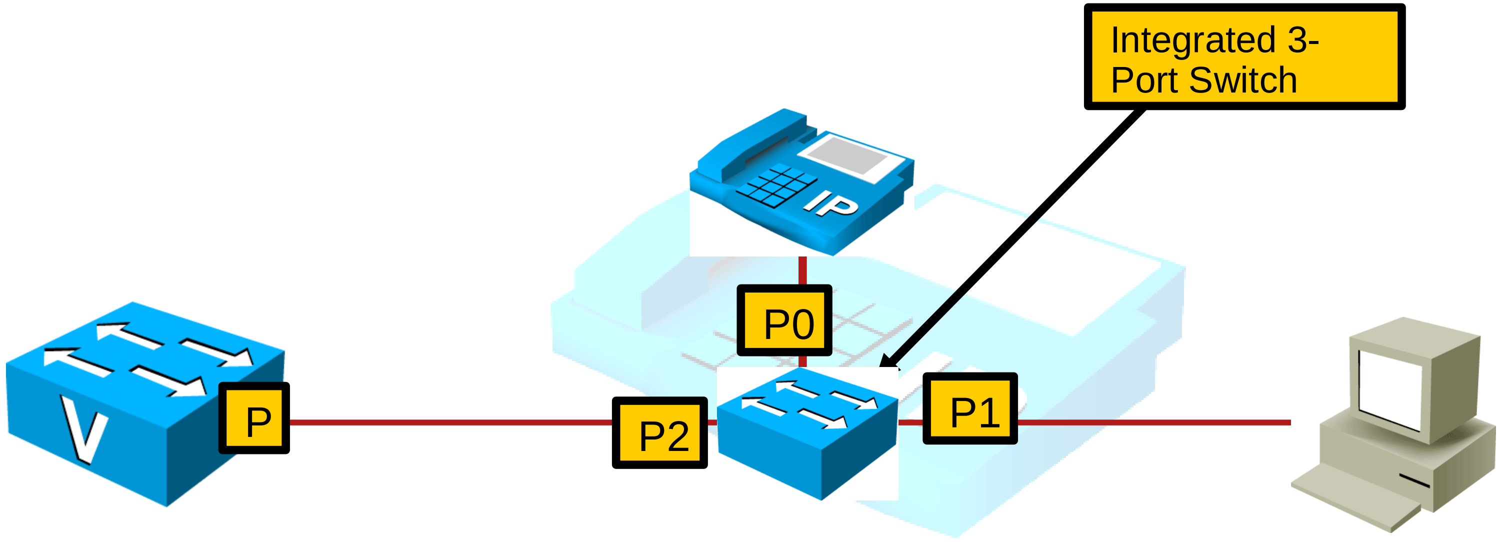
```
CSCOIOS(config-if)#  power inline <auto/never>
```

Cisco Catalyst Switch: Show Inline Power Status

```
show port inline power 7
Default Inline Power allocation per port: 10.000 Watts (0.23 Amps @42V)
Total inline power drawn by module 7: 75.60 Watts (1.80 Amps @42V)
Port     InlinePowered     PowerAllocated
         Admin    Oper     Detected         mWatt            mA @42V
----     -----    ----     --------         ---------        -----------
7/1      auto     off      no               0                0
7/2      auto     on       yes              6300             150
7/3      auto     on       yes              6300             150
7/4      auto     off      no               0                0
7/5      auto     off      no               0                0
7/6      auto     off      no               0                0
7/7      auto     off      no               0                0
```

```
show power inline
Interface         Admin    Oper     Power ( mWatt )   Device
----------        -----    ----     ---------------   ------
FastEthernet9/1   auto     on       6300              Cisco 6500 IP Phone
FastEthernet9/2   auto     on       6300              Cisco 6500 IP Phone
FastEthernet9/3   auto     off      0                 n/a
```

Cisco IP Phone Connected to the Network

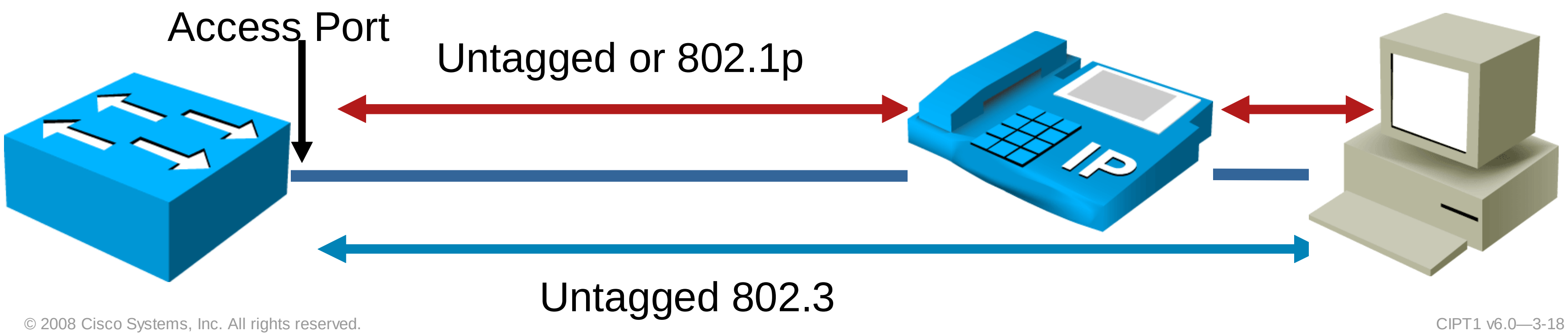


Voice VLAN Support

- A Cisco Catalyst switch can be configured to support voice traffic in various ways:
  - Single VLAN access port
  - Multi-VLAN access port
  - Trunk port
- Considerations:
  - Security
  - Cisco IP phones/non-Cisco IP phones/IP softphones
  - Spanning tree
  - QoS

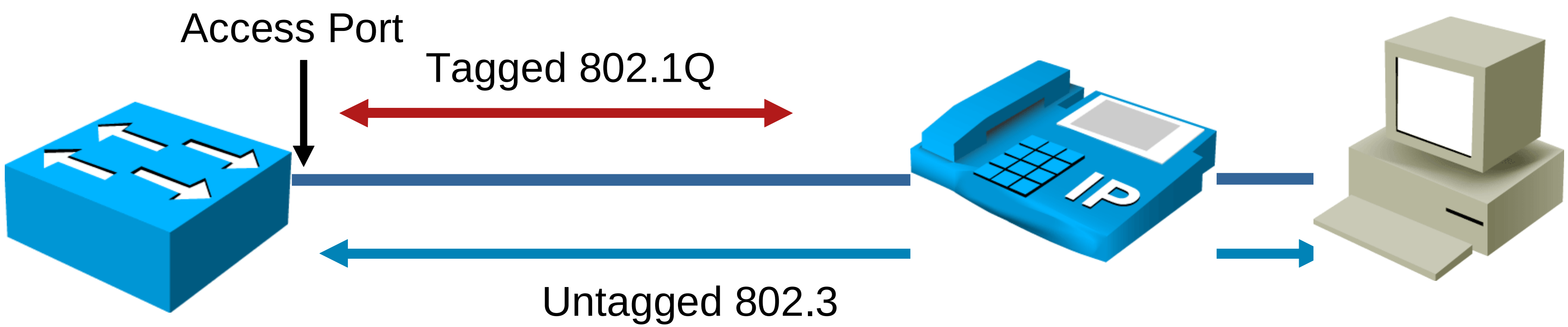
Single VLAN Access Port

- An access port configured for one VLAN only
- Typically used for non-Cisco IP phones or softphones
  - Non-Cisco IP phones: Use voice VLAN for access port
  - Softphones: Use data VLAN for access port and allow required IP communication to voice VLAN (IP ACLs)
- If used with Cisco IP phones:
  - Not recommended with PC attached
  - If no PC attached: Use voice VLAN for access port
- Voice can be tagged with 802.1p (VLAN ID=0) or untagged



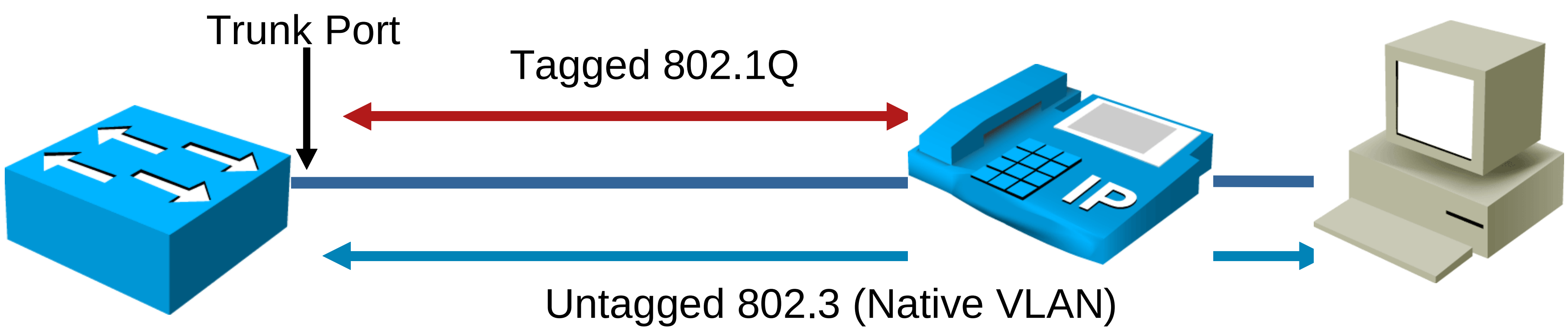
Multi-VLAN Access Port

- An access port able to handle two VLANs
  - Access (data) VLAN and voice (auxiliary) VLAN
- Voice traffic is tagged with 802.1Q VLAN ID
  - Data traffic is untagged and is forwarded by IP to and from PC port.
  - Phone can be hardened to prevent PC from seeing the voice traffic (by default, phone acts like a hub).
  - Best choice with Cisco IP phones.
  - Voice VLAN does not need to be configured on IP phone but can be learned from Cisco Discovery Protocol messages sent out by the switch.



Trunk Ports

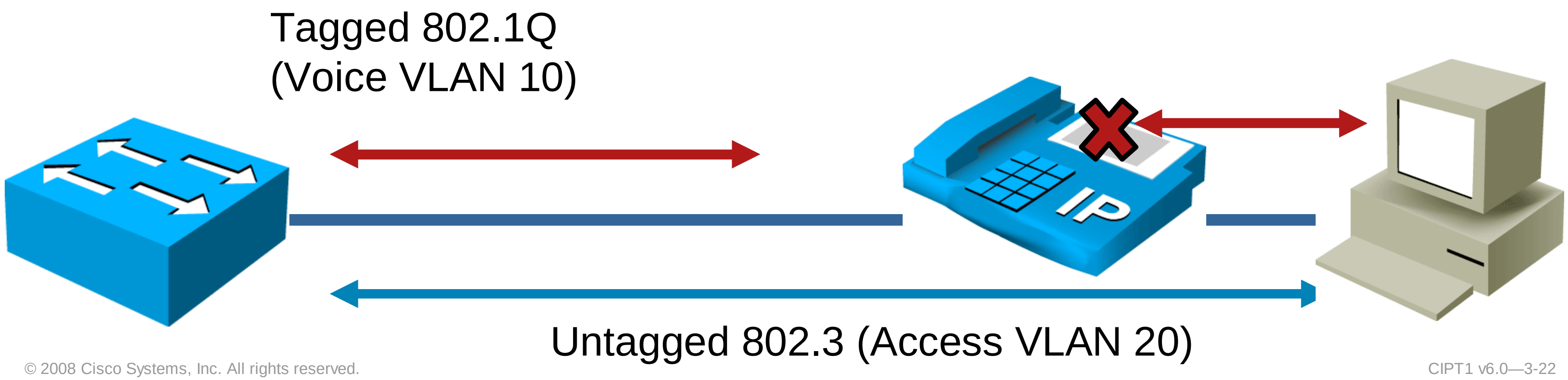
- A trunk port is able to handle multiple VLANs.
- Usually data traffic is untagged and put into a native VLAN.
- Data traffic can be tagged with any 802.1Q VLAN ID if supported by PC (and permitted by IP phone).
- A voice VLAN does not need to be configured on IP phone but can be learned from Cisco Discovery Protocol messages sent out by the switch.
- Security considerations:
  - Cannot be configured as secure port
  - If allowed VLANs are not limited, PC has access to all VLANs of the switch



Blocking PC VLAN Access at IP Phones

With default configuration on a trunk port, if PC sends 802.1Q tagged frames, all VLANs can be accessed from PC.

- Disable voice VLAN access at phone
  - Prevent PC from sending and receiving data tagged with voice VLAN ID
  - Other VLAN IDs are permitted on some IP phones
- Disable span to PC port (on supported IP phones)
  - Prevent PC from sending and receiving any 802.1Q tagged frames



Limiting VLANs on Trunk Ports at the Switch

- VLANs allowed on a trunk port can be configured at the switch.
- Recommendation is to only allow native VLAN and voice VLAN.
  - Blocks PC access to all other VLANs, independent of IP phone configuration and model
  - Access to voice VLAN, can only be prevented by IP phone configuration but is supported on all IP phone models with PC ports
  - Improves performance
  - Improves stability – Minimizes STP issues

Configuring Voice VLANs in Access Port Using Native Cisco IOS Software

Example 1 (single VLAN access port):

```
Console(config)#interface FastEthernet0/1
Console(config-if)#switchport mode access
Console(config-if)#switchport voice vlan dot1p
Console(config-if)#switchport access vlan 261
```

Example 2 (multi-VLAN access port):

```
Console(config)#interface FastEthernet0/1
Console(config-if)#switchport mode access
Console(config-if)#switchport voice vlan 261
Console(config-if)#switchport access vlan 262
```

Configuring Trunk Port Using Native Cisco IOS Software

Example 3 (trunk port):

```
Console(config)#interface FastEthernet0/1
Console(config-if)#switchport trunk encapsulation dot1q
Console(config-if)#switchport mode trunk
Console(config-if)#switchport trunk native vlan 262
Console(config-if)#switchport voice vlan 261
Console(config-if)#switchport trunk allowed vlan 261
```

Verifying Voice VLAN Configuration Using Native Cisco IOS Software

```
Class-1-Switch#sh interfaces fa0/4 switchport
Name: Fa0/4
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 262 (VLAN0262)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: 261 (VLAN0261)
.
.
.
```

Configuring Voice VLANs Using Cisco Catalyst Operating System

Example 1 (single VLAN access port):

```
Console>(enable) set port auxiliaryvlan 2/1-3 dot1p
Console>(enable) set vlan 262 2/1-3
Console>(enable) set trunk 2/1-3 off
```

Example 2 (multi-VLAN access port):

```
Console>(enable) set port auxiliaryvlan 2/1-3 261
Console>(enable) set vlan 262 2/1-3
Console>(enable) set trunk 2/1-3 off
```

Configuring Trunk Ports Using Cisco Catalyst Operating System

Example 3 (trunk port):

```
Console>(enable) set trunk 2/1-3 on
Console>(enable) clear trunk 2/1-3 1-4096
Console>(enable) set vlan 262 2/1-3
Console>(enable) set port auxiliaryvlan 261 2/1-3
Console>(enable) set trunk 261 2/1-3
```

Verifying Voice VLAN Configuration Using Cisco Catalyst Operating System

```
Console> (enable)show port auxiliaryvlan 222
AuxiliaryVlan AuxVlanStatus Mod/Ports
------------- ------------- ----------
222           active        1/2,2/1-3
```

```
Console> (enable)show port 2/1
...
Port  AuxiliaryVlan AuxVlan-Status
----- ------------- --------------
 2/1  222           active
...
```