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

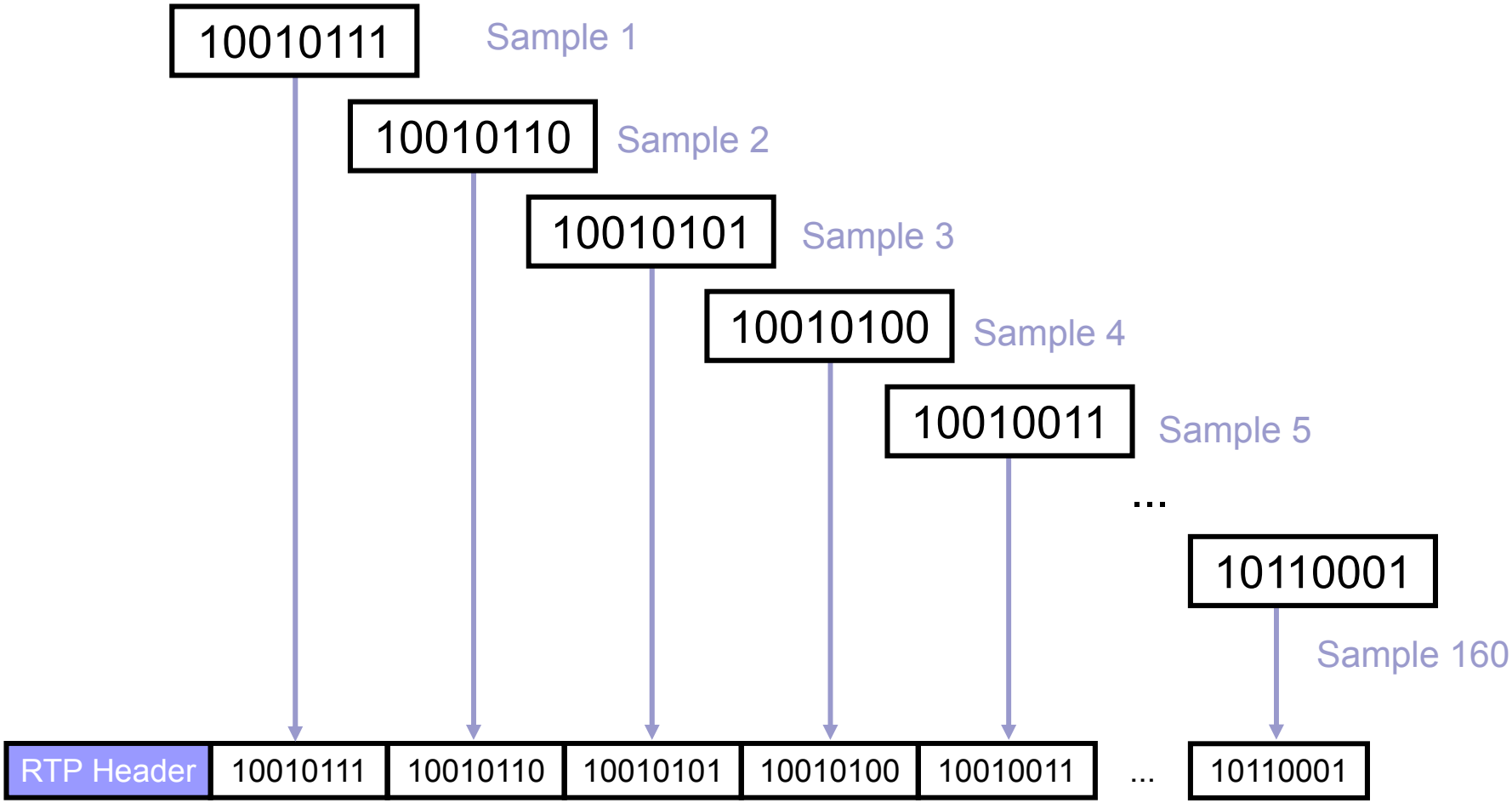
RTP Control Protocol

- 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)

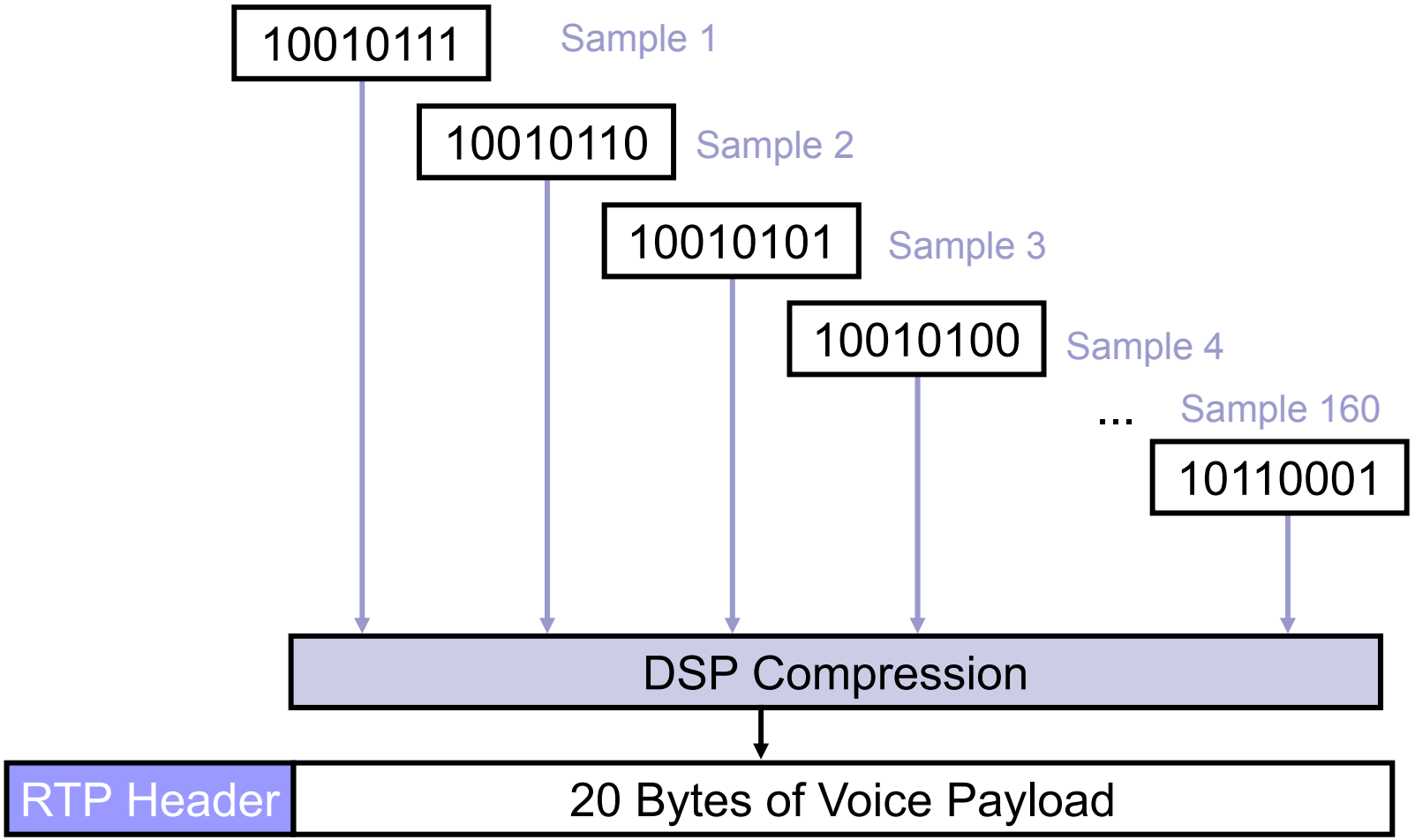
Packetization

- 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.

G.711 codec example



G.729 codec example



G.729 20 ms of voice contained in packet

Codecs—Bandwidth Implications

Codec	G.711	iLBC	G.729
Bandwidth not including overhead	64 kb/s	13.3 kb/s	8 kb/s

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

Some Additional DSP Functions

- Conferencing
- Transcoding between two different codecs
- Echo cancellation

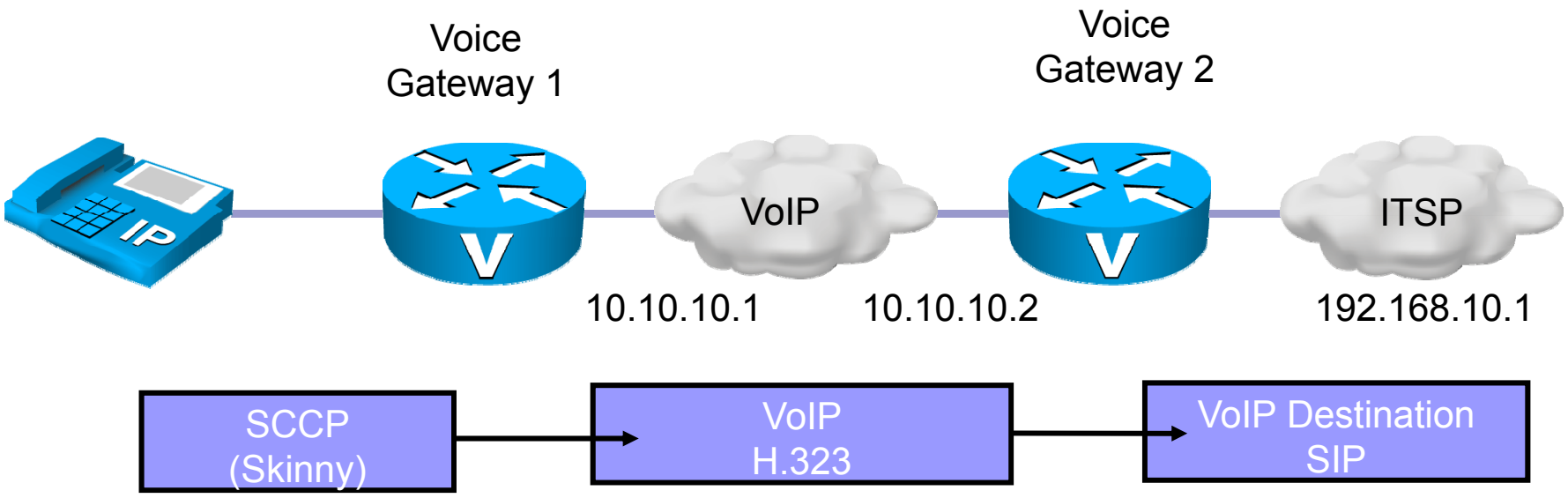
VoIP Signaling Protocols

- 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

	Used on Gateways	Used on Cisco Unified IP Phones	Architecture
H.323	Yes	No	Peer-to-peer
SIP	Yes	Yes, Cisco Unified IP Phones and third-party phones	Peer-to-peer
SCCP (Skinny)	Yes, limited	Yes, Cisco Unified IP Phones only	Client/server

Voice Protocols Example

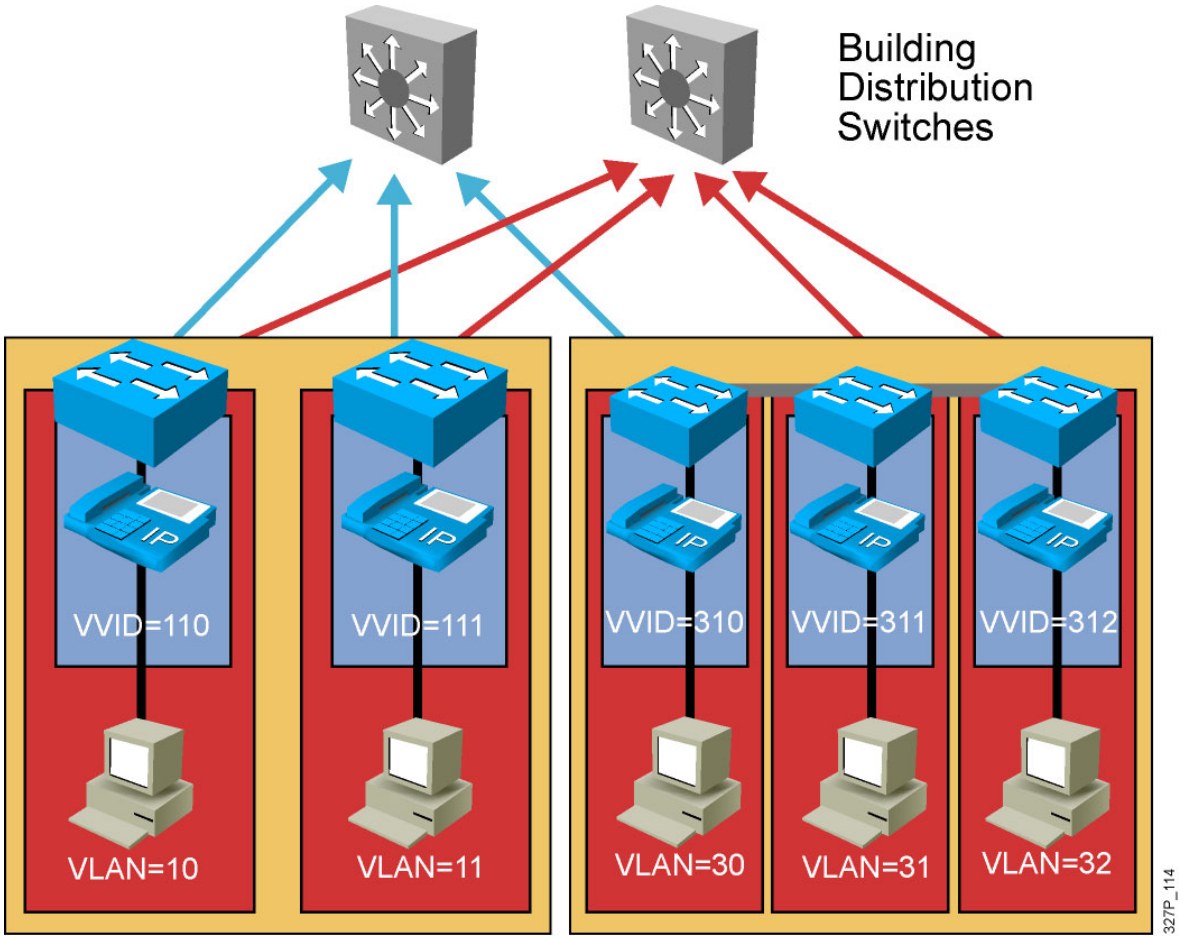


Introducing VoIP Signaling Protocols Summary

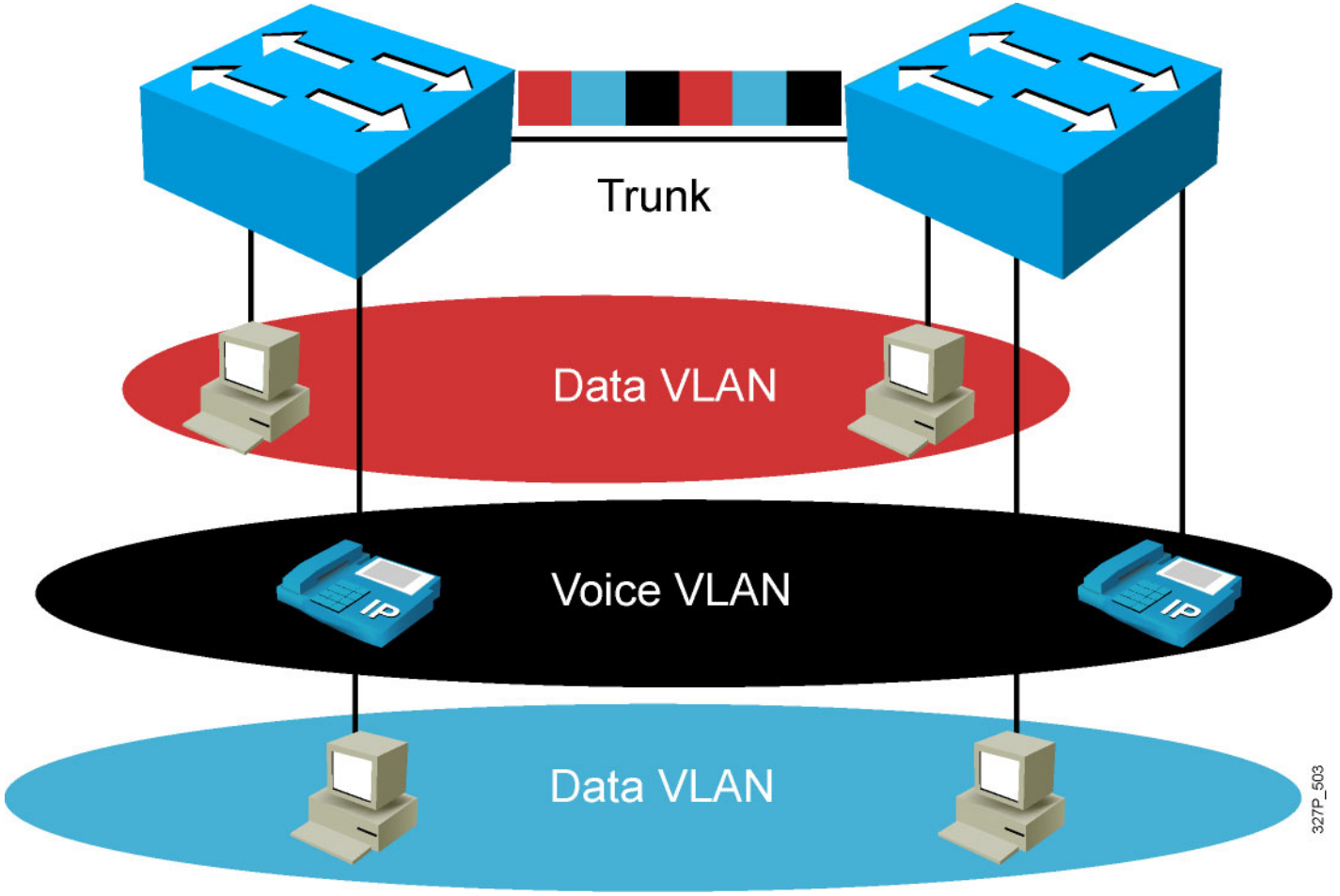
- Signaling protocols are used in VoIP networks to set up new calls, monitor current calls, tear down calls, pass informational signaling, pass supervisory signaling, and pass address signaling.
- SCCP is a proprietary protocol used between Cisco Unified IP Phones and Cisco Unified Communications call control products.
- H.323 is a stable, mature, vendor-neutral protocol that is widely deployed.
- SIP is an emerging protocol based on parts of existing protocols. It is still evolving.

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

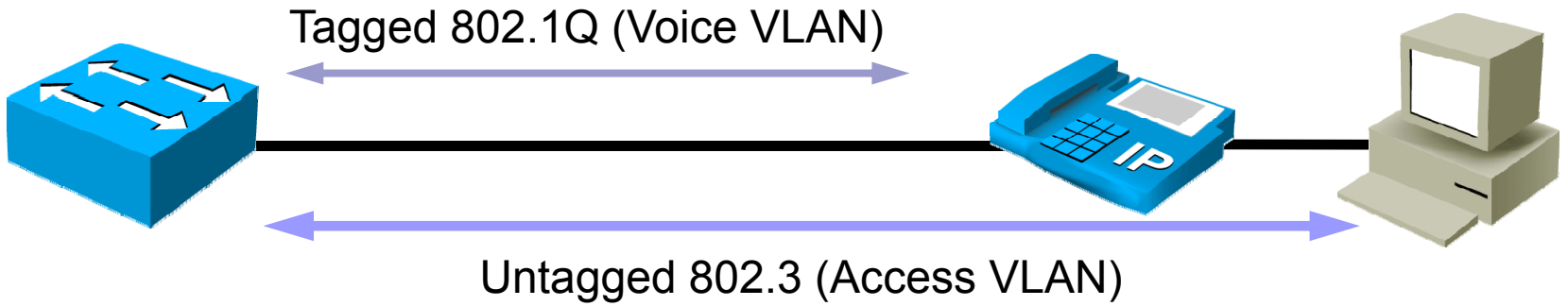


Voice VLANs

- Separates voice and data traffic
- Prevents unnecessary IP address renumbering
- Simplifies QoS configurations
- Requires two VLANs: one for data traffic and one for voice traffic
- Requires only one Ethernet cable drop for the Cisco IP phone
  and the PC that is plugged into the phone
- Requires two IP subnets: one for the data VLAN and one for the voice VLAN

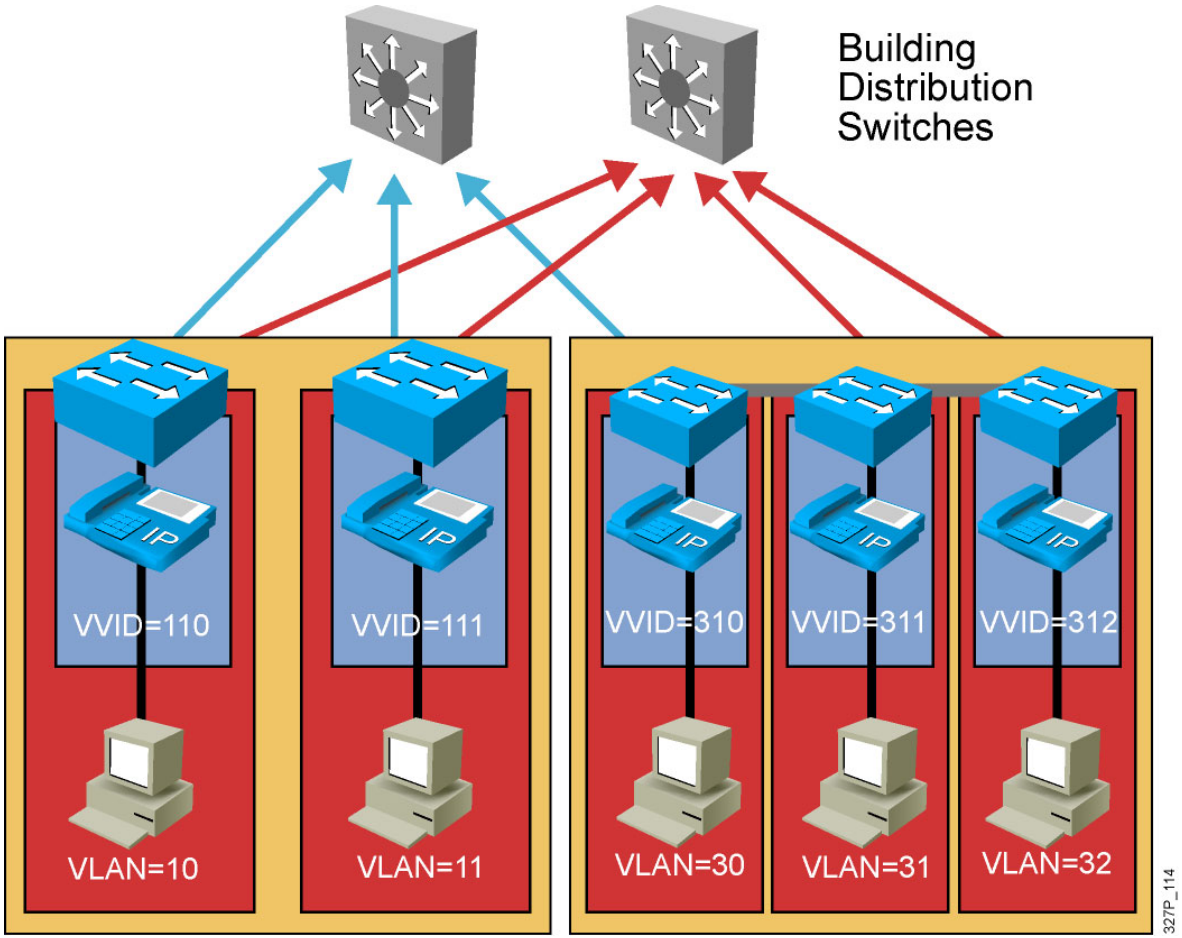
Voice VLANs (Cont.)

- An access port can handle two VLANs:
  - Access VLAN
  - Voice VLAN

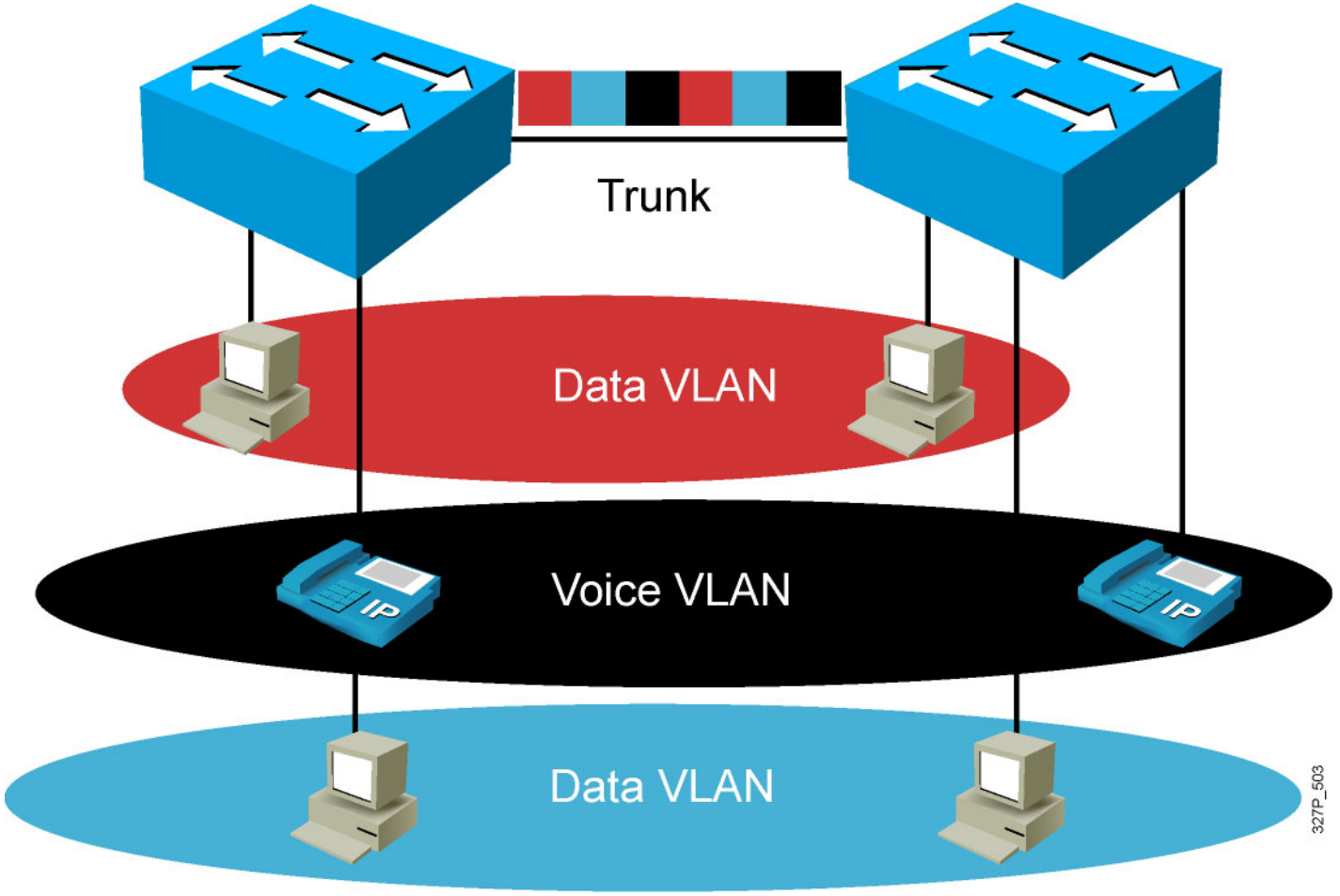


Advantages of Voice VLANs

- 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



Voice VLANs

- Separates voice and data traffic
- Prevents unnecessary IP address renumbering
- Simplifies QoS configurations
- Requires two VLANs: one for data traffic and one for voice traffic
- Requires only one Ethernet cable drop for the Cisco IP phone
  and the PC that is plugged into the phone
- Requires two IP subnets: one for the data VLAN and one for the voice VLAN

Voice VLANs (Cont.)

- An access port can handle two VLANs:
  - Access VLAN
  - Voice VLAN