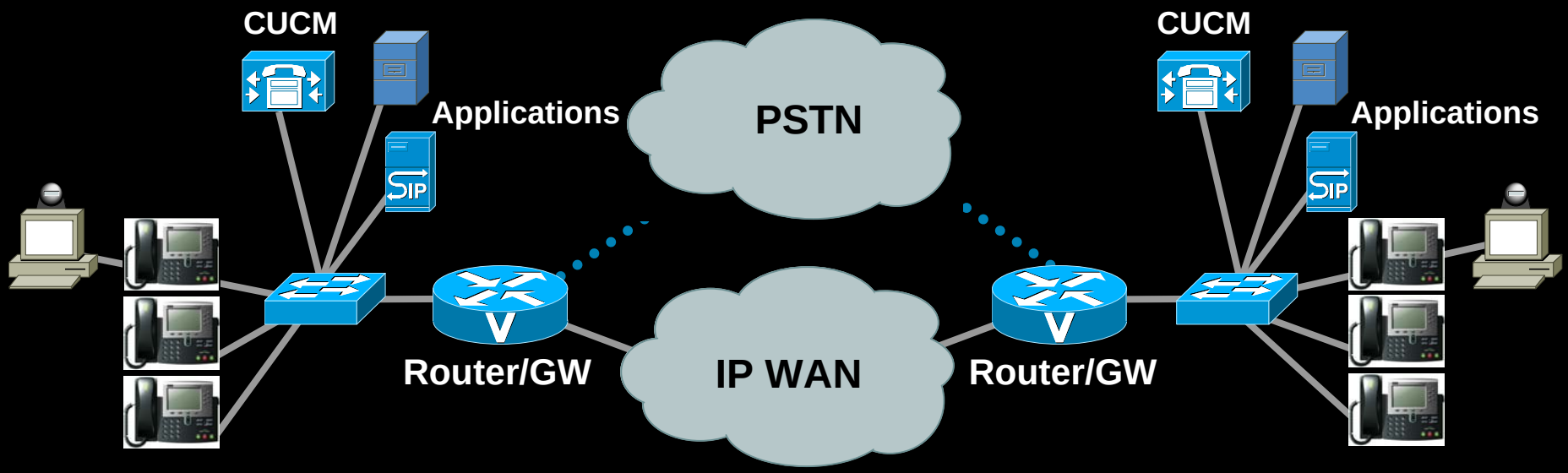
Unified Communications

Cisco Technologies 2007

Enterprise IP Telephony Design and Deployment

Melinda Delplace

Scope of This Seminar



- Understanding what can be built today
- Learning how to build it
- To find out more about Unified Communications design:

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

Note : Name Change - Cisco Unified Communications Manager = CUCM

Agenda

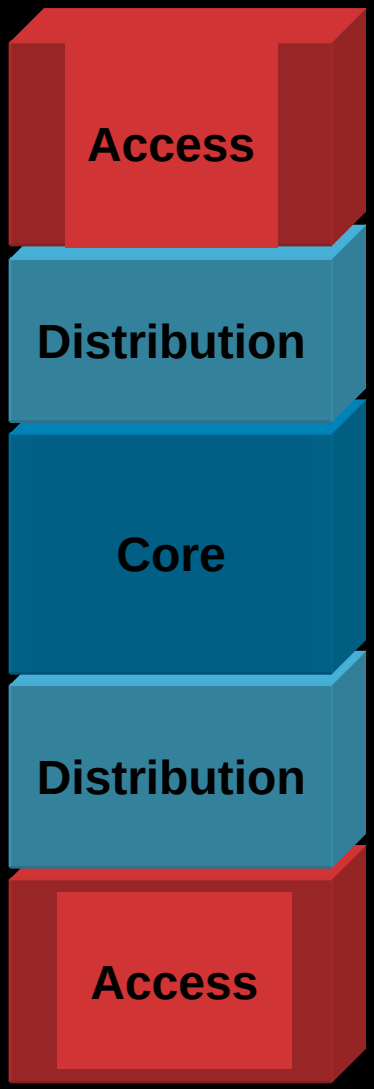
- Network Infrastructure
- Unified Communications/Telephony Infrastructure
- Security and Management

Network Infrastructure Agenda

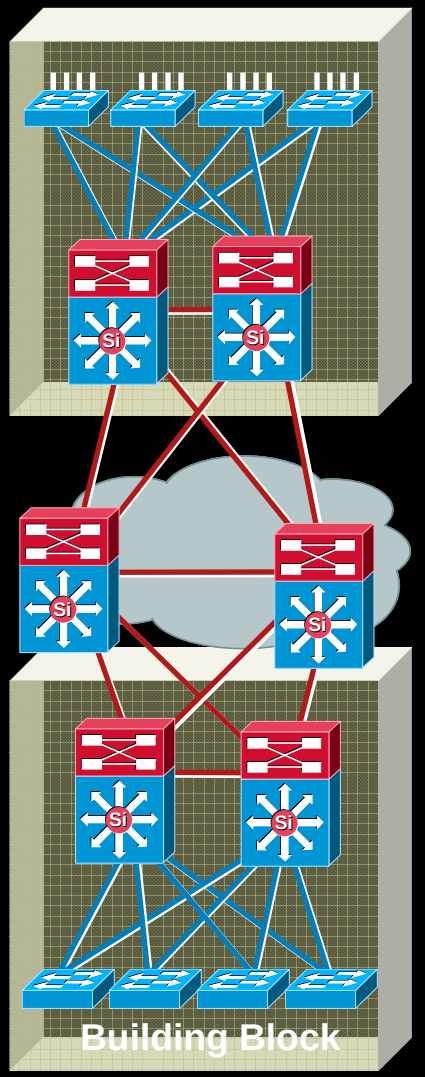
- Building a Campus Network
- Enabling QoS in the Campus
- Enabling QoS in the WAN

Building a Campus Network
Hierarchical Network Design

Without a Rock Solid Foundation the Rest Doesn't Matter

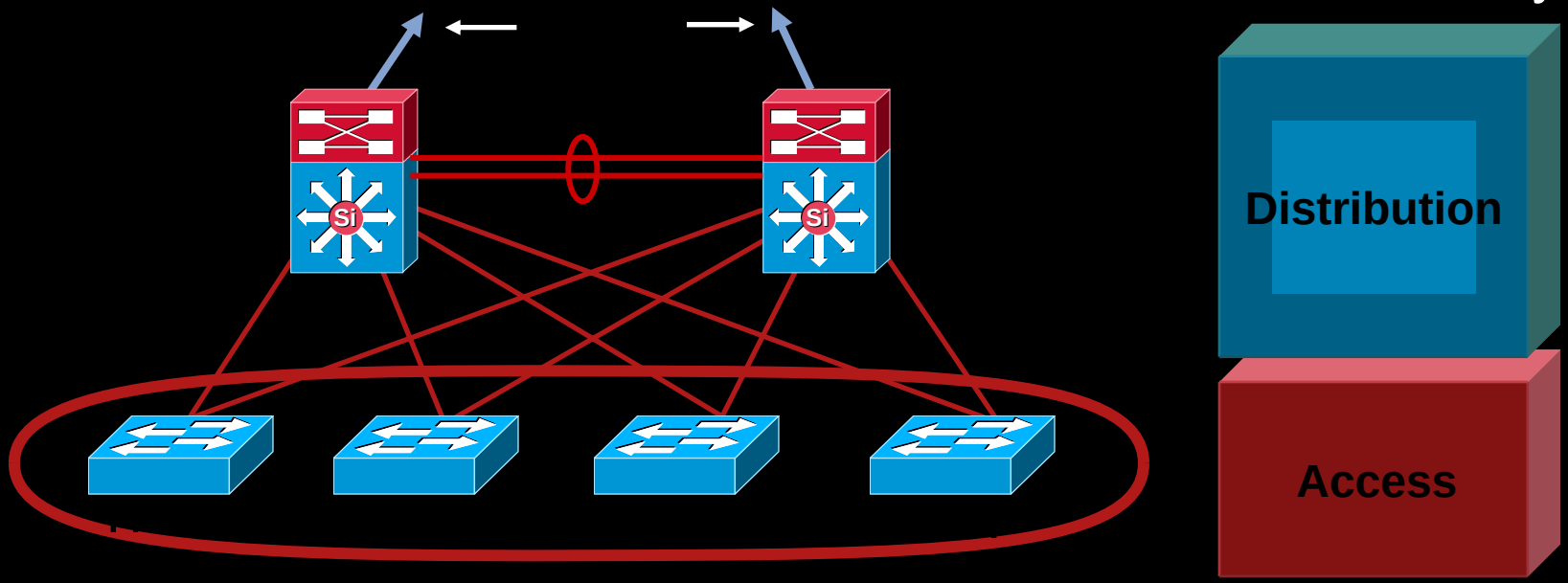


- Offers hierarchy – each layer has specific role
- Modular topology - building blocks
- Easy to grow, understand, and troubleshoot
- Creates small fault domains – Clear demarcations and isolation
- Promotes load balancing and redundancy
- Promotes deterministic traffic patterns
- Incorporates balance of both Layer 2 and Layer 3 technology, leveraging the strength of both
- Utilizes Layer 3 Routing for load balancing, fast convergence, scalability, and control



Building a Campus Network—The Access Layer

Feature Rich Environment—Not Just About Connectivity

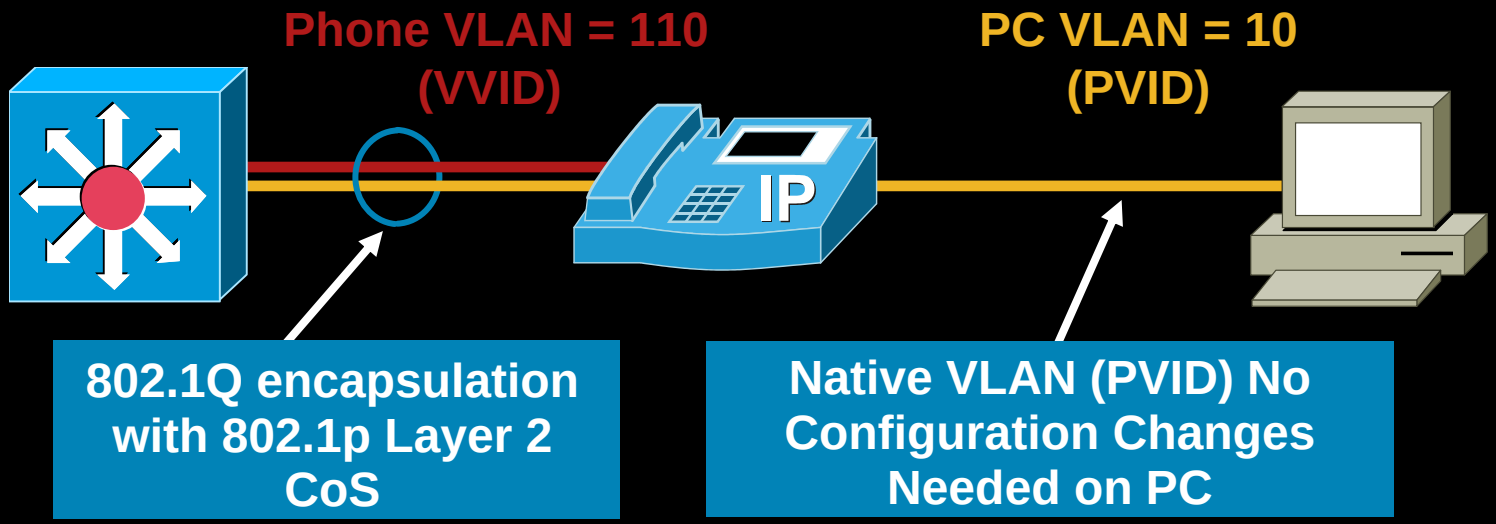


VLANS do not span access switches

- Aggregates network end-points
- Layer 2/Layer 3 feature rich environment; convergence, HA, security, QoS, IP multicast, etc
- Intelligent network services: QoS, trust boundary, broadcast suppression, IGMP snooping
- Intelligent network services: Rapid PVST+, EIGRP, OSPF, DTP, PAgP, UDLD, etc.
- Catalyst® integrated security features 802.1x, Port security, DHCP snooping, Dynamic ARP Insp, IP Source Guard, etc.
- Automatic phone discovery, conditional trust boundary, Power Over Ethernet, auxiliary VLAN, etc.
- Spanning tree toolkit: Portfast, UplinkFast, BackboneFast, LoopGuard, BPDUGuard, BPDUFilter, RootGuard, etc.

Campus Network—Access Layer

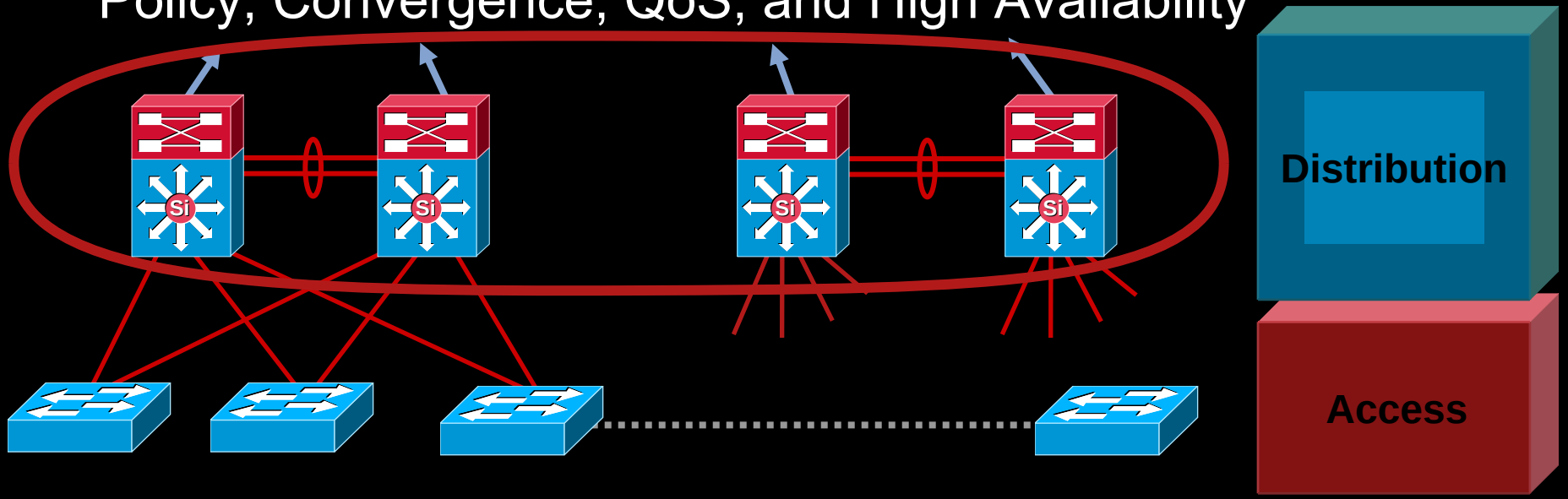
Voice and Data VLANs



- During initial CDP exchange phone is configured with a Voice VLAN ID (VVID)
- Phone also supplied with QoS configuration via CDP TLV fields
- Quality—Separation of broadcast domains i.e. phones and PCs are on separate subnets
- Security—Different network policies for different subnets; WORM attacks can be contained to the PC VLANs.

Building a Campus Network—The Distribution Layer

Policy, Convergence, QoS, and High Availability

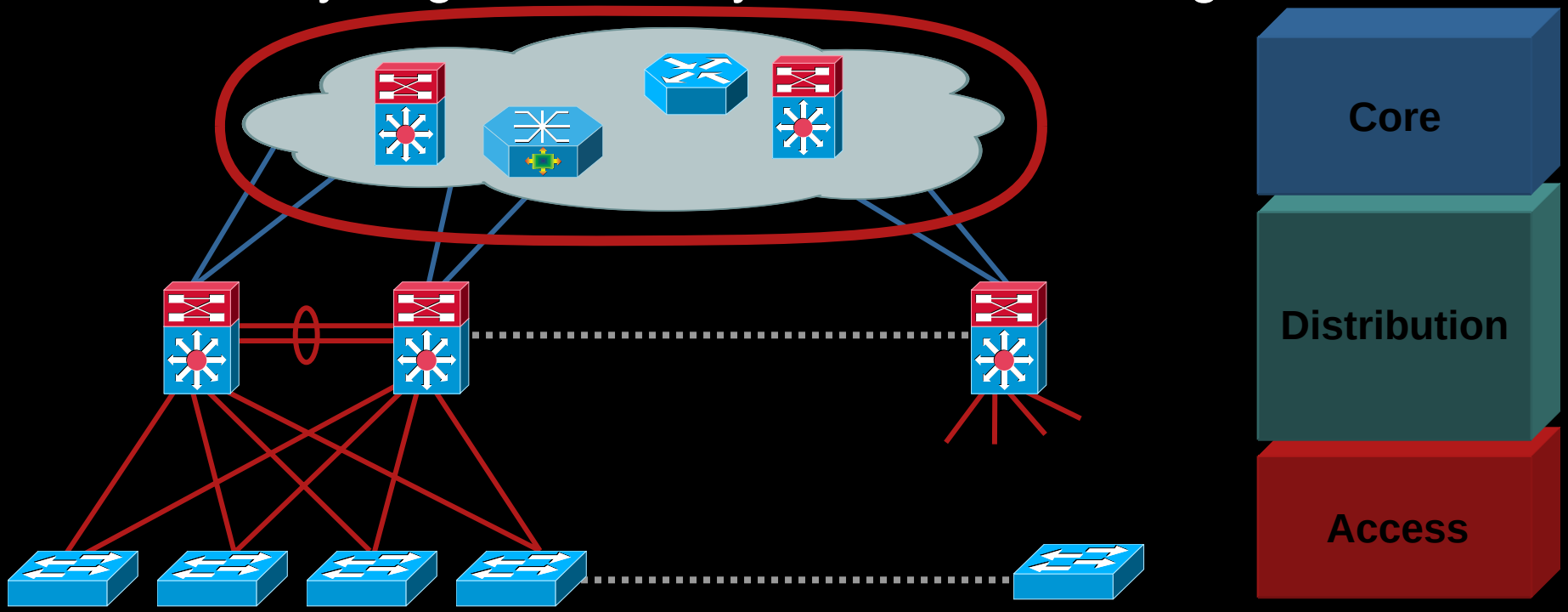


- Availability, load balancing, QoS and provisioning are the important considerations at this layer
- Aggregates wiring closets (access layer) and uplinks to core
- Use Layer 3 switching in the distribution layer
- Protects core from high density peering and problems in access layer

- EIGRP/ OSPF - Route summarization, passive interfaces to access layer, sub second convergence possible with timer adjustment, redundant path load sharing
- HSRP or GLBP to provide first hop redundancy, sub second convergence possible with timer adjustment
- Spanning tree features (Only if needed):
  - Setting STP Root, Root Guard, Rapid PVST+—Per VLAN 802.1w

Building a Campus Network—The Core Layer

Scalability, High Availability, and Fast Convergence

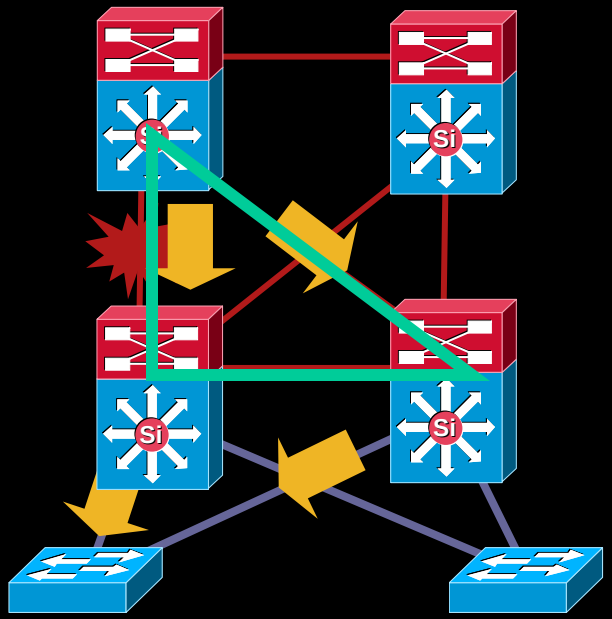


- Backbone for the network—connects network building blocks
- Performance and stability vs. complexity—less is more in the core
- Aggregation point for distribution layer
- Tune routing protocol timers for sub second convergence
- Separate core layer helps in scalability during future growth

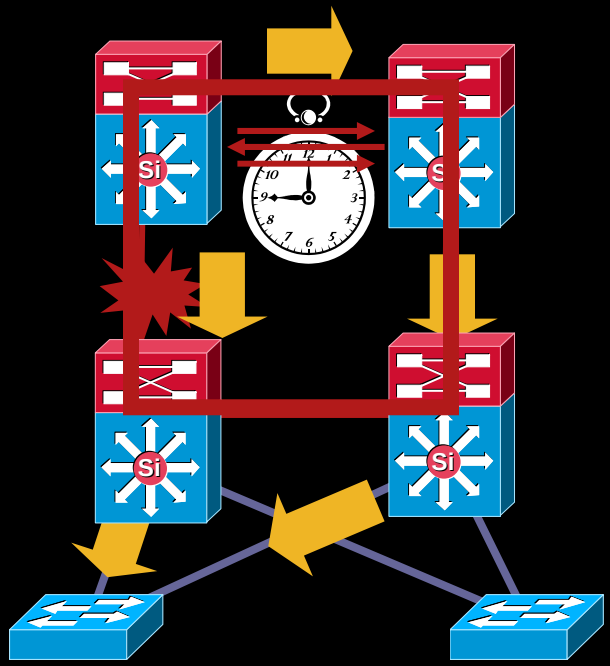
Campus Design Best Practice Build Triangles Not Squares

Deterministic vs. Non-Deterministic

Triangles: Link/Box Failure Does NOT Require Routing Protocol Convergence



Squares: Link/Box Failure Requires Routing Protocol Convergence



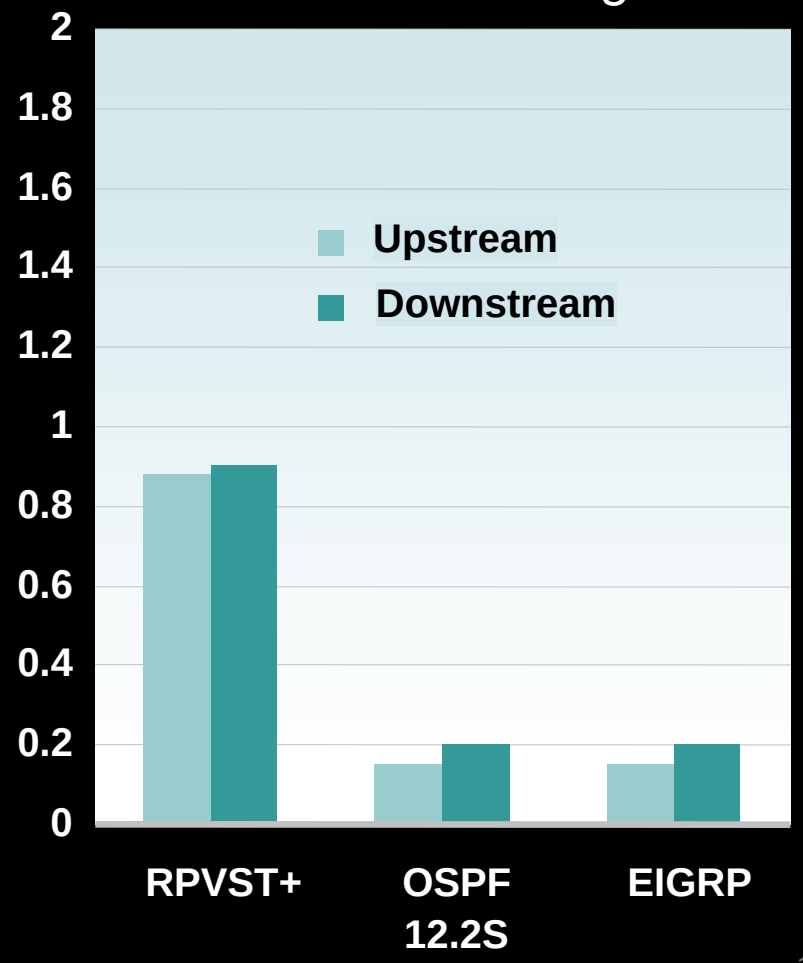
- Layer 3 redundant equal cost links support fast convergence
- Hardware based—fast recovery to remaining path
- Convergence is extremely fast (dual equal-cost paths: no need for OSPF or EIGRP to recalculate a new path)

Campus Design—Routing to the Edge?

Advantages, Yes in the Right Environment

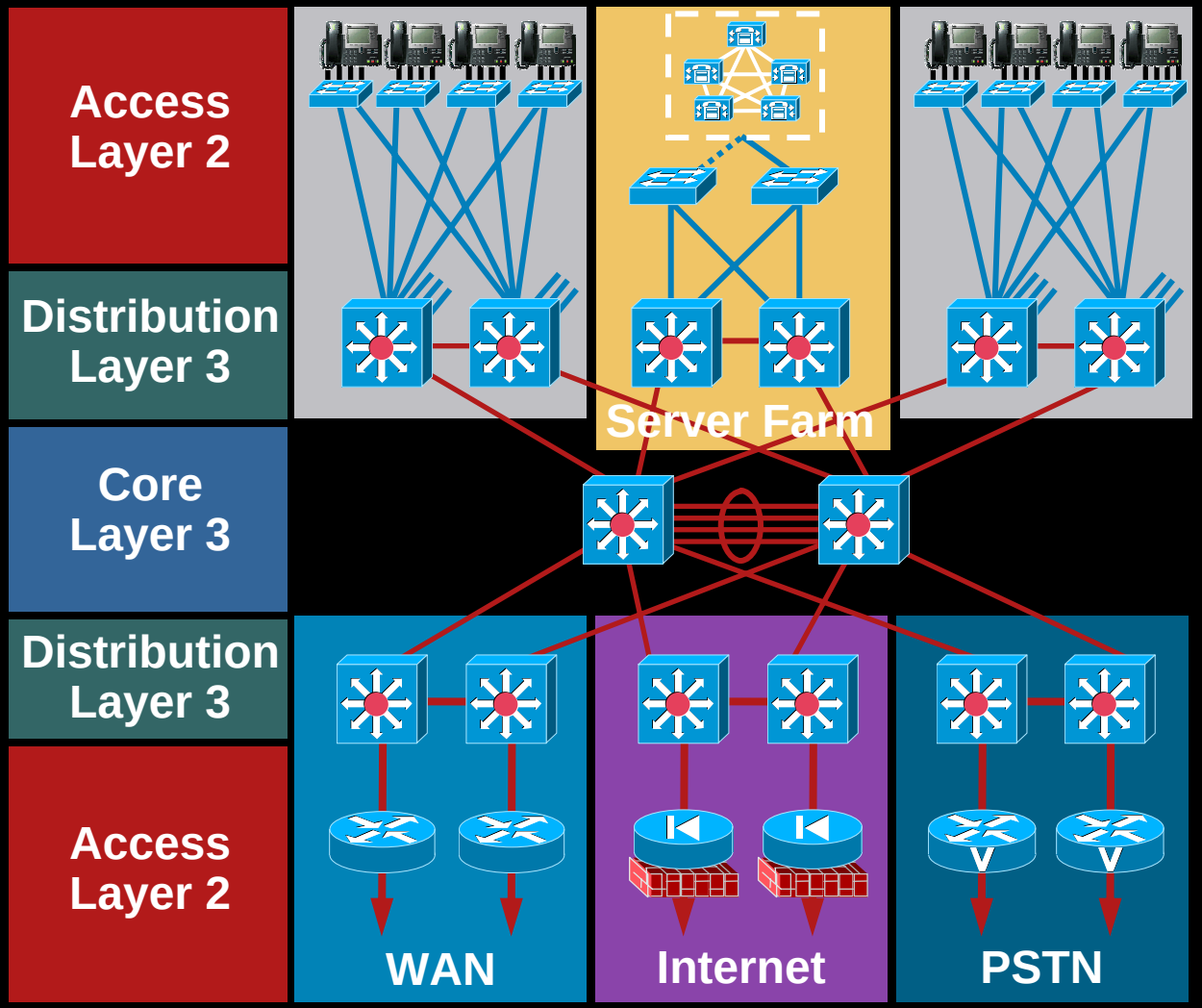
- Easier implement, less to get right
  - No matching of STP/HSRP/GLBP priority
  - No L2/L3 Multicast topology inconsistencies
- Well known tool set
  - traceroute, show ip route, show ip eigrp neighbor, etc.
- Most Catalyst switches support L3 Switching
- EIGRP converges in <200 msec
- OSPF with sub-second tuning converges in <200 msec
- RPVST+ convergence times dependent on GLBP/HSRP tuning

Both L2 and L3 Can Provide Sub-Second Convergence



Building a Campus Network
Summary

- Access layer
  - Rapid Per-VLAN spanning-tree (PSVT +)
  - Rootguard
  - Portfast
  - UplinkFast
  - Layer 3 to the edge ?
- Distribution Layer
  - HSRP/GLBP with load balancing
  - OSPF/EIGRP configured for fast convergence
- Core Layer
  - OSPF/EIGRP configured for fast convergence



http://www.cisco.com/en/US/netsol/ns656/networking_solutions_design_guidances_list.html#anchor2

Network Infrastructure Agenda

- Building a Campus Network
- Enabling QoS in the Campus
- Enabling QoS in the WAN

Enabling QoS in the Campus
Traffic Profiles and Requirements

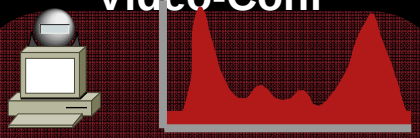
Voice

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

- Latency ≤ 150 ms
- Jitter ≤ 30 ms
- Loss ≤ 1%

One-Way Requirements

Video-Conf

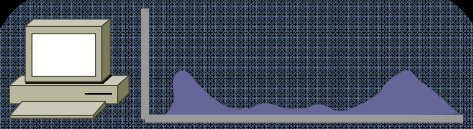


- Bursty
- Greedy
- Drop sensitive
- Delay sensitive
- UDP priority

- Latency ≤ 150 ms
- Jitter ≤ 30 ms
- Loss ≤ 1%

One-Way Requirements

Data

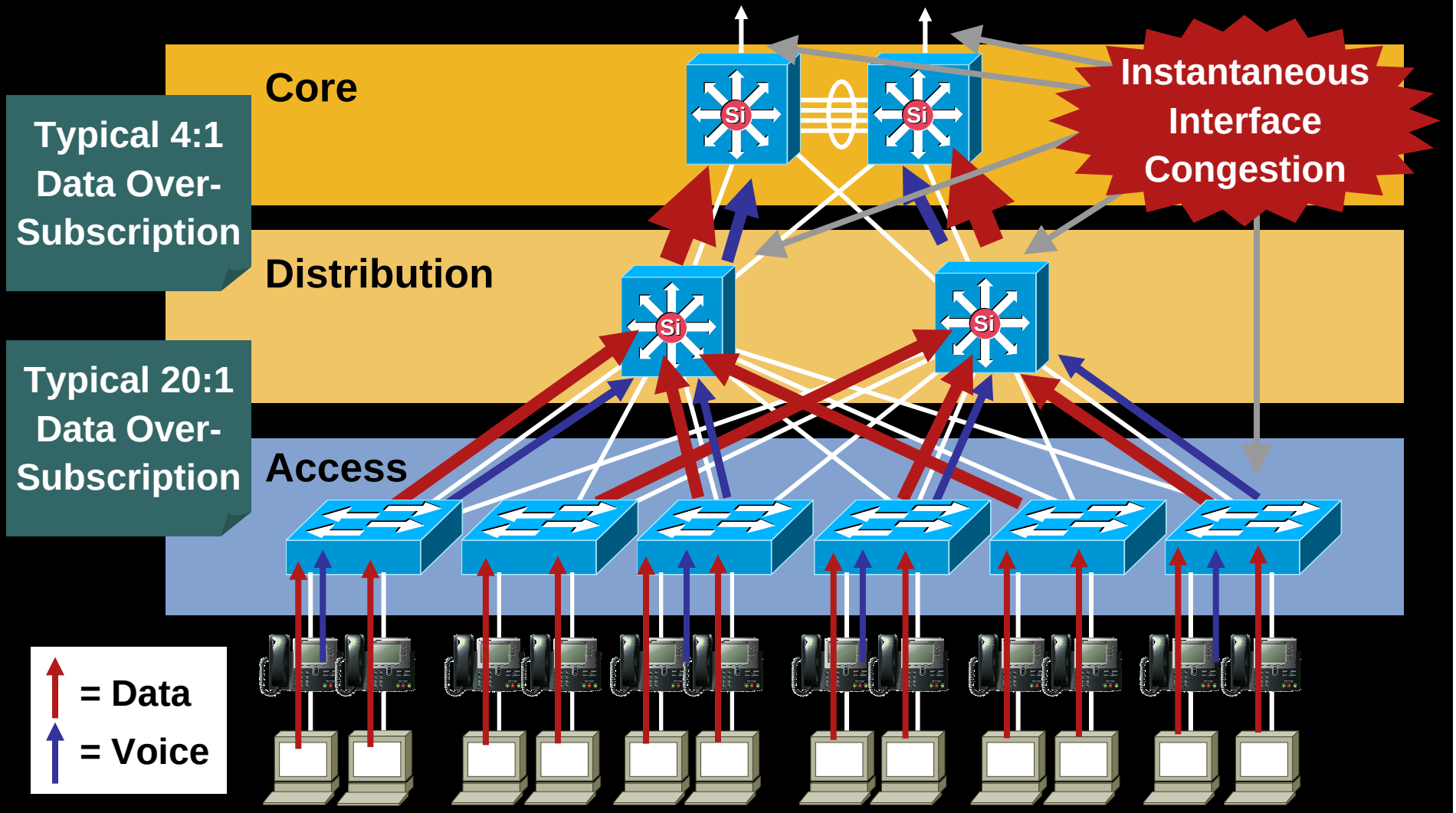


- Smooth/bursty
- Benign/greedy
- Drop insensitive
- Delay insensitive
- TCP retransmits

Data Classes:
Mission-Critical Apps
Transactional/Interactive Apps
Bulk Data Apps
Best Effort Apps (Default)

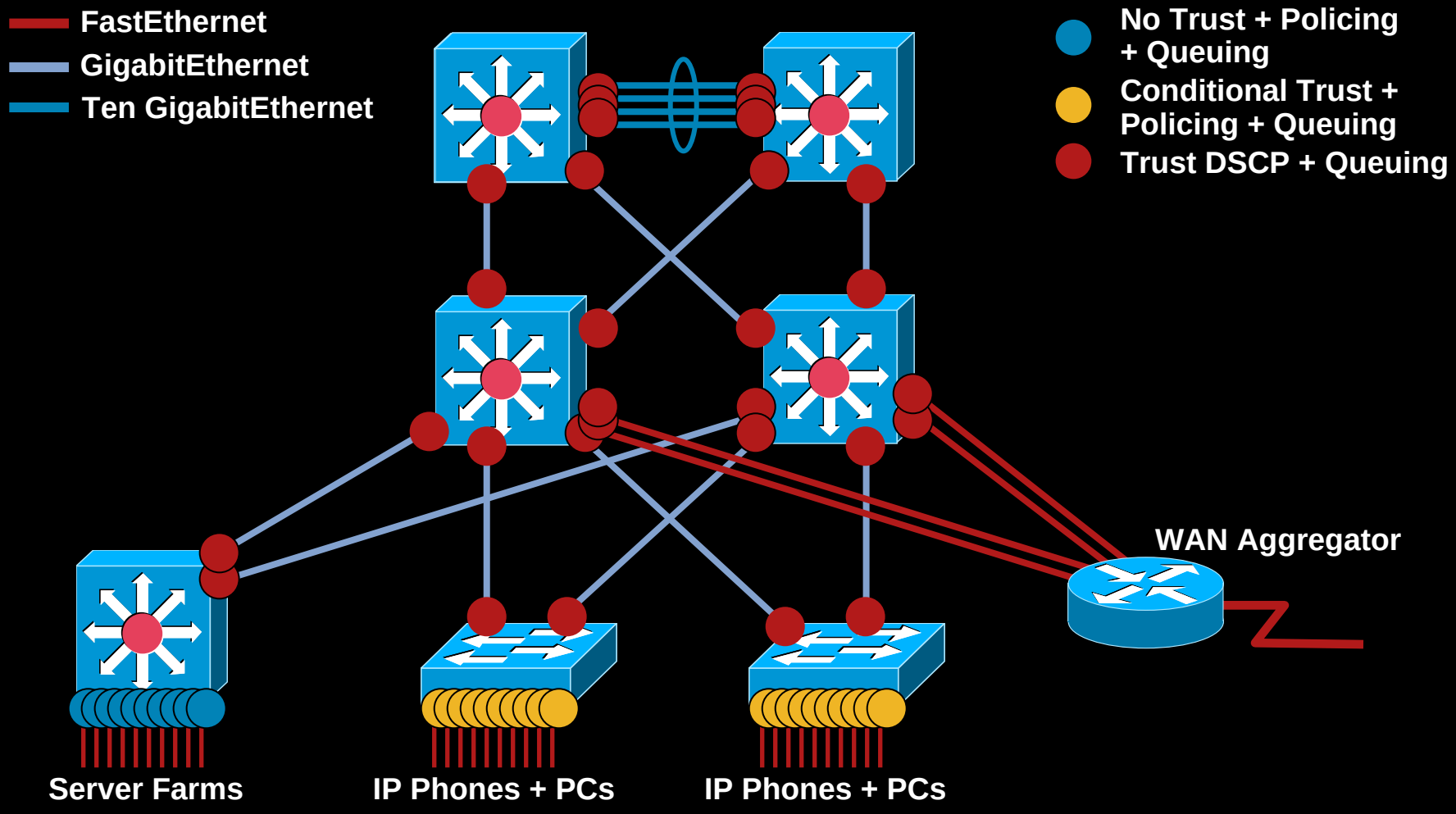
Enabling QoS in the Campus

Congestion Scenario: TCP Traffic Burst + VoIP



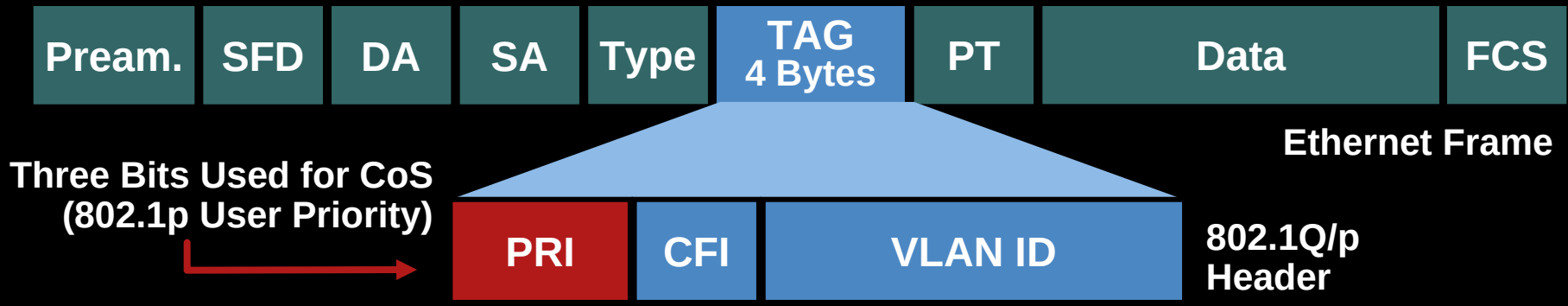
Campus QoS Considerations

Where Is QoS Required Within the Campus?



Enabling QoS in the Campus

Layer 2 Classification: 802.1p, CoS

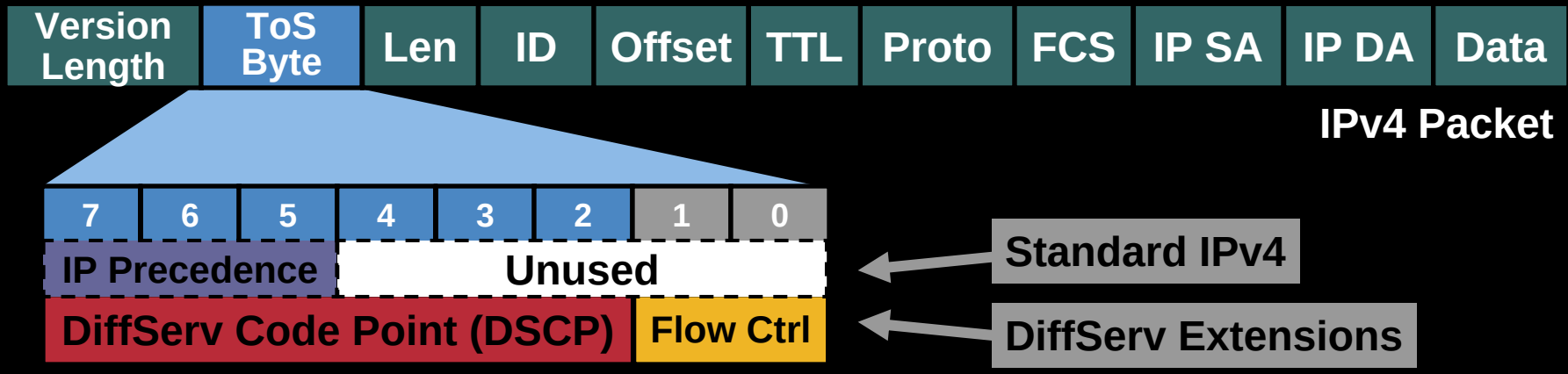


- 802.1p user priority field also called Class of Service (CoS)
- Different types of traffic are assigned different CoS values
- CoS six and seven are reserved for network use

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

*** Including Audio and Video**

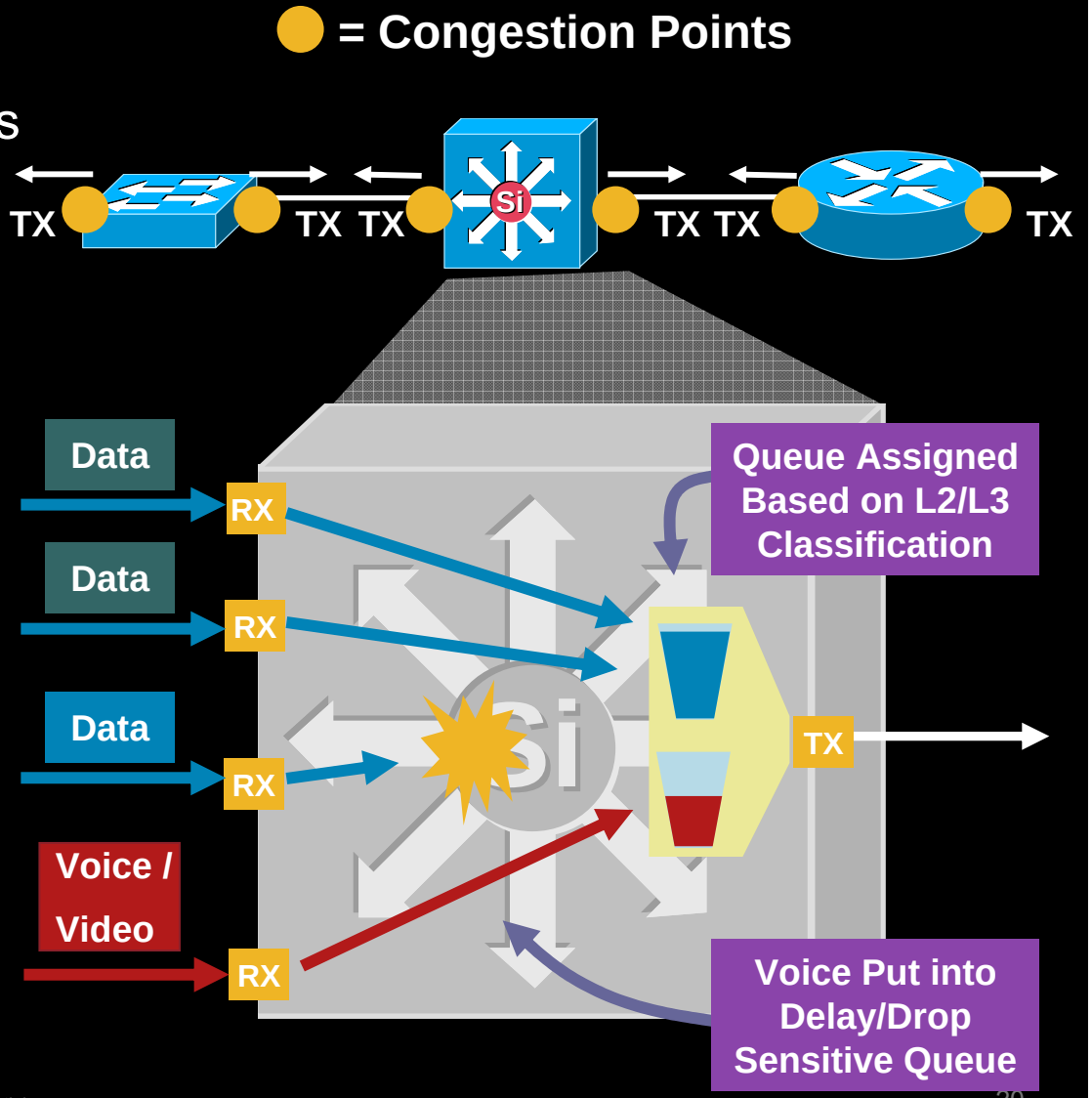
Enabling QoS in the Campus
Layer 3 Classification: IP Precedence, DSCP



- IPv4: three most significant bits of ToS byte are called IP precedence—other bits unused by IP precedence
- DiffServ: six most significant bits of ToS byte are called Diff Serv Code Point (DSCP)—remaining two bits used for flow control
- DSCP is backward-compatible with IP precedence
- DSCP values correspond to Per Hop Behavior (PHB) designations
- RFC 2474 provides more information on DSCP

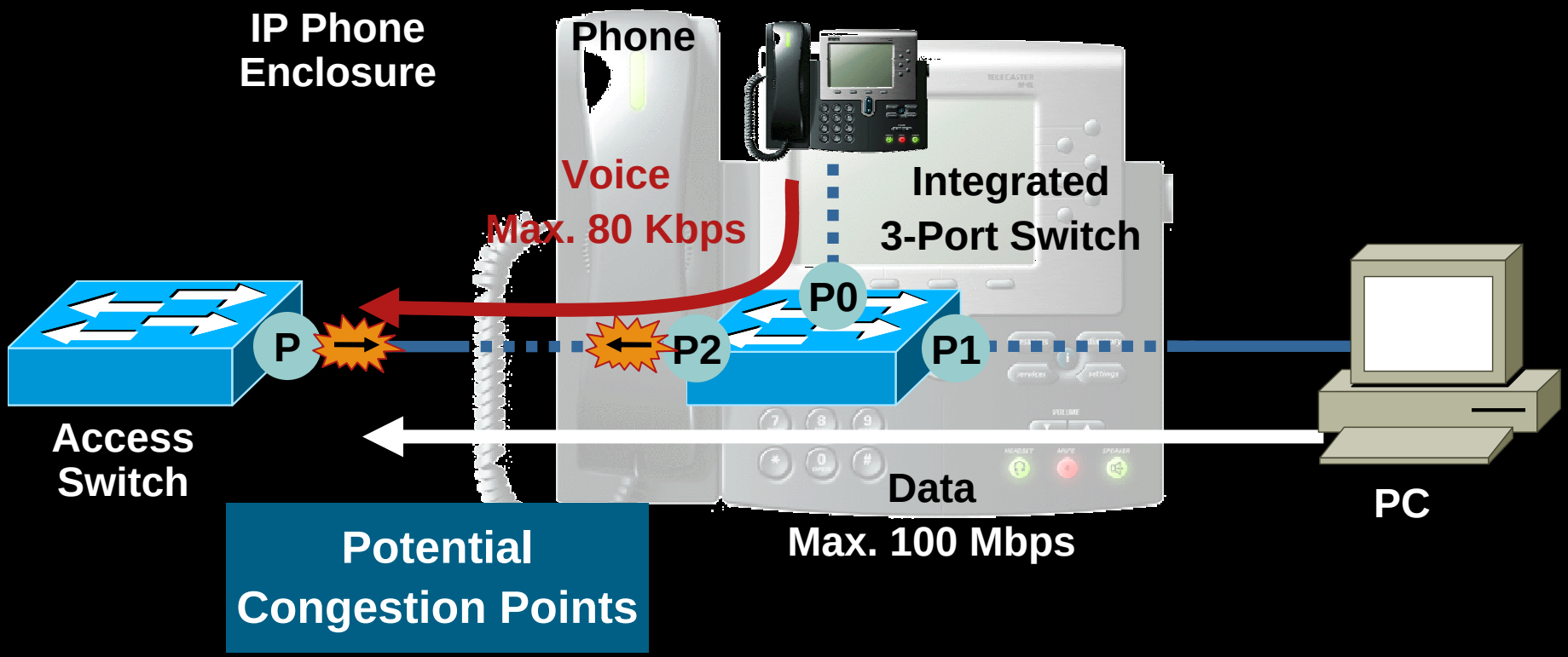
Enabling QoS in the Campus
Scheduling in the Campus

- Output buffers can reach 100% in campus networks resulting in dropped voice packets
- QoS required when there is a possibility of congestion in buffers
- Multiple queues are the only way to "guarantee" voice quality
- No hubs!
- Check your legacy switches



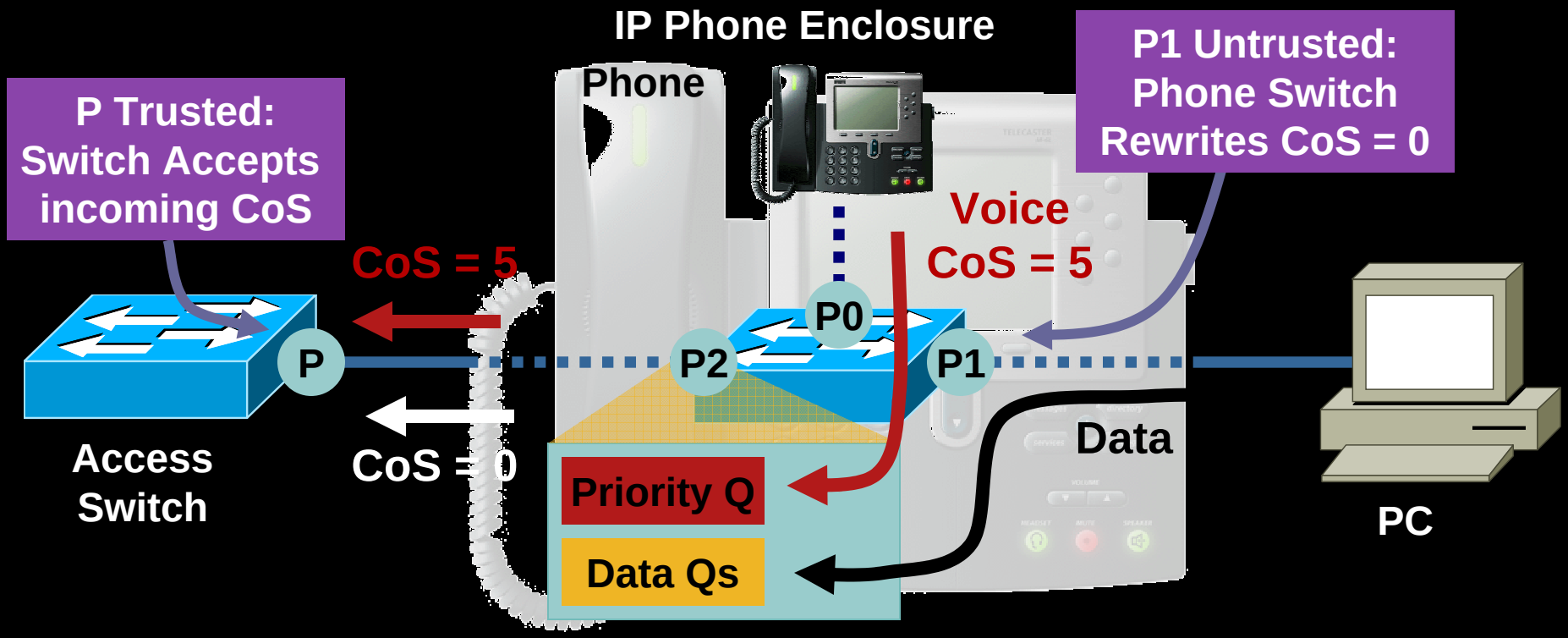
Enabling QoS in the Campus

Congestion Scenario: Data + VoIP



During Data Traffic Bursts, Buffers Can Become Congested, Causing Voice Packets to Be Dropped

Enabling QoS in the Campus
Scheduling in IP Phones



- Voice media traffic is marked with CoS 5/ DSCP EF (high priority)
- Data traffic from the PC is remarked with CoS 0 (low priority) by the IP phone switch; this occurs if PC tags frames as 802.1p/Q; phone switch transparent if PC frames untagged

Network Infrastructure Agenda

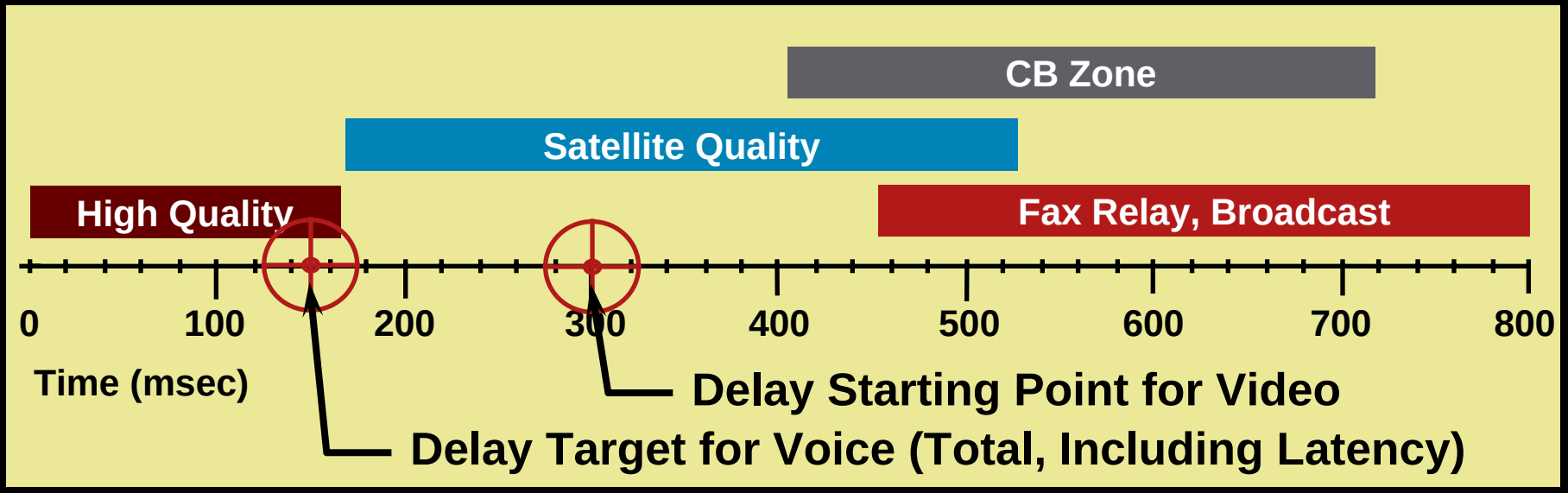
- Building a Campus Network
- Enabling QoS in the Campus
- Enabling QoS in the WAN

Enabling QoS in the WAN

Factors That Negatively Affect Packet-Based Voice/Video

Enabling QoS in the WAN
End-to-End Latency or Voice and Video

ITU G.114 "Recommendation": 0–150msec One-Way Delay



- Video takes longer to encode/decode than voice
- Average is 150-ms encode and 150-ms decode = 300 ms
- The audio is typically delayed to sync up with the video (except for VT advantage)

Agenda

- Network Infrastructure
- Unified Communications/Telephony Infrastructure
- Security and Management

Unified Communications/Telephony Infrastructure Agenda

- Unified Communications/Telephony Infrastructure
  - Network Services
  - Cisco Unified Communications Cluster
  - Deployment Models
  - Signaling Protocols
  - Failover and Redundancy

Unified Communications Infrastructure
Network Services

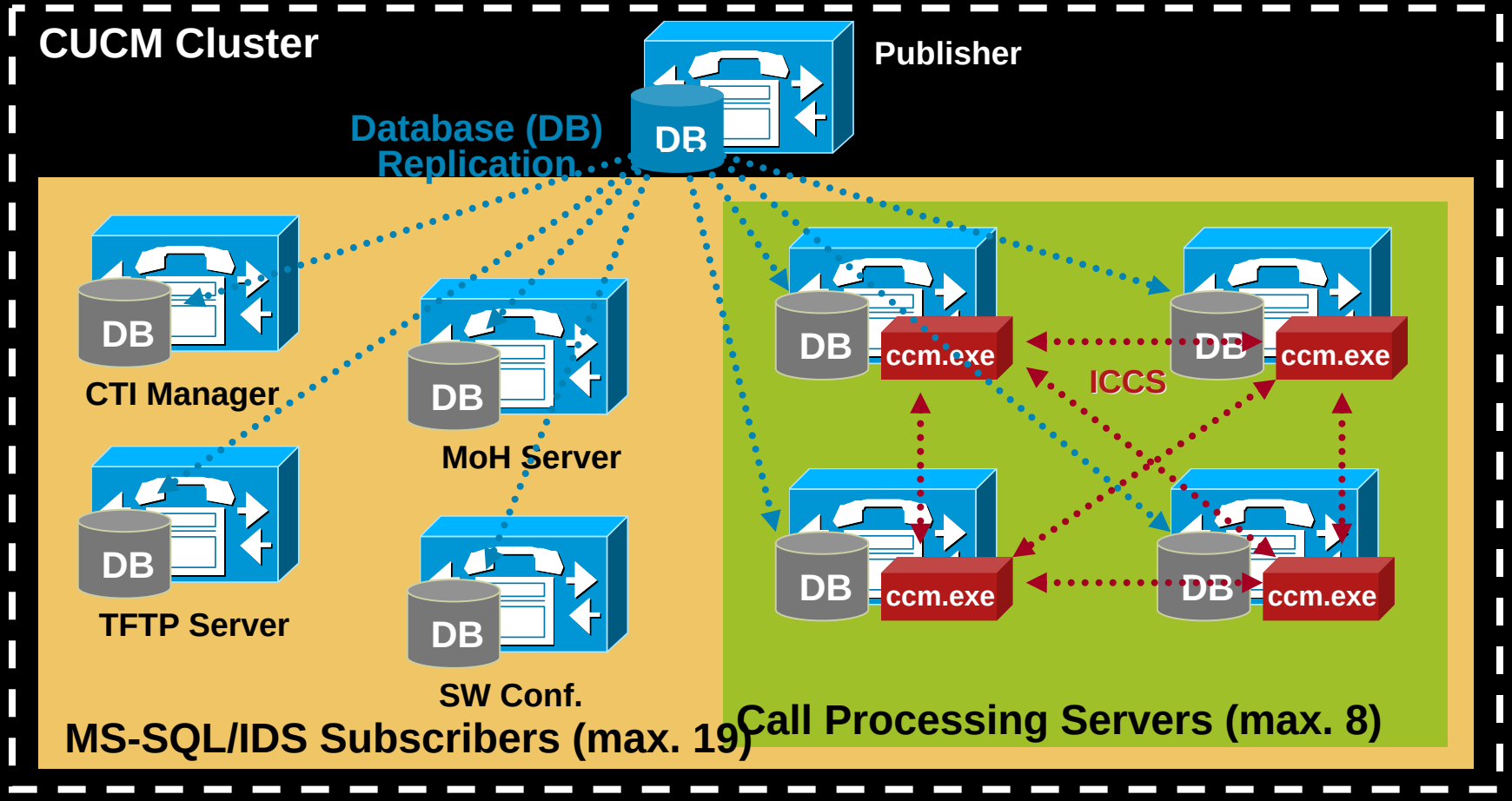
- CDP puts IP phone in correct voice VLAN/subnet and allows for proper power computation
- DHCP used to automate network access
  - DHCP server needs to provide the following:
    - IP address and network mask
    - Default gateway
    - Option 150, TFTP server
    - DNS server (optional)
  - Can be centrally managed (IP helper address)
  - Can be locally implemented (e.g., Cisco IOS DHCP server function)
- TFTP server provides configuration file and phone s/w distribution to endpoints (e.g. IP phones)
- DNS server is optional

Unified Communications/Telephony Infrastructure Agenda

- Unified Communications/Telephony Infrastructure
  - Network Services
  - Cisco Unified Communications Cluster
  - Deployment Models
  - Basic Call Processing
  - Signaling Protocols
  - Failover and Redundancy

Unified Communications Infrastructure

Cisco Communications Manager Cluster



DB=MS-SQL (CM 4.X); DB= IBM-IDS (CM 6.X &5.X)

OS=MS W2K server (CM 4.X); OS= Linux (CM 6.X & 5.X)

Unified Communications Infrastructure
Clustering Properties and Rules

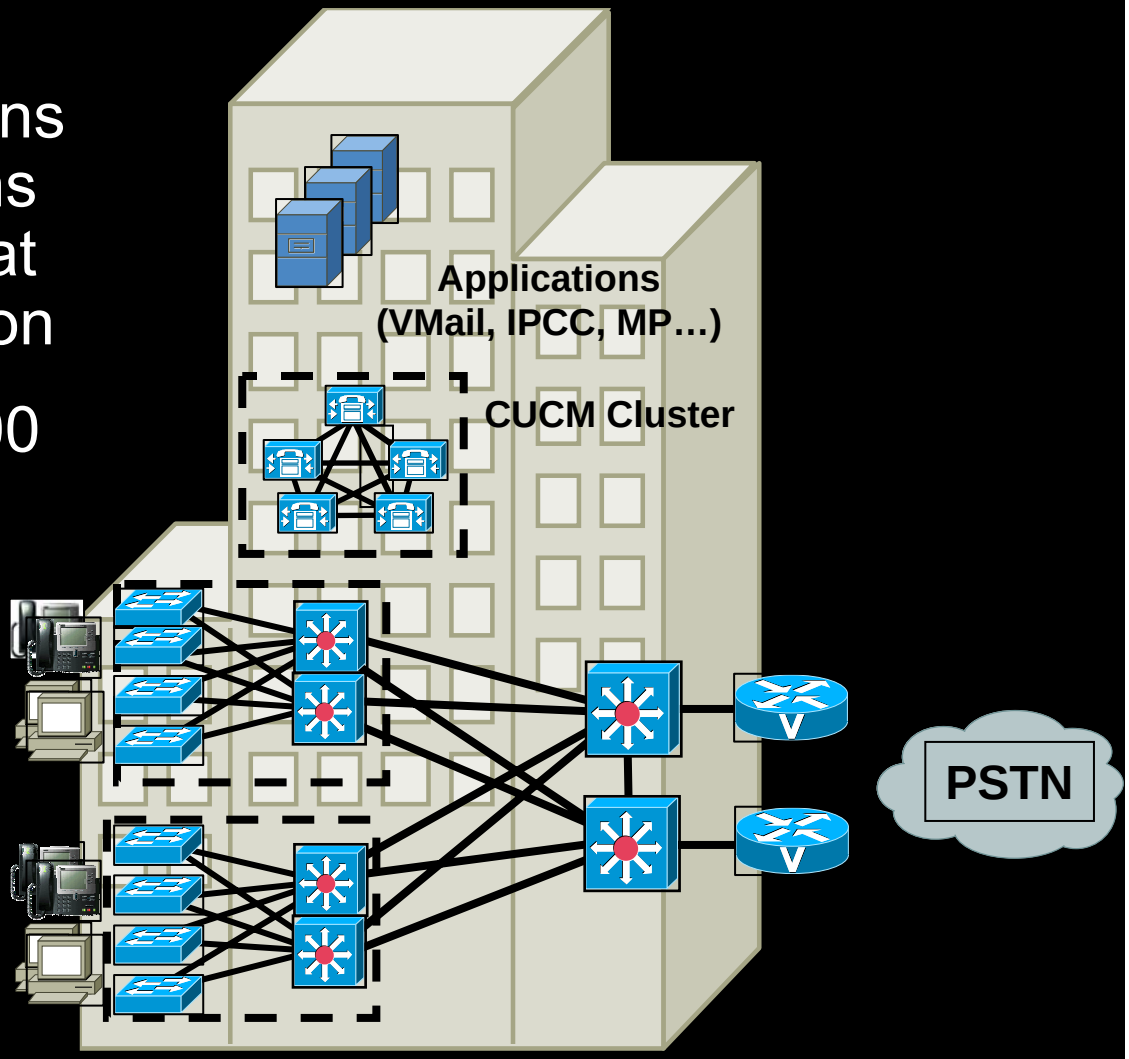
- The cluster appears as one entity, with a single point of administration (the publisher)
- Several functions can be collocated on the same server, depending on cluster size and server type
- Maximum of 19 subscribers per cluster (20 servers in a cluster)
- Maximum of 8 call processing servers per cluster
- Maximum of 7500 IP phones per Cisco Unified CM server (depending on server platform)
- Maximum of 30,000 IP phones per Cisco Unified CM cluster (depending on server platforms and configuration)

Unified Communications/Telephony Infrastructure Agenda

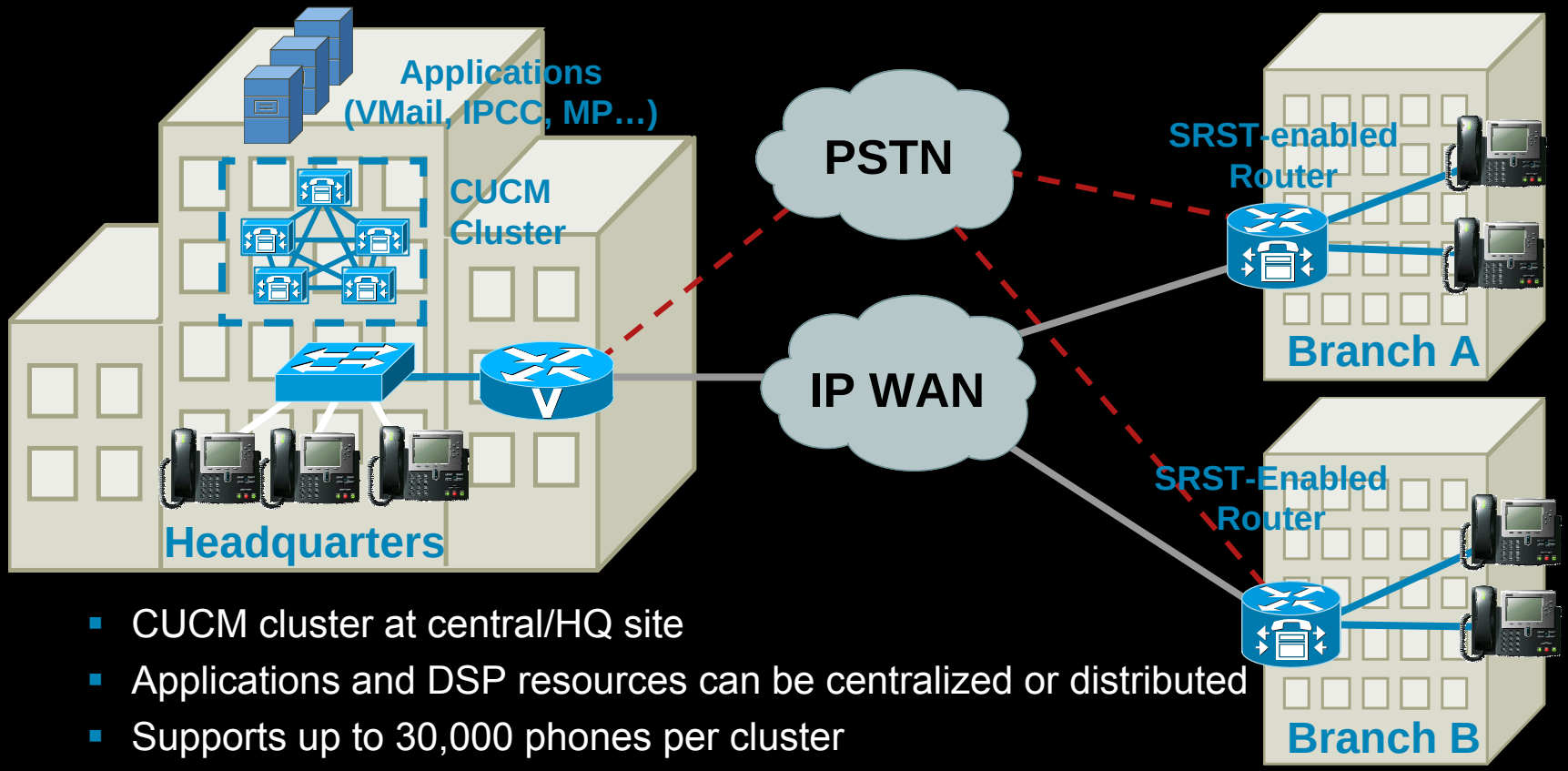
- Unified Communications/Telephony Infrastructure
  - Network Services
  - Cisco Unified Communications Cluster
  - Deployment Models
  - Basic Call Processing
  - Signaling Protocols
  - Failover and Redundancy

Deployment Models
Single Site

- Cisco Communications Manager, applications and DSP resources at same physical location
- Supports up to 30,000 phones per cluster
- PSTN used for all external calls

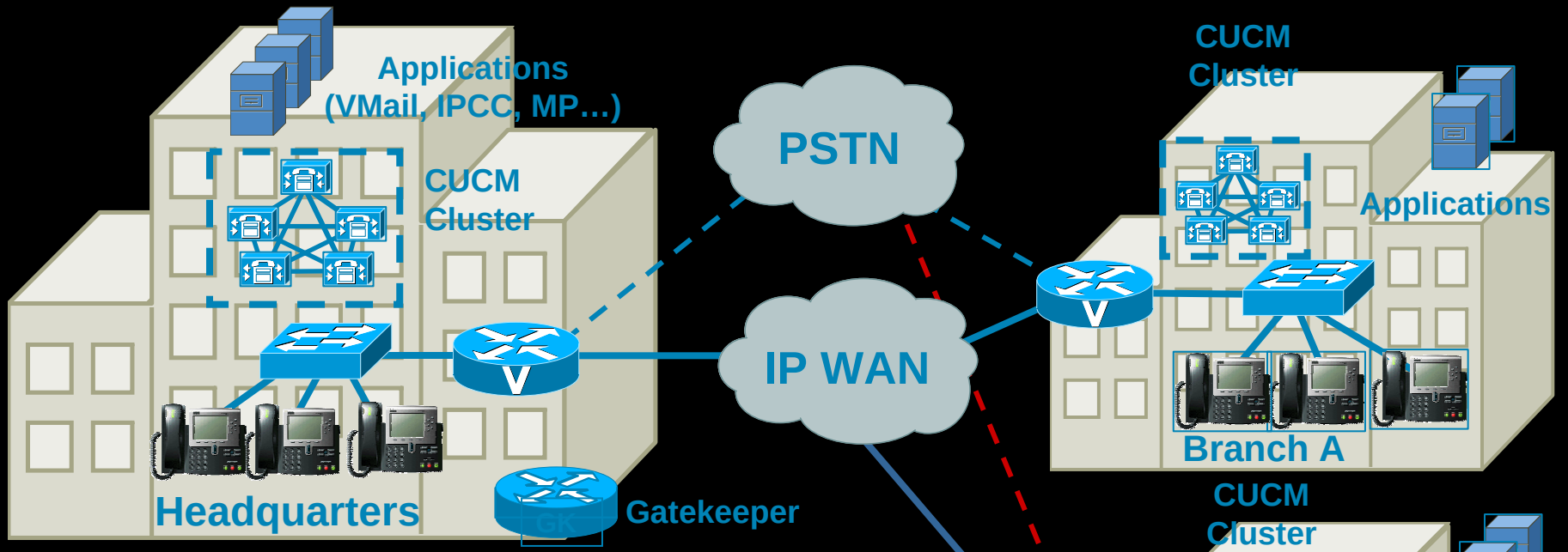


Deployment Models
Centralized Call Processing



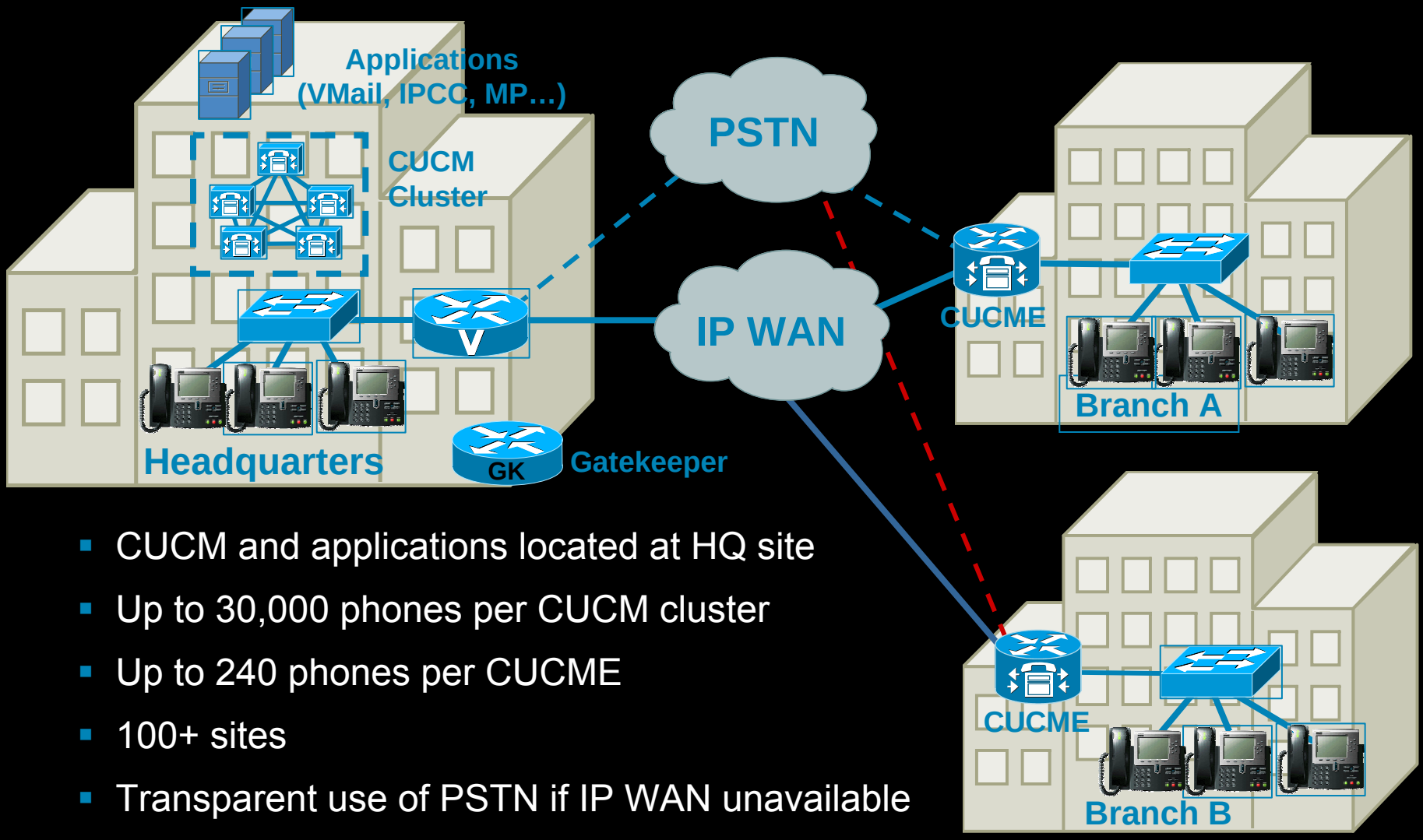
- CUCM cluster at central/HQ site
- Applications and DSP resources can be centralized or distributed
- Supports up to 30,000 phones per cluster
- If WAN is “busy”, transparent use of PSTN (AAR)
- Survivable remote site telephony for remote branches
- Maximum 1000 branches per cluster (500 branches before CUCM 6.0)

Deployment Models
Distributed Call Processing (CCM Model)



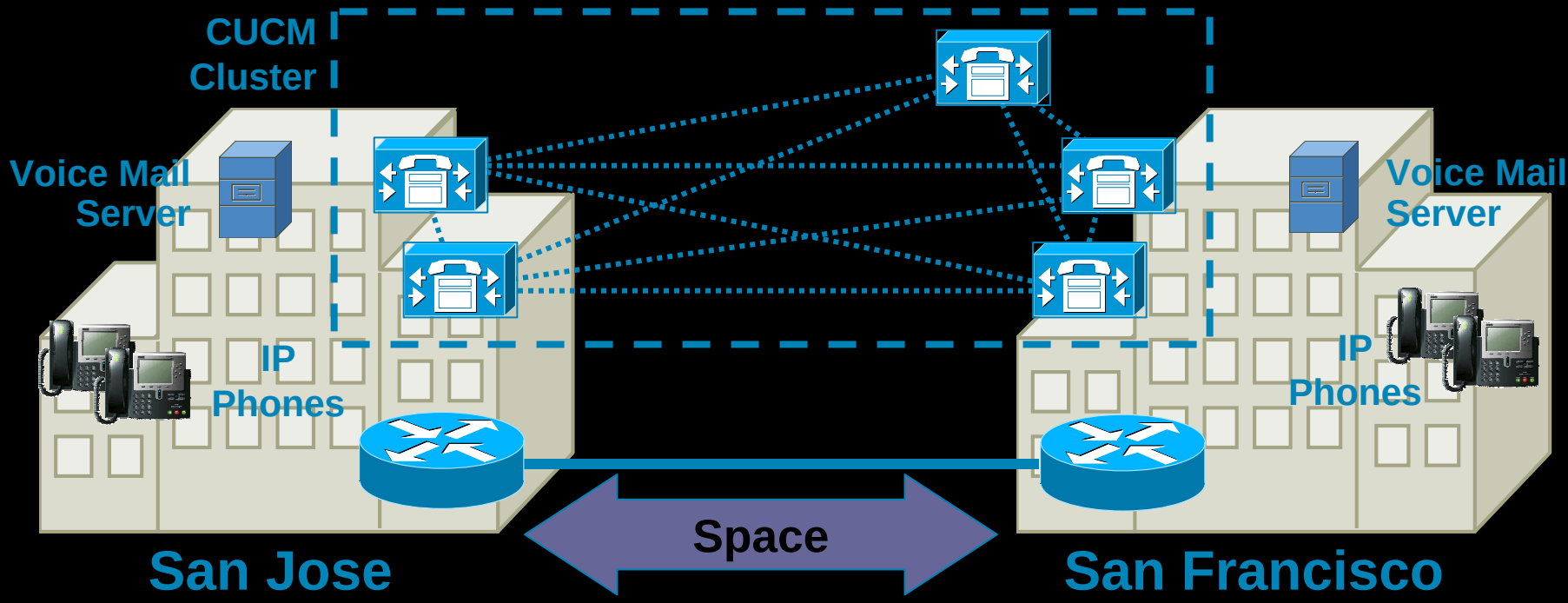
- CUCM and applications located at each site
- Up to 30,000 phones per cluster
- 100+ sites
- Transparent use of PSTN if IP WAN unavailable
- Each cluster can be single site or centralized call processing topology

Deployment Models
Distributed Call Processing (CCM-CME Model)



- CUCM and applications located at HQ site
- Up to 30,000 phones per CUCM cluster
- Up to 240 phones per CUCME
- 100+ sites
- Transparent use of PSTN if IP WAN unavailable

Deployment Models
Clustering over the WAN (COW)



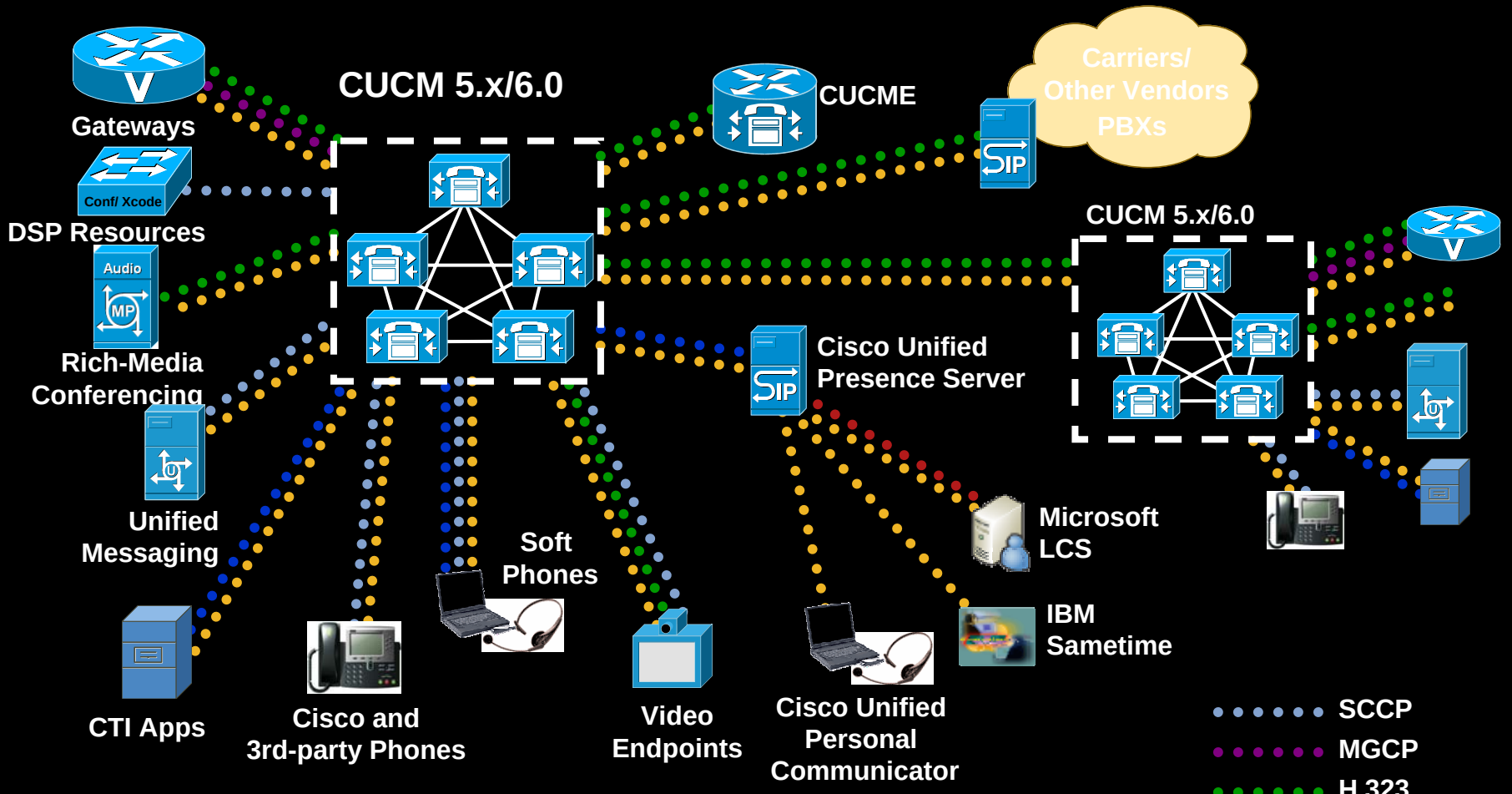
- CUCM servers in a cluster separated by WAN for spatial redundancy
- Applications may be located at each site, thus separated by WAN
- Single point of administration, feature transparency (e.g. Extension Mobility), Unified Dial Plan
- Max 40-ms round-trip delay between any two CUCM across the WAN
- 900 kbps bandwidth for each 10,000 BHCA between sites
- Maximum of 8 active locations

Unified Communications/Telephony Infrastructure Agenda

- Unified Communications/Telephony Infrastructure
  - Network Services
  - Cisco Unified Communications Cluster
  - Deployment Models
  - Signaling Protocols
  - Failover and Redundancy

Unified Communications Infrastructure

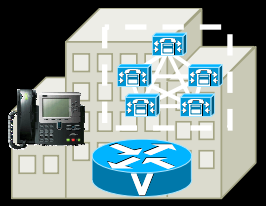
Signaling Protocols



Cisco Unified Communications integrates rich, native SIP and SIMPLE support on both line-side and trunk-side interfaces with integrated presence on phones and applications while maintaining seamless inter-working with existing H.323, MGCP, SCCP, TAPI/JTAPI and Q.SIG protocols

Gateway Protocol Deployment Considerations

Large/Campus Sites



- Characteristics of larger site(s)—often best served by MGCP
- High-density GWs to PSTN, often PRI
- Dedicated GW platforms
- Caller ID/name delivery required
- QSIG connectivity (with supplementary services) to legacy PBXs required
- Other considerations
  - NFAS is H.323/SIP only
  - Very high density GWs such as T3 (5x00) are H.323/SIP only

Small/Branch Sites

- Characteristics of branch site(s)—often best served by H.323/SIP
- Low-density GW to PSTN, often analog
- Caller ID on analog FXO required
- Mixes of PSTN TDM protocols required (FXO, A-DID, BRI, Frac-PRI)
- CVP/VXML application control
- Other considerations
  - Can mix H.323 and MGCP on the same GW (not on same voice port)
  - H.323 dial-peers are needed anyway for MGCP GW Fallback

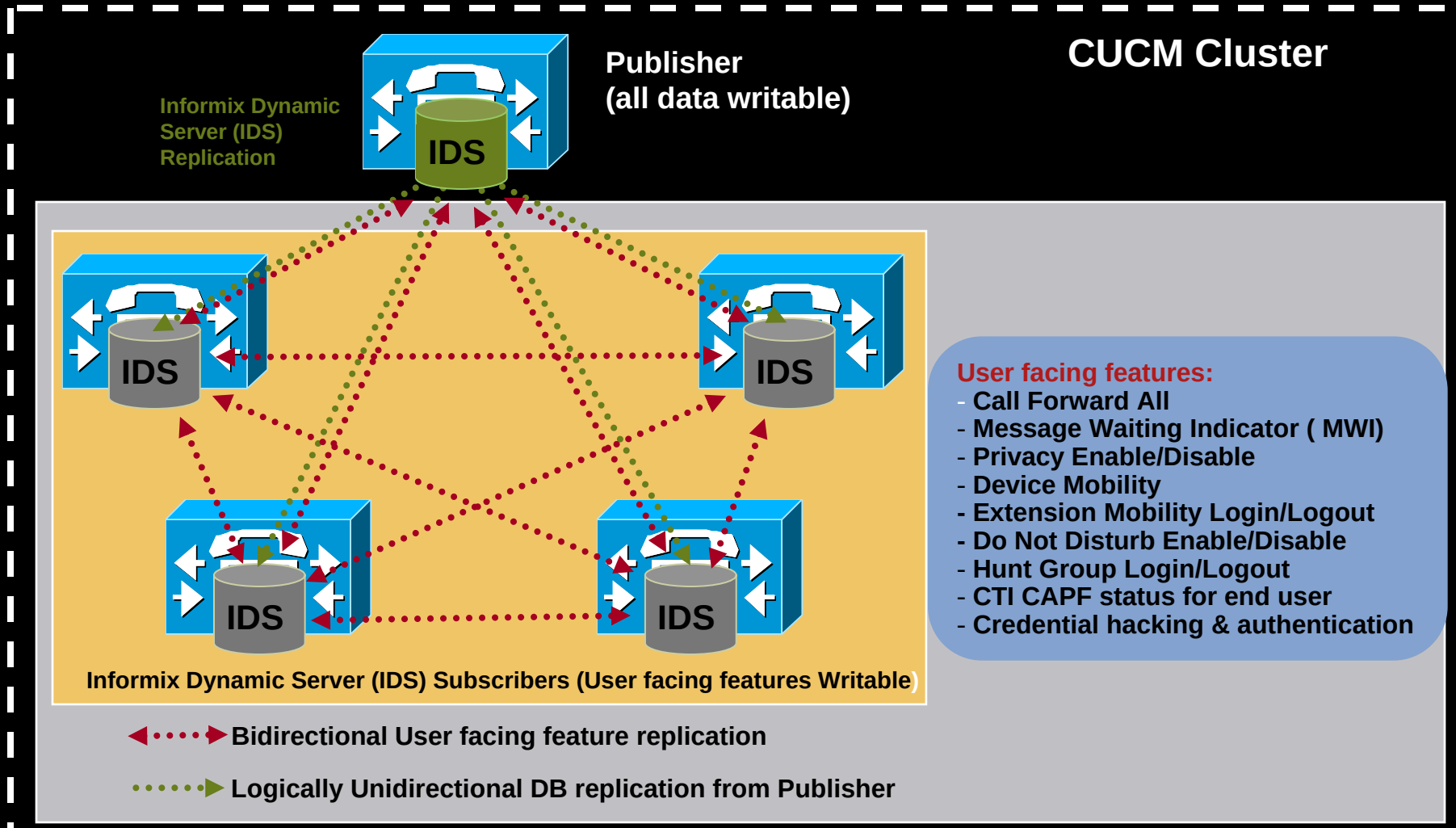
Gateway Protocol and Platform Summary

Gateway Platform	Line Side	Trunk Side		
	SCCP (FXS)	H.323	SIP	MGCP (CUCM)
VG224	Yes	Yes	Yes	Yes
VG248	Yes	No	No	No
1751/60	No	Yes	Yes	Yes
2600XM, 2691	No	Yes	Yes	Yes
2800	Yes	Yes	Yes	Yes
3700	No	Yes	Yes	Yes
3800	Yes	Yes	Yes	Yes
5x00	No	Yes	Yes	No
7x00	No	Yes	Yes	No
Cat 6K CMM	No	Yes	Yes	Yes

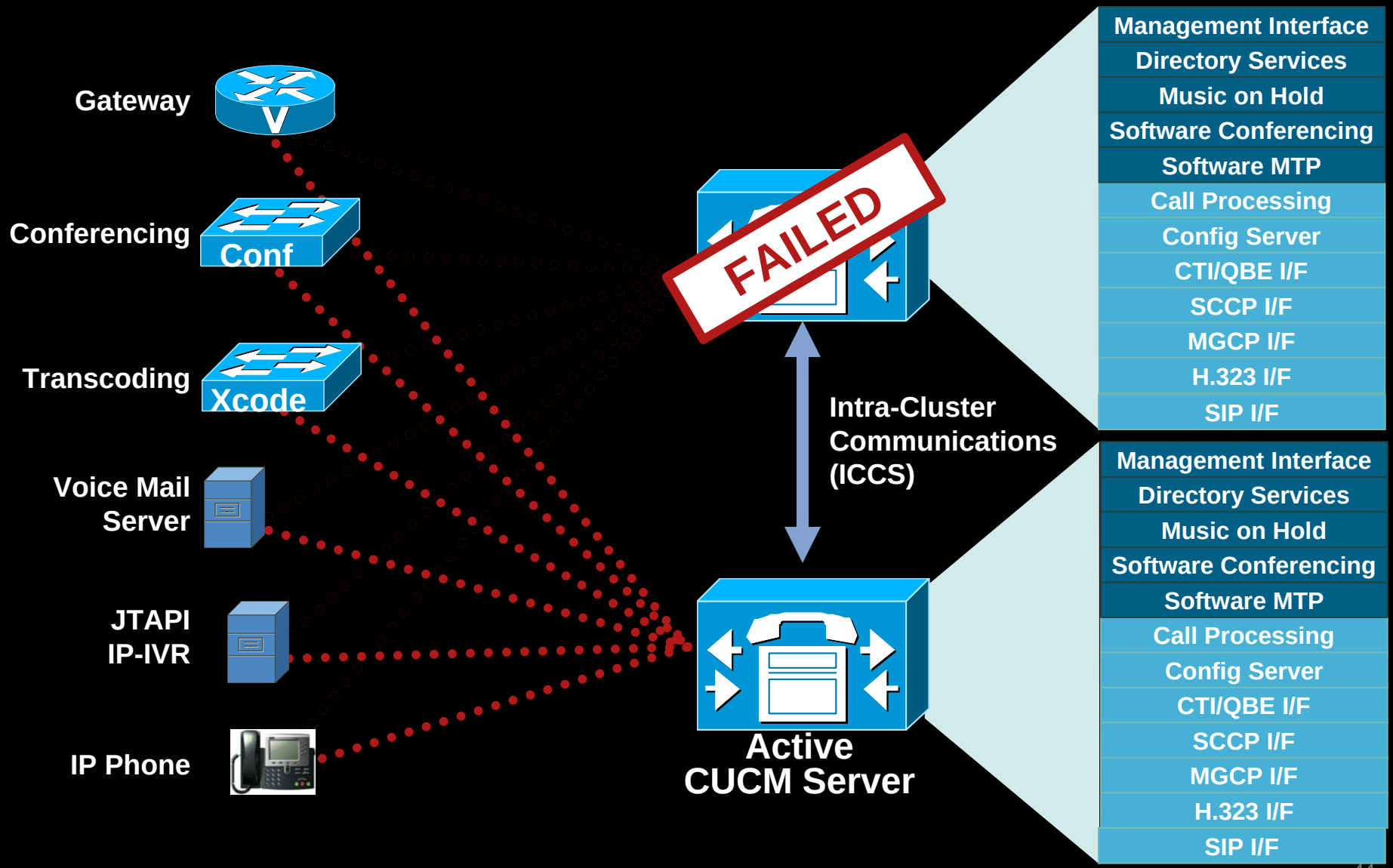
Unified Communications/Telephony Infrastructure Agenda

- Unified Communications/Telephony Infrastructure
  - Network Services
  - Cisco Unified Communications Cluster
  - Deployment Models
  - Signaling Protocols
  - Failover and Redundancy

Failover and Redundancy
Database Resiliency (CUCM version 6.0)

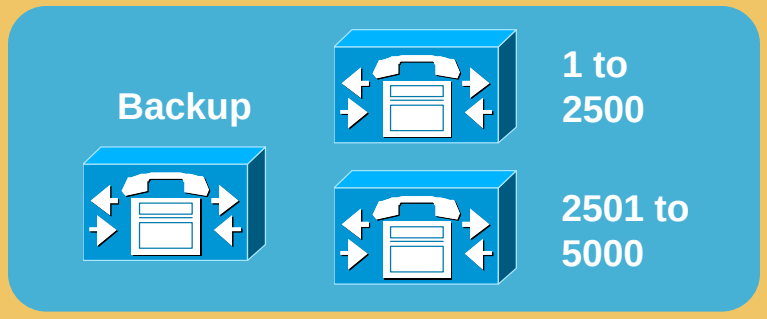


Failover and Redundancy
Server Redundancy



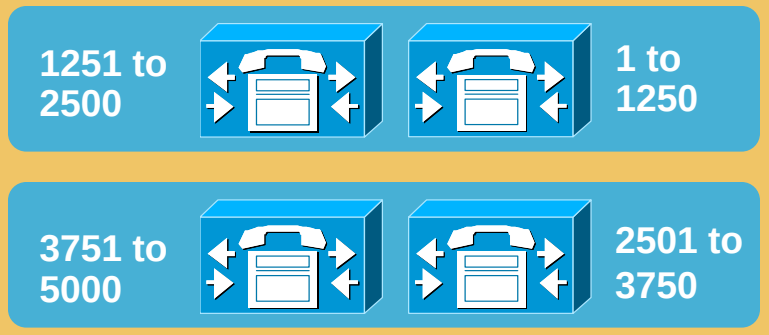
Failover and Redundancy
1:1 vs. 2:1 Redundancy Scheme

2:1 Redundancy Scheme



- Cost-efficient redundancy
- Degraded service during upgrades
- Maximum of 10,000 backup registrations

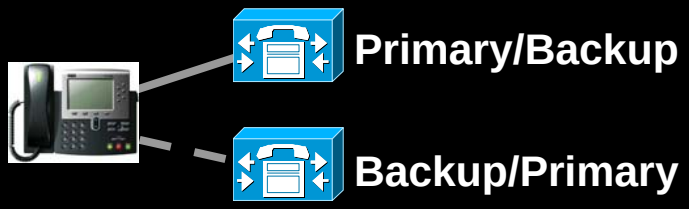
1:1 Redundancy Scheme



- High availability during upgrades
- Simplified configuration
- Load sharing
- Faster failover

Failover and Redundancy

1:1 Redundancy (CM 5.X/6.X and MCS 7845)



- MCS 7845 supports 7500 phones/server
- Load-share between primary and backup servers

To 7,500 IP Phones

Publisher and TFTP Server(s)

1 to 3750: Primary
3751 to 7500: Backup

3751 to 7500: Primary
1 to 3750: Backup

To 15,000 IP Phones

Publisher and TFTP Server(s)

3751 to 7500 — 1 to 3750

11,251–15,000 — 7501–11,250

To 30,000 IP Phones

Publisher and TFTP Server(s)

3751 to 7500 — 1 to 3750

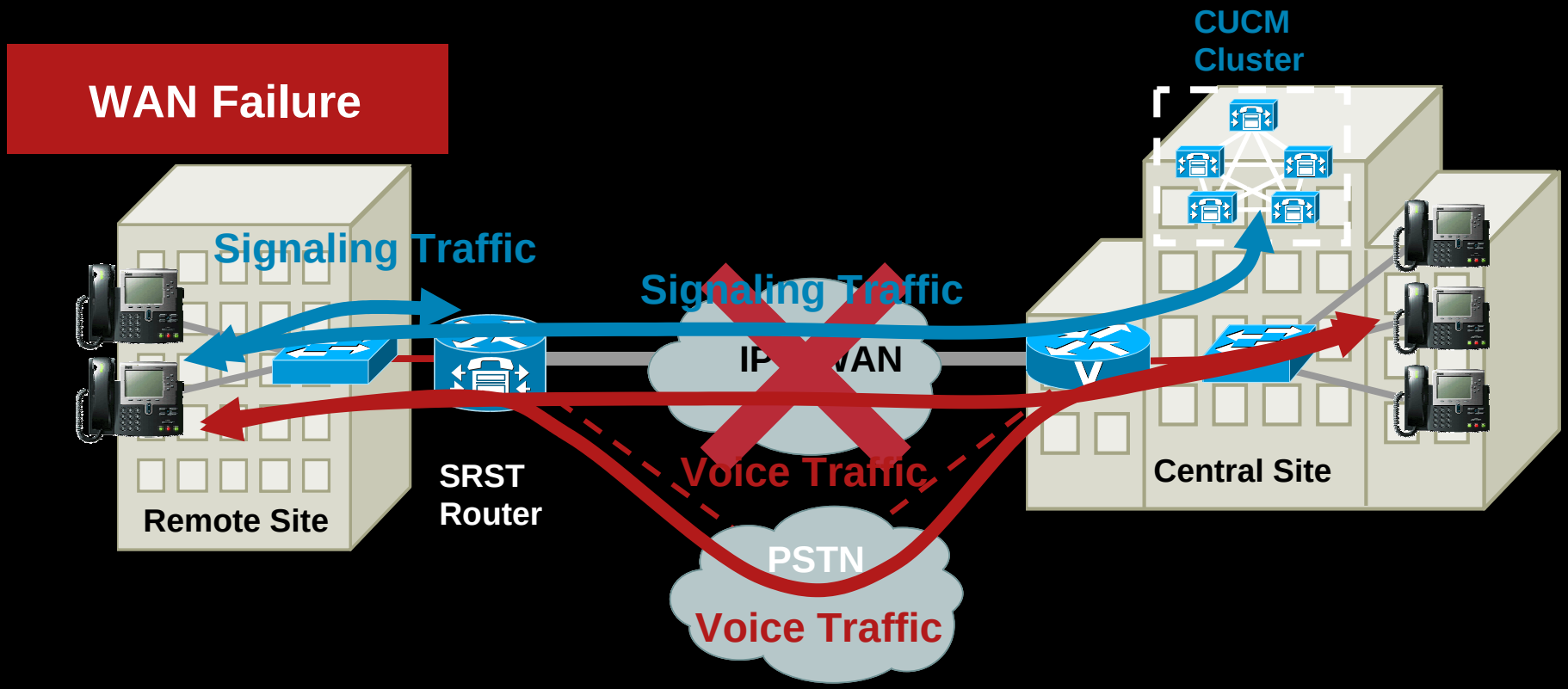
11,251–15,000 — 7501–11,250

18,251–22,500 — 15,001–18,250

26,251–30,000 — 22,501–26,250

Failover and Redundancy

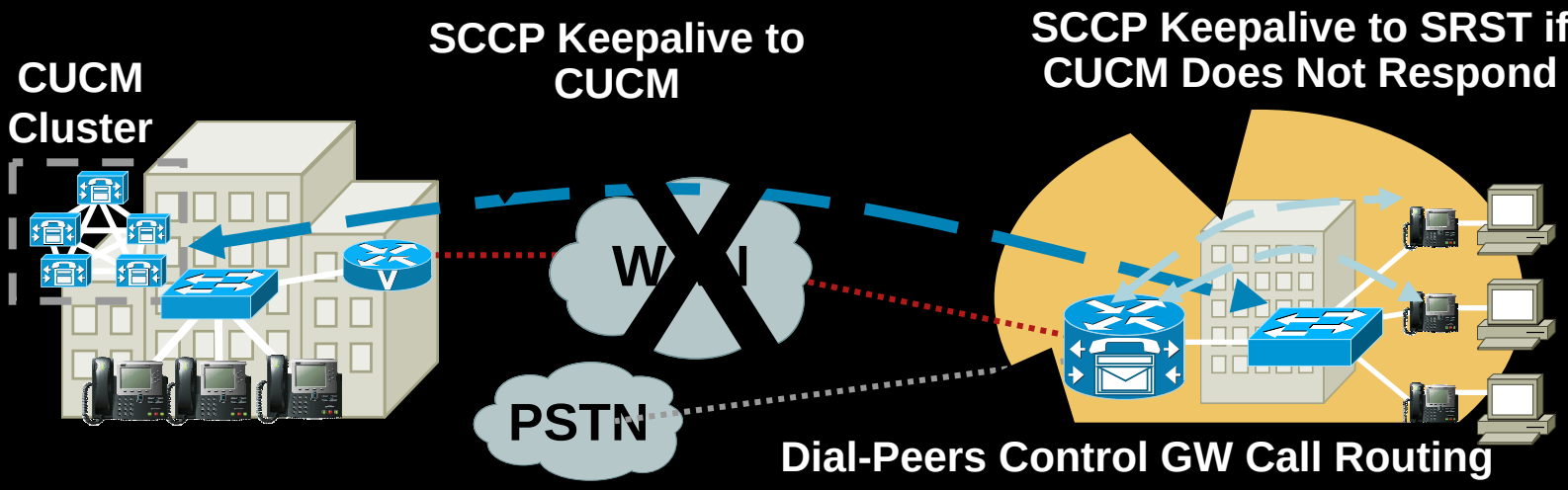
Voice over PSTN



- If WAN is unavailable, media can be sent over PSTN
- Subset of features available to the phones (DID, DOD, call hold, transfer, speed dial, caller ID)

IP Phone Failover
Survivable Remote Site Telephony (SRST)

- Phones have list of backup Cisco Unified CMs to fail over to in case of no response to keepalives
  - SRST is the “Cisco Unified CM of last resort” in the phone list
- SRST only controls IP phone connectivity—it does not provide or control GW connectivity or availability
- PSTN GW connectivity during failure modes:
  - POTS/VoIP dial-peers
  - MGCP GWs requires the MGCP GW failover feature
  - Calls from IP phones (under SRST) access the dial-peers to route calls



IOS GW Audio Preservation Summary

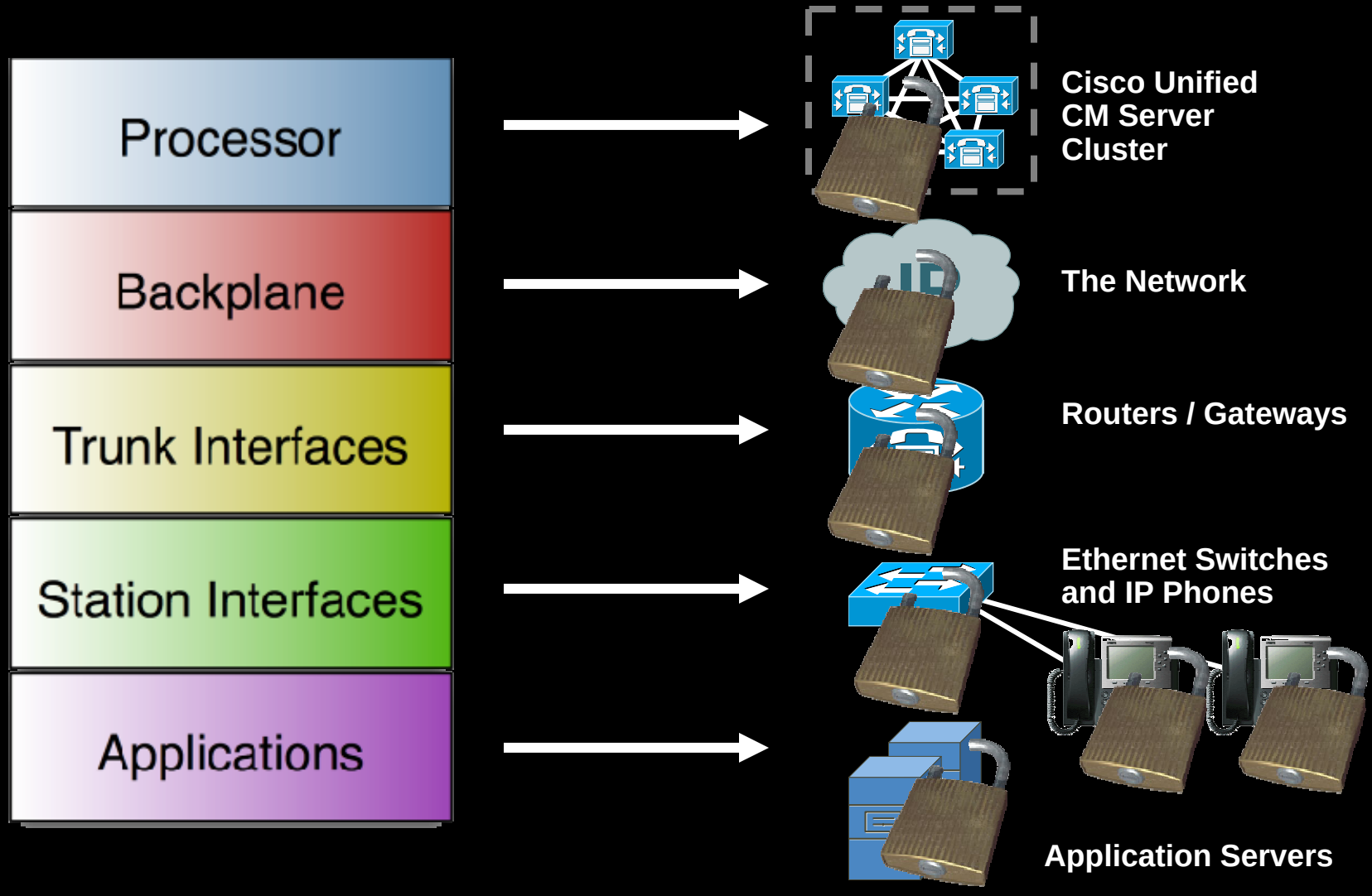
		H.323	MGCP
Primary-to-Secondary CUCM Failover		12.4.4XC/12.4.9T, CUCM4.1.3-SR2 preserve	Preserved
CUCM to SRST	ISDN	Preserved (Disable TCP timer)	Fail
	Non-ISDN		Preserved
Flapping Links		12.4.4XC/12.4.9T, CUCM4.1.3-SR2 preserve	Failures Depend on Timing
VXML Calls in Queue		TCL Script to Reroute to SRST Hunt-Group	N/A

- Audio is preserved with no supplementary services
- Audio is preserved as long as the RTP stream is not interrupted by the failure
- SIP is still being tested—behaves like H.323

Agenda

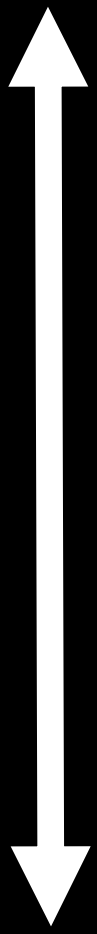
- Network Infrastructure
- Unified Communications/Telephony Infrastructure
- Security and Management

The Secure Network Is the System



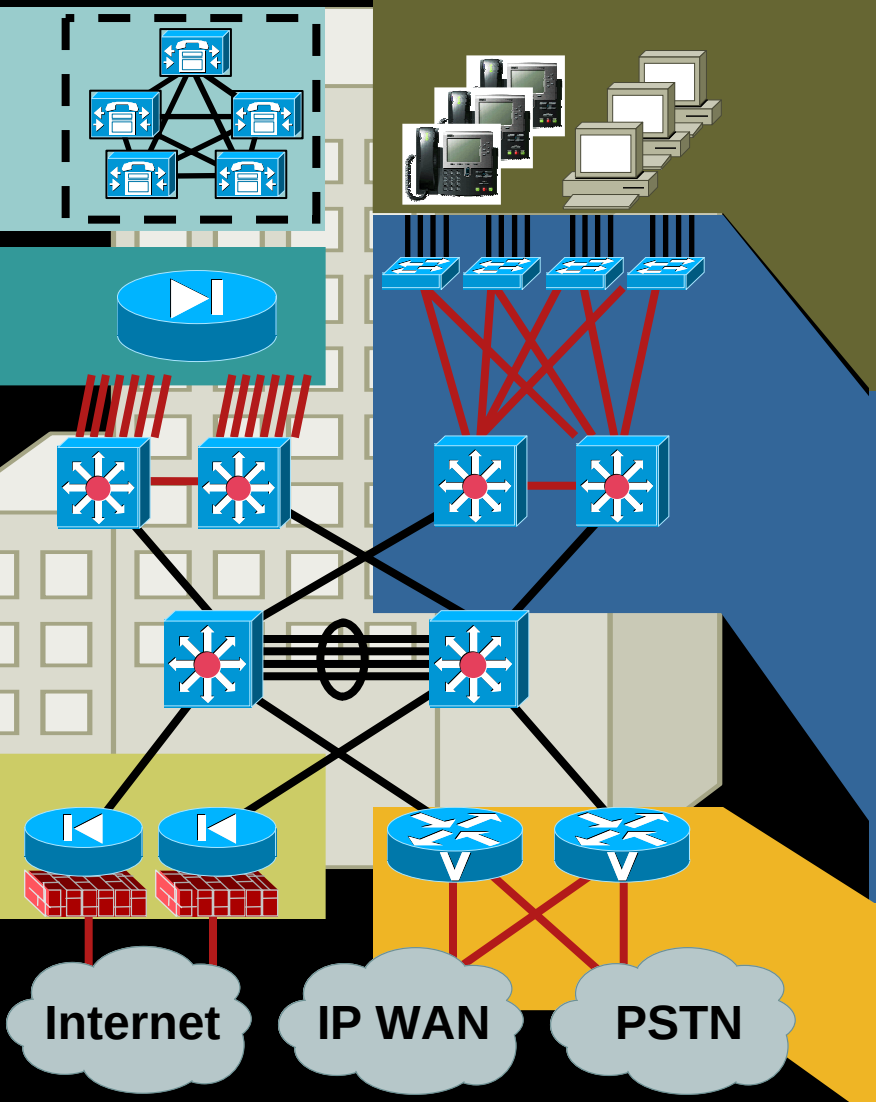
Voice Is Data

- Don’t make security an end to itself.
- Rank voice by your business requirements
- Evaluate whether your existing security policy for data is sufficient for voice.



Banking
Oracle
Trading
Billing
POS
Voice
Web Traffic
E-Mail
Directory

Cisco Security—Built in Layers



Cisco Unified CM

- Hardened OS
- Minimize Win2K services
- MLA
- HIPS/antivirus

Firewall or ACLs

- Allow only call control, LDAP, management
- Control source addresses

Outside World

- Use Cisco IOS DoS tools
- Use V3PN
- Network IDS

Endpoints

- Separate voice and data VLANS
- Disable GARP and voice VLAN on PC port
- Authentication and Encryption

Campus Network

- High availability
- Layer 2/3 security
- IP filters between voice and data
- Policers
- Secure access (TACACS+, SSH..)
- OOB Management

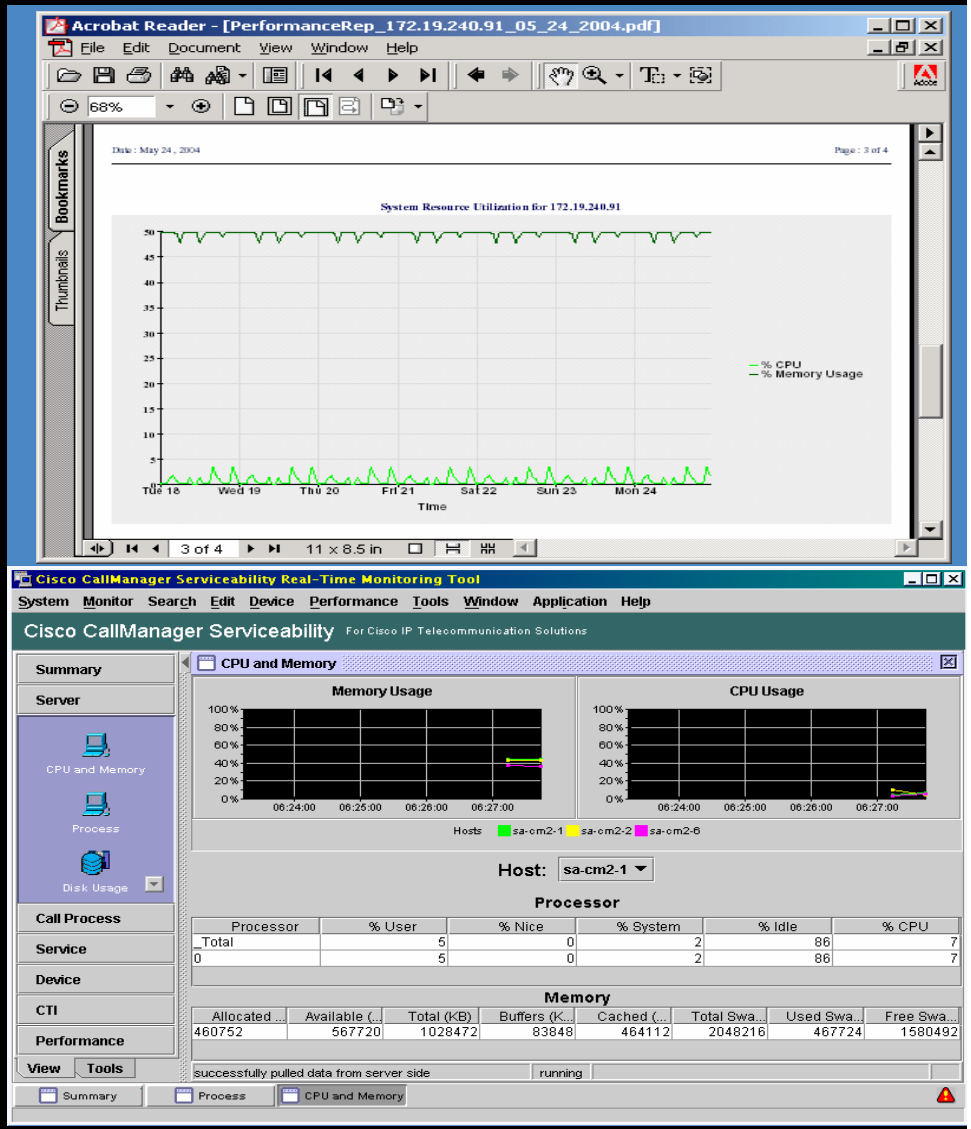
- Toll fraud
- Transfer to outside line

Unified Communications Security and Management

- Security
- Management
  - Real Time Monitoring Tool
  - Cisco Unified Provisioning Manager
  - Cisco Unified Operations Manager
  - Cisco Unified Service Monitor
  - Cisco Unified Service Statistics Manager

Management
Real Time Monitoring Tool

- Built in CUCM
- Windows and Linux Client
- Integrated Trace and Syslog Viewer
- HTTPS Support
- OS monitoring
- CUCM Pre-canned DB Activity
- SIP Phone/Protocol Activity



Cisco Unified Communications Management Suite

Plan and Design

Assess/prepare network for IP Communications

- Hardware/software compliance
- Predict overall call quality
- Best practice analysis

Implement

Provisioning Manager

Deploy and provision

- Voice infrastructure provisioning
- Dial plans & partitioning
- Batch provisioning

CiscoWorks Voice Manager

GW/GK Configuration

- Voice port configuration
- GW/GK dial plans

Operate

Provisioning Manager

Manage moves, adds, changes

- Endpoint devices
- Users, services
- Phones, lines, voicemail, …

Service Statistics Manager

- Executive & Operations reports
- Capacity planning reports

Service Monitor

Track and report on user experience

- Voice quality using sensors and phones
- Reporting & SLAs
- Video support

Operations Manager

Monitor and diagnose problems

- Service-level views
- Proactive testing including SCCP & SIP phones
- Track inventory, changes
- Video endpoint support
- Phone-Phone testing
- Mobility support

Q and A