DESIGNING AN ENTERPRISE IP TELEPHONY NETWORK

Session TECVVE117

Networkers Solution Forum Chile

Presenters:

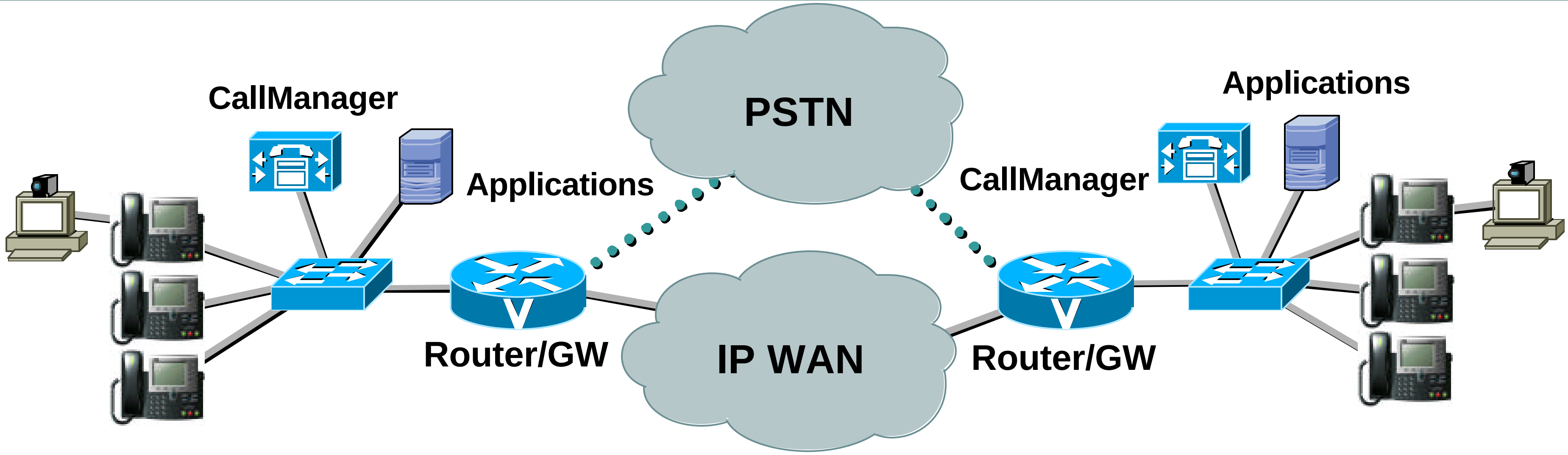
Mariano O'Kon	Voice CCIE	okon@cisco.com
Jeff Seifert	Voice CCIE	jseifert@cisco.com

Agenda

- Introduction
- Network Infrastructure
- Telephony Infrastructure
- Legacy Migration and Integration

Scope of This Seminar

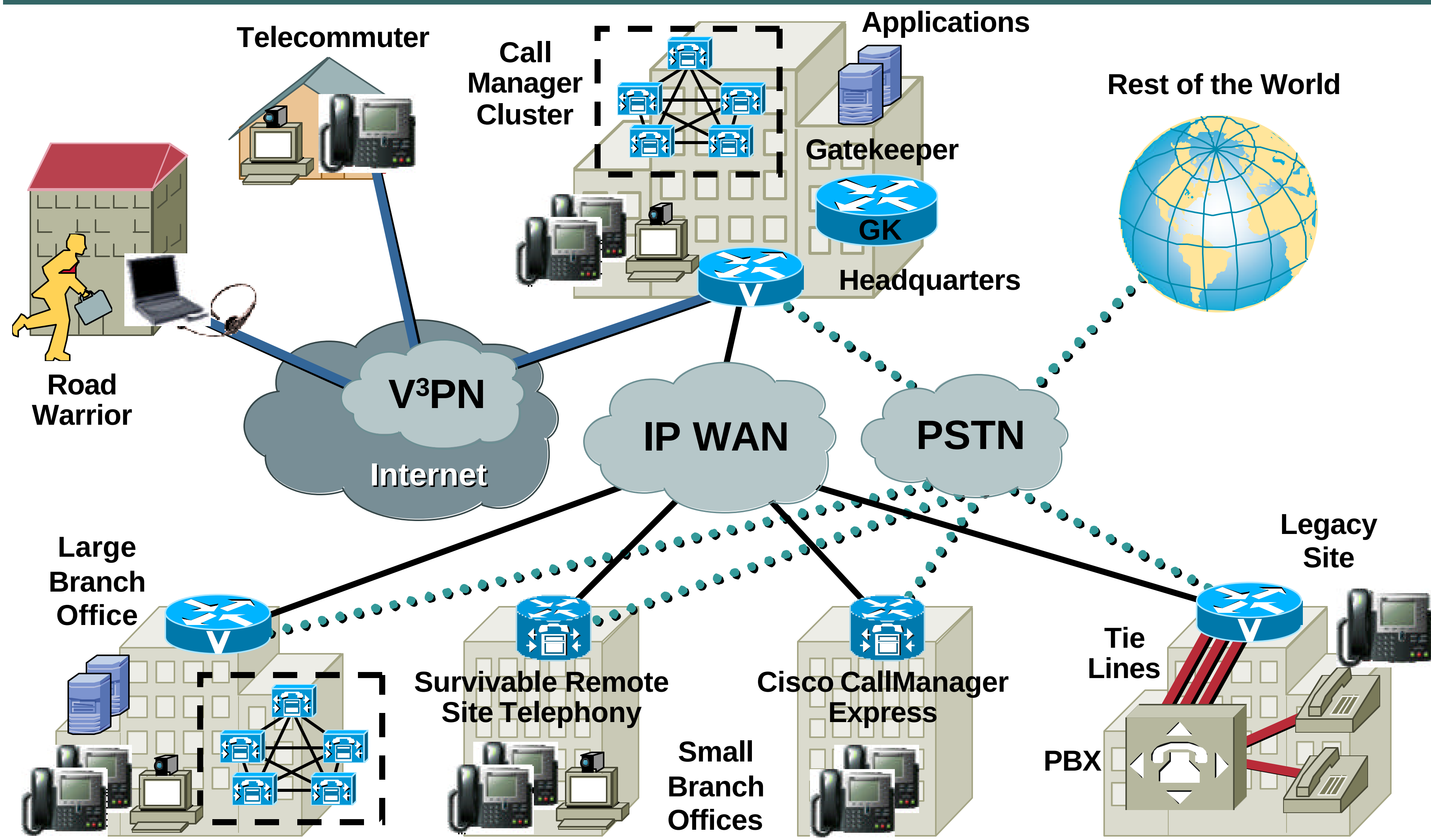
Cisco.com



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

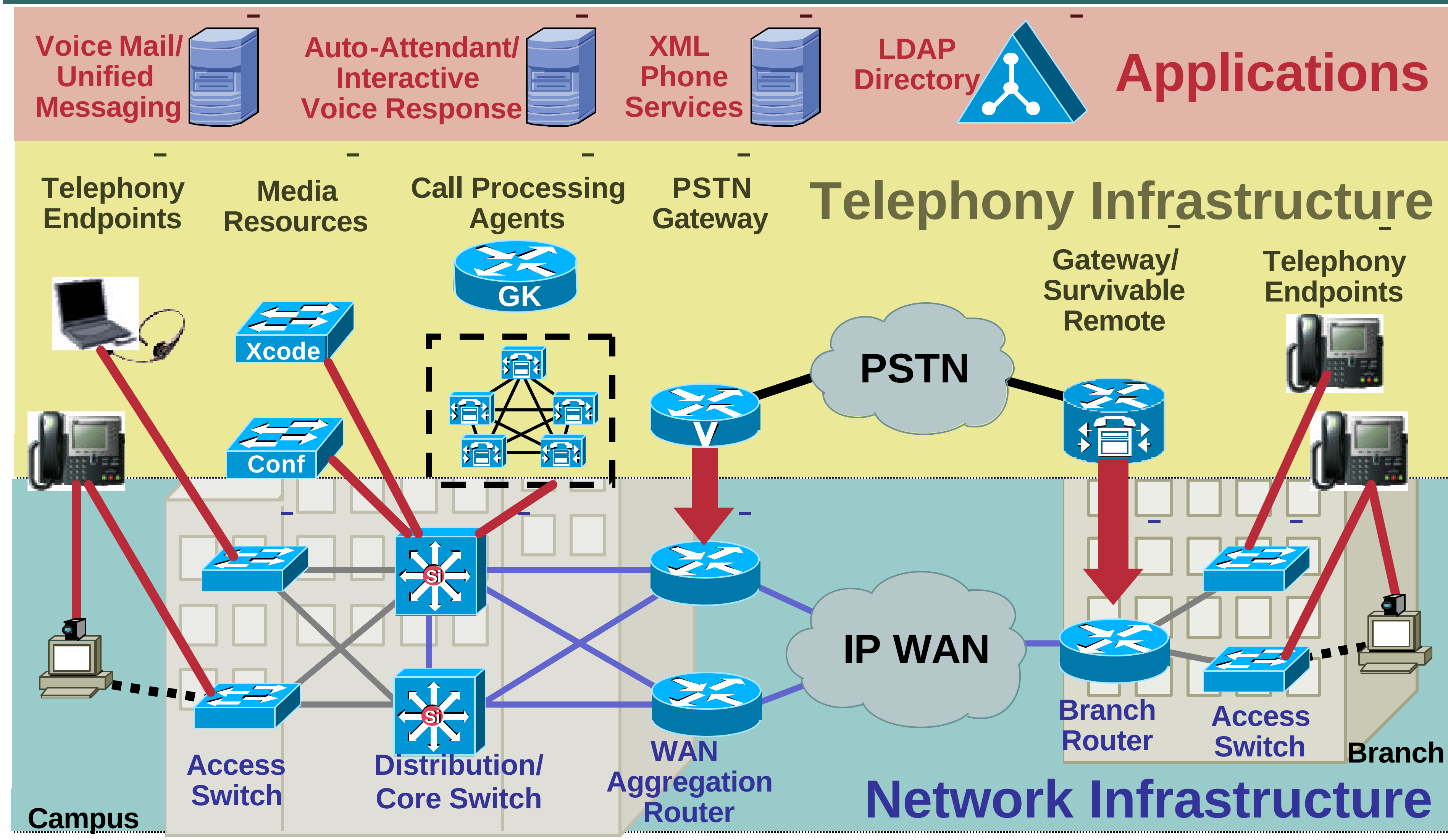
  http://www.cisco.com/go/srnd/

The Big Picture: End-to-End IP Telephony



The Elements of IP Telephony

Cisco.com



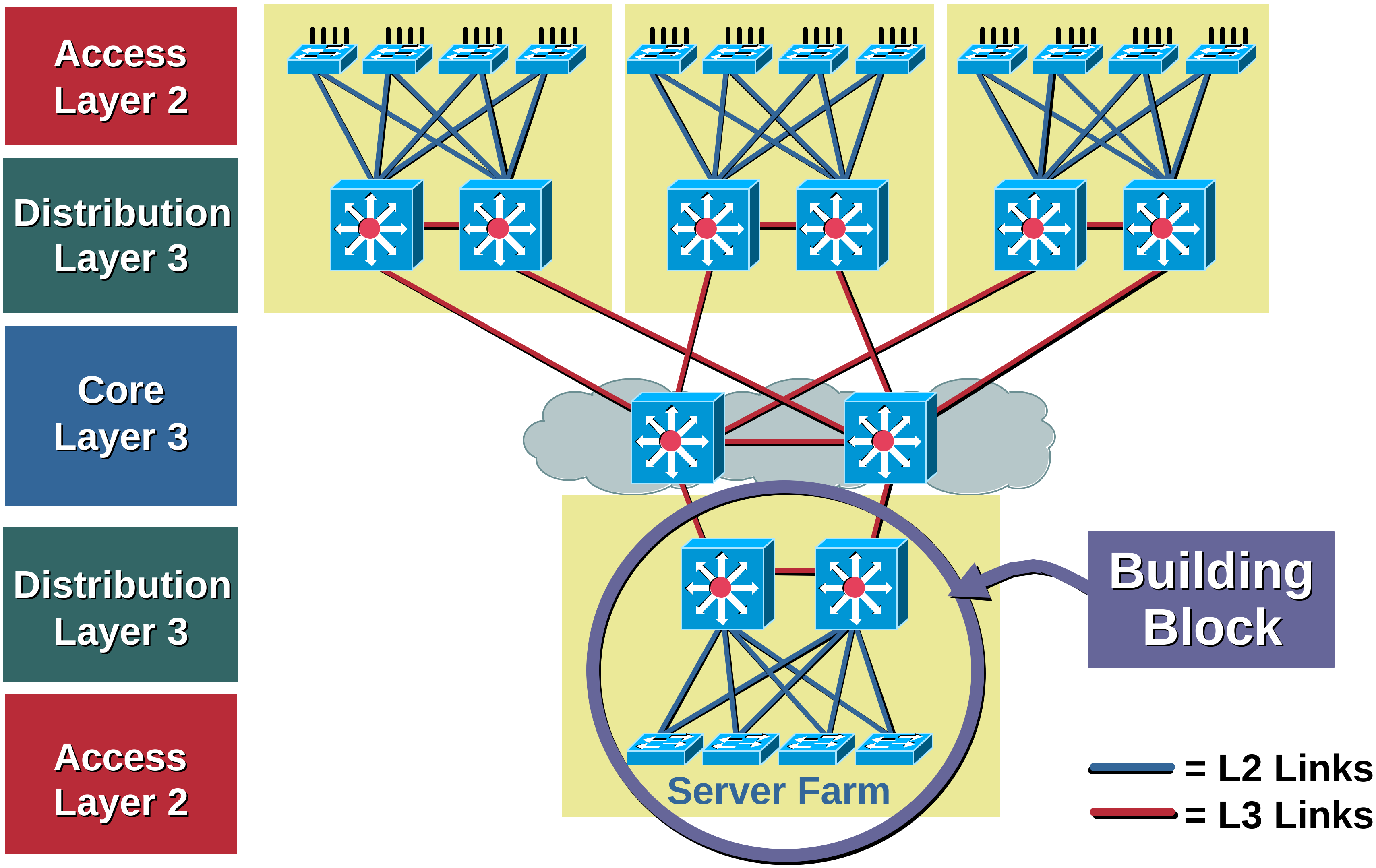
Agenda

- Introduction
- Network Infrastructure
- Telephony Infrastructure
- Legacy Migration and Integration

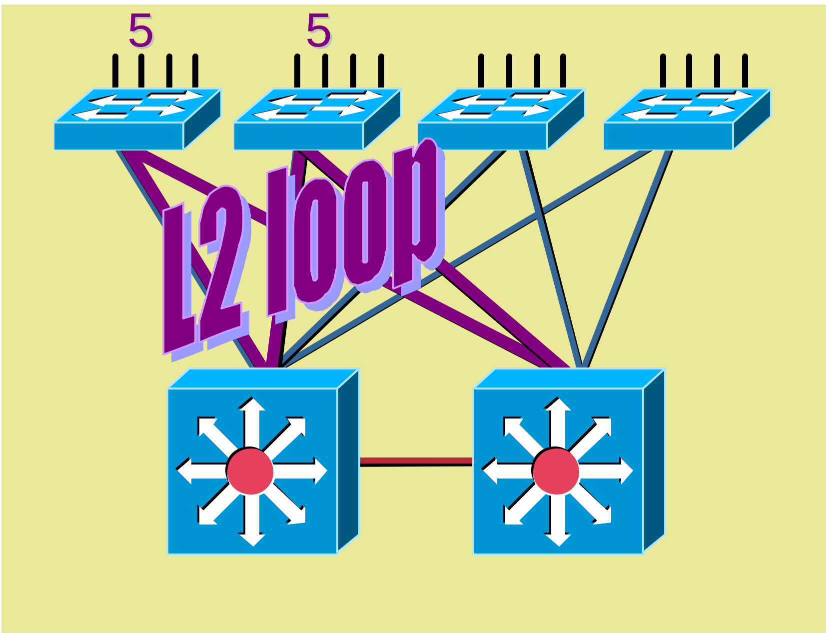
Network Infrastructure Agenda

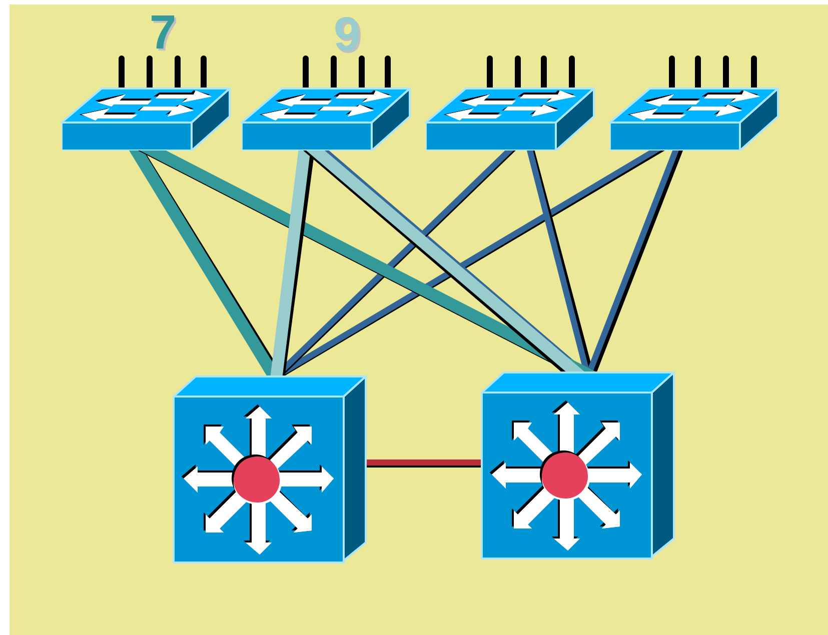
- Building a Campus Network
- Enabling QoS in the Campus
- Providing Inline Power to IP Phones
- Overlaying Wireless LANs
- Building a WAN
- Enabling QoS in the WAN
- Networks Services

Building a Campus Network
Multilayer Network Design



Building a Campus Network
VLAN Model



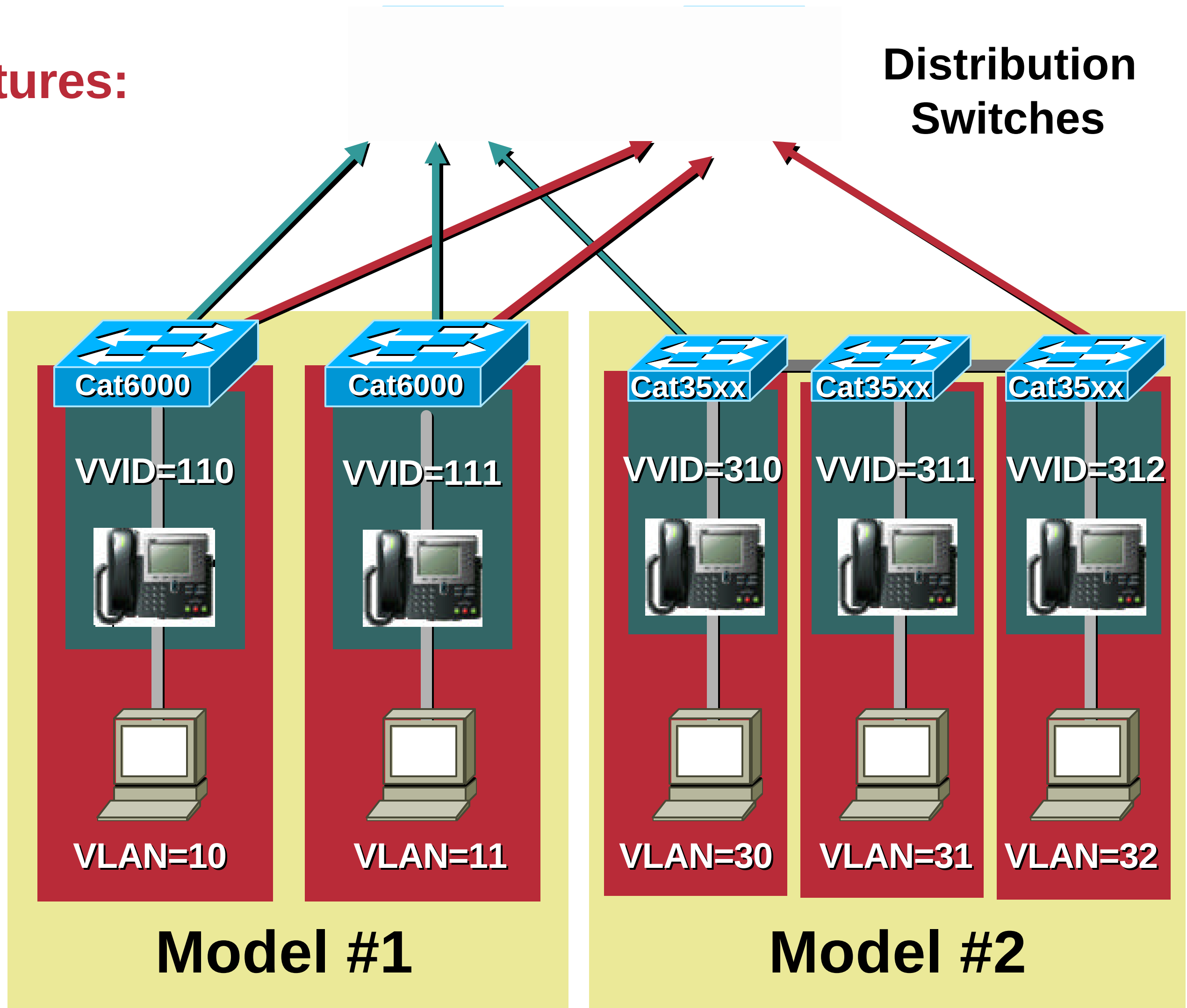


- **A VLAN = an IP subnet**
- **VLANs do <u>not</u> span different wiring closet switches**
- **If 2+ VLANs per access switch, load sharing is very easy to achieve**
- **This model achieves fast convergence and high stability**
- **Topology could be used for voice VLANs while existing data VLANs are left untouched (only if need be)**

Building a Campus Network Access Layer

Wiring Closet Features:

- Auxiliary VLAN
- 802.1p/Q
- STP PortFast
- RootGuard
- UDLD
- UplinkFast
- BackboneFast
- *Rate policing*
- *Conditional trust*

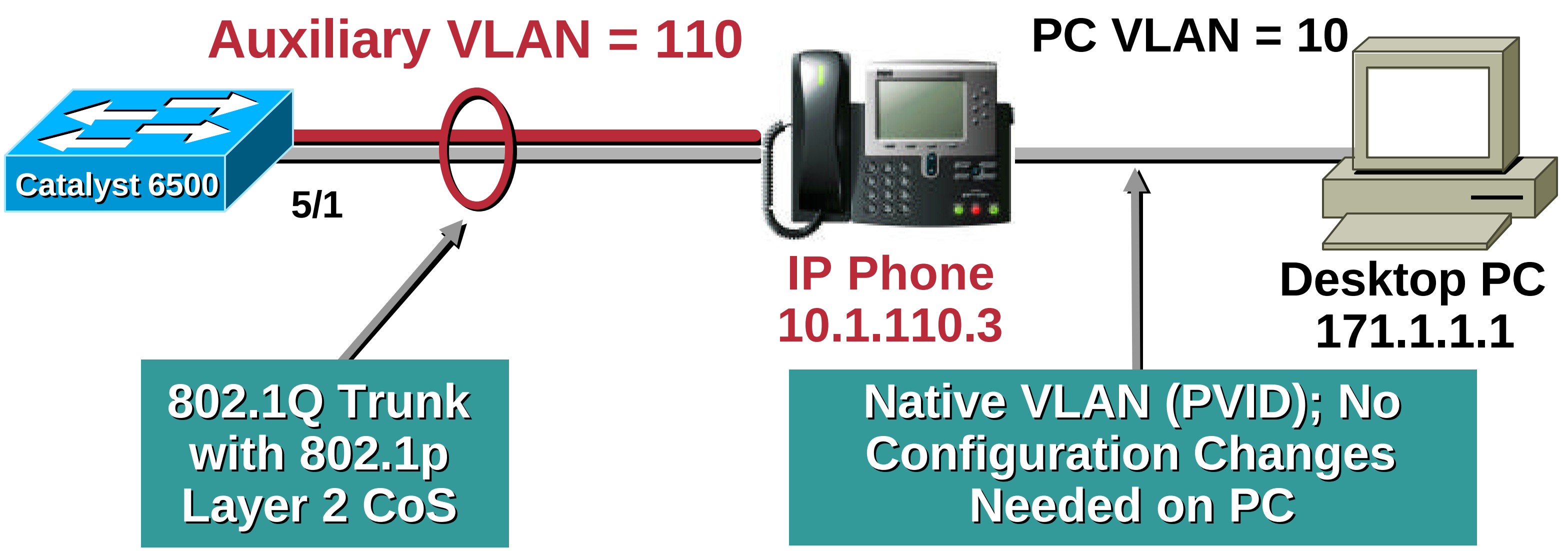


IEEE 802.1w/s

- **802.1w—Rapid Spanning-Tree Protocol (RSTP)**
  - Enhances STP convergence speed
  - Similar to Cisco's implementation of 802.1D with STP extensions like PortFast, UplinkFast and BackboneFast
- **802.1s—Multiple Spanning-Tree (MST)**
  - Runs logical instances of STP
  - Maps many VLANs to an instance
  - Reduces complexity of running a unique STP instance for every VLAN in the network

Building a Campus Network
Access Layer: Catalyst 6000 (Catalyst OS)

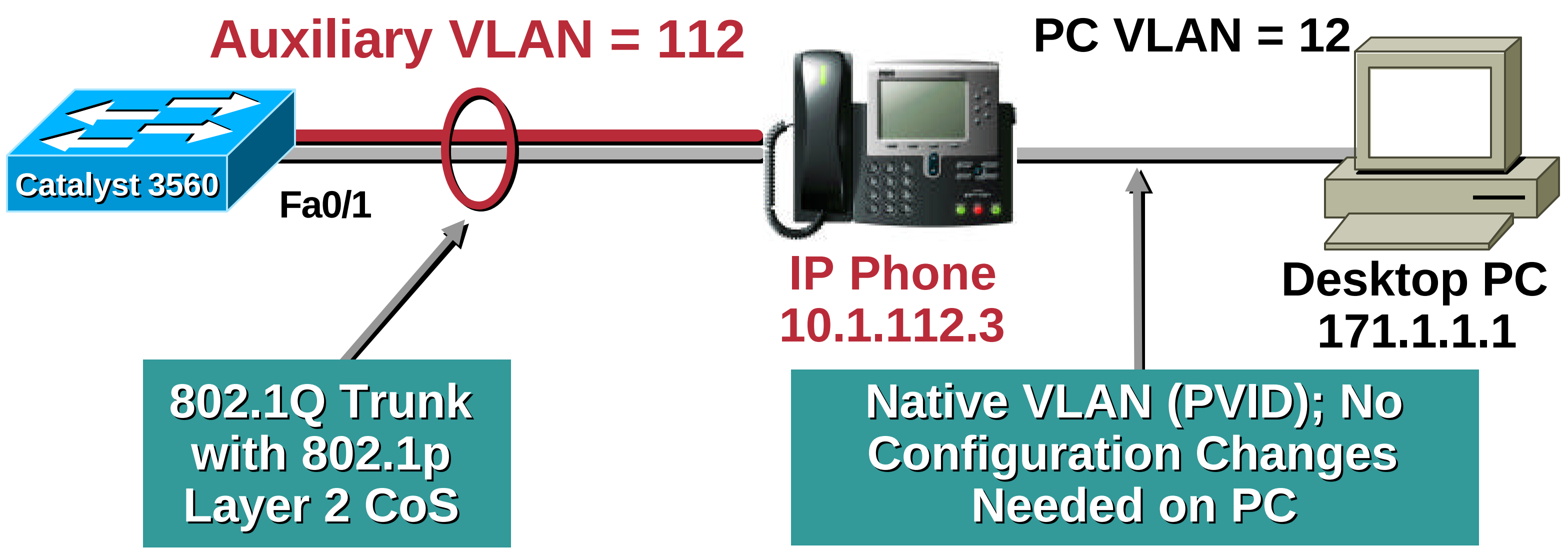
Cisco.com



Cat6500>(enable)set vlan 10 5/1-48 !Native vlan for untagged frames
Cat6500>(enable)set port qos 5/1-48 trust-device ciscoipphone !IP phone is a qos trust device
Cat6500>(enable)set port auxiliaryvlan 5/1-48 110 !Voice vlan for 802.1Q frames
Cat6500>(enable)set port qos 5/1-48 trust trust-cos !Trust the cos marking
Cat6500>(enable) set port qos 5/1-48 trust-ext untrusted !IP Phone port to override the cos value to 0 of the tagged frames received from the PC or the attached device

IPT and QoS SRND have details of other platforms (www.cisco.com/go/srnd)

Building a Campus Network
Access Layer: Catalyst 3560 (IOS)

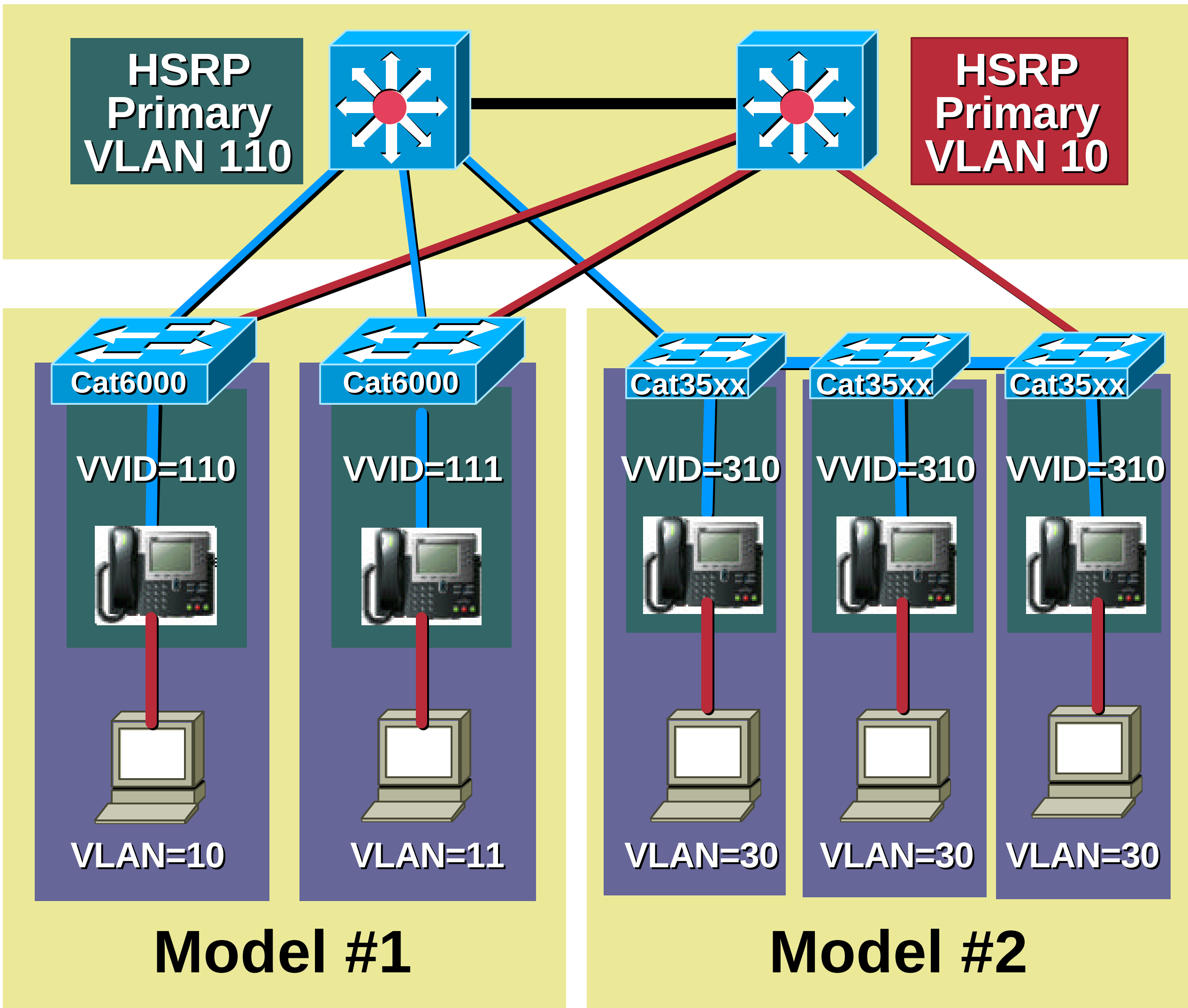


Cat3560(config)#interface interface fastethernet0/1
Cat3560(config-if)#mls qos trust device cisco-phone ***!IP phone is a qos trust device***
Cat3560(config-if)#mls qos trust cos ***!Trust the cos marking***
Cat3560(config-if)#switchport mode access ***!Set the port to access mode***
Cat3560(config-if)#switchport voice vlan 112 ***!Voice vlan for the 802.1Q frames***
Cat3560(config-if)#switchport access vlan 12 ***!Native vlan for untagged frames***

Building a Campus Network
Distribution Layer

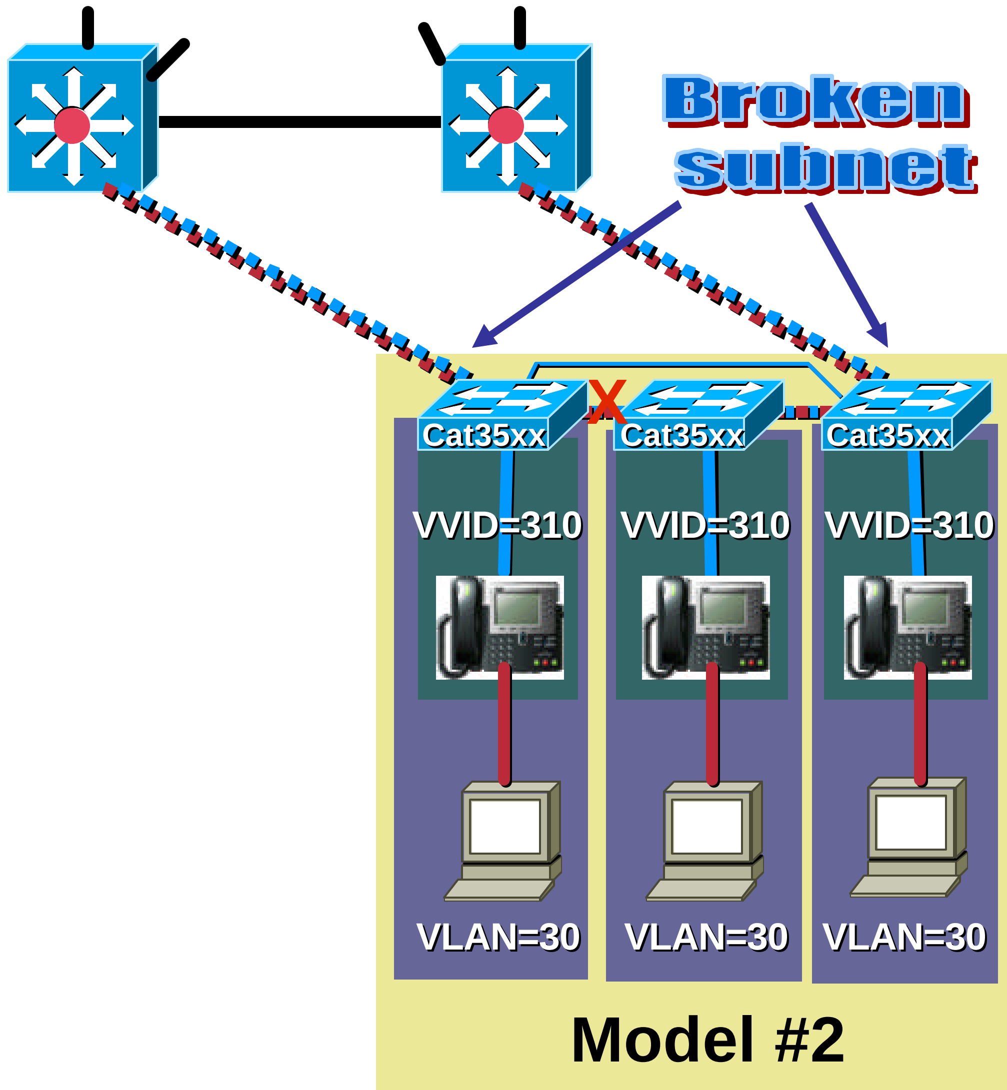
Distribution Layer Features:

- **Passive interface default**
- **HSRP, HSRP Track/Preempt**
- **OSPF/EIGRP:**
  - **Adjust timers**
  - **Summary address**
  - **Path costs**



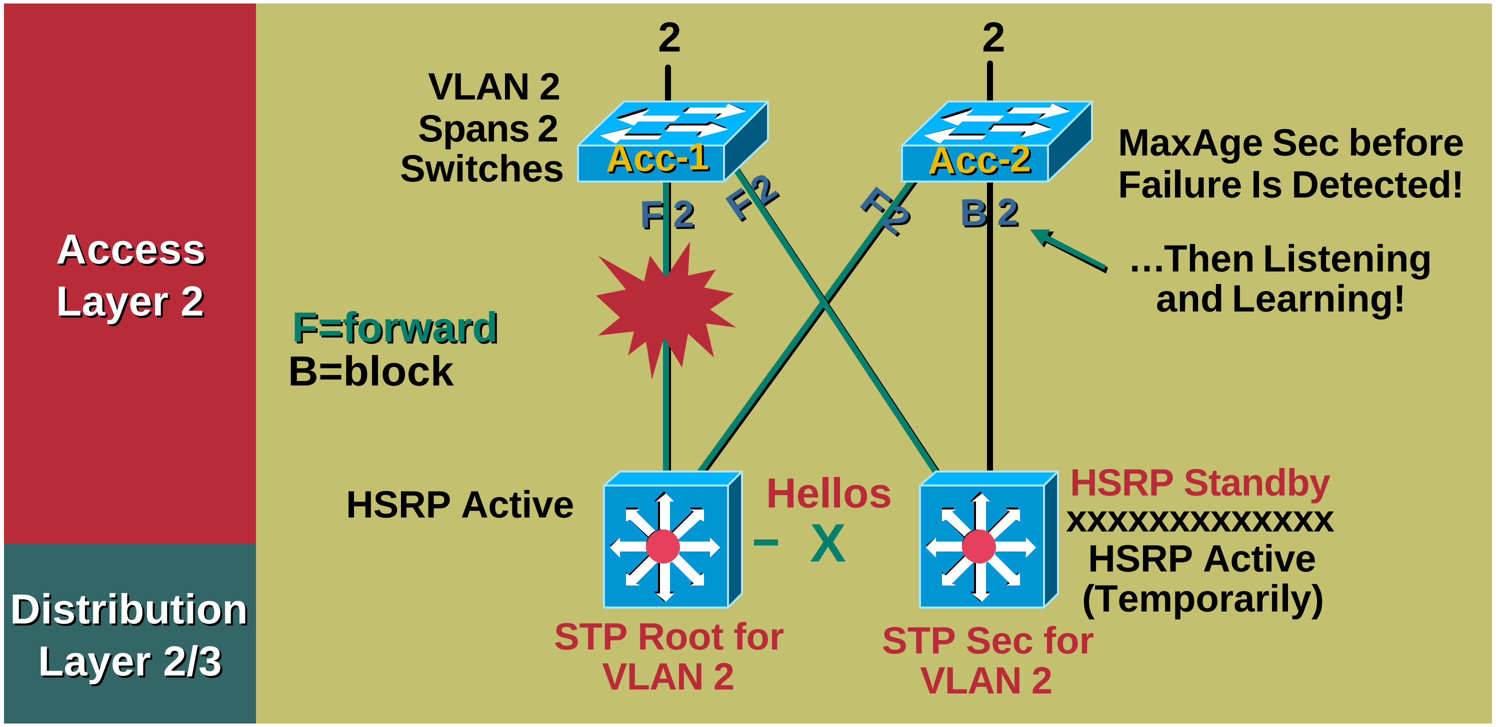
Using Stacking Access LAN Switches

- Potential broken subnet issue with access switches
- Catalyst 3560/3550
  - GBICs all used up between switch and uplink
  - Avoid 35xx gigastack for voice – half duplex - collisions
  - Alternate 100Mbps connection between top of first/last – limited L2
  - Configure STP appropriately
- Catalyst 3750
  - Use stackwise connections between switches



Building a Campus Network

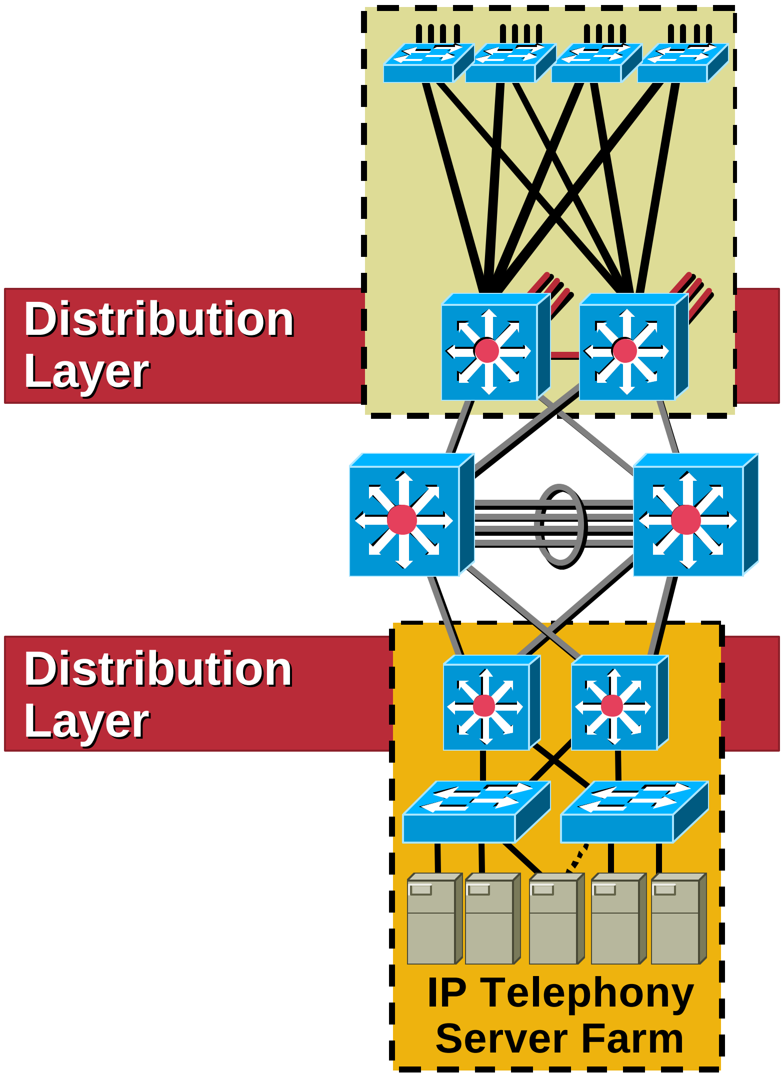
Distribution Layer: L2 Between the Distribution Switches?



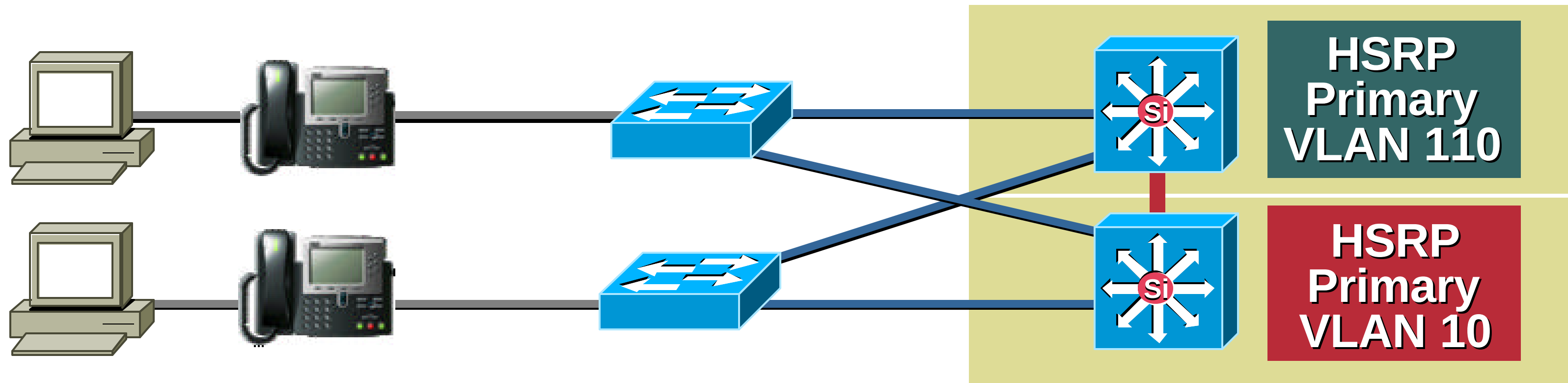
- If failure, only part of the users can be reached (traffic from left distribution switch to users on Acc-1 for instance -> black hole for 50 seconds)
- When topology has converged, consider the path taken by users on Acc-1 (3 “hops”)

Building a Campus Network
Which Features for the Distribution Layer?

- Distribution layer features
  - Set STP root—Dictate STP topology
  - Set STP secondary—Backup root bridge
  - Enable HSRP—Provide redundant gateways
  - Tune HSRP timers—Reduce fail-over
  - Set HSRP-track—Ensure optimal routing
  - Set HSRP-preempt delay—Time for RP
  - Weigh routes—Ensure symmetry
  - No L2 link between switches—If possible
  - Route summarization—Towards the core



Building a Campus Network
Distribution Layer: Cisco Catalyst 6000 (Native IOS)




```
interface Vlan10
 ip address 172.26.216.35 255.255.255.240
 standby priority 100 preempt
 standby ip 172.26.216.33
 standby track Gi1/1 12
interface Vlan110
 ip address 10.10.10.2 255.255.255.0
 standby priority 110 preempt
 standby ip 10.10.10.1
 standby track Gi1/1 12
router eigrp 100
 passive-interface Vlan110
```

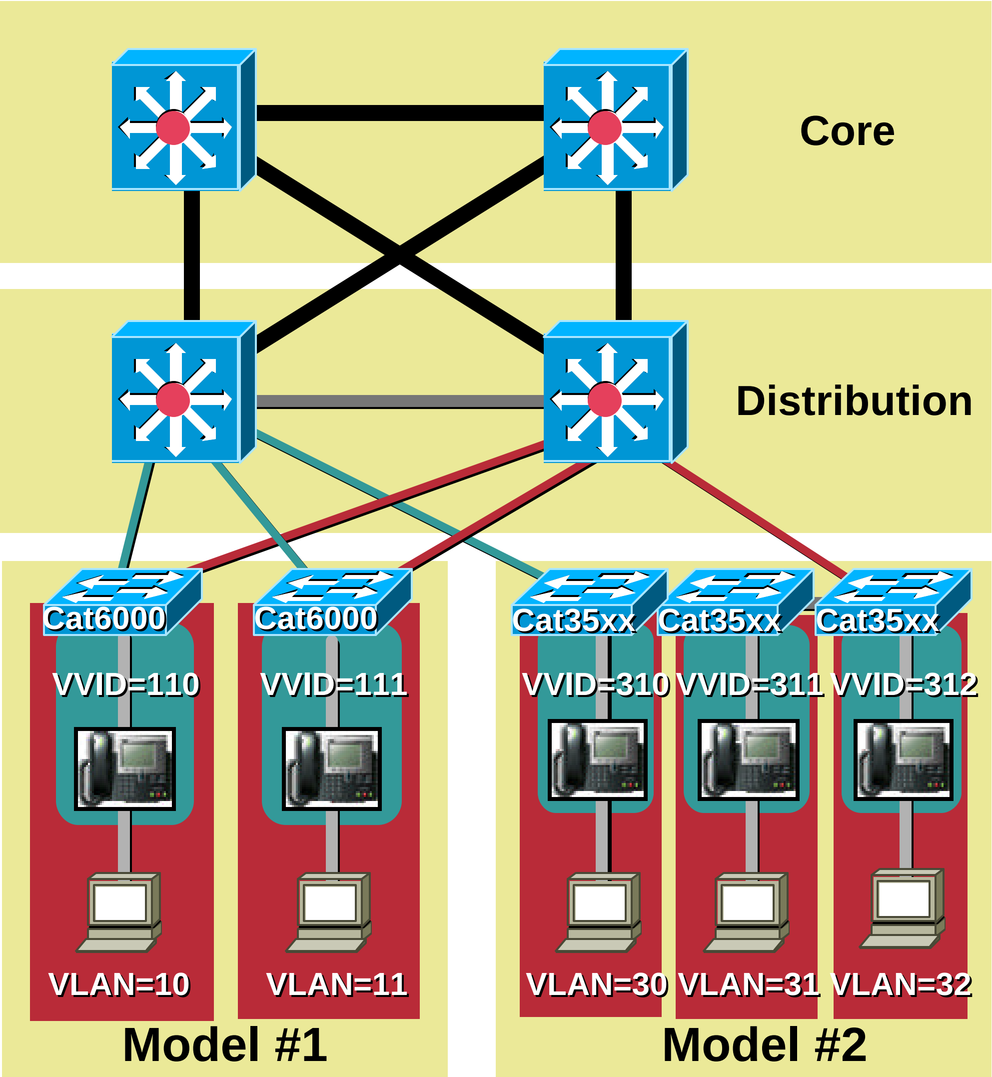
= L2 Links
= L3 Links

Building a Campus Network
Core Layer

Cisco.com

Core Layer Features:

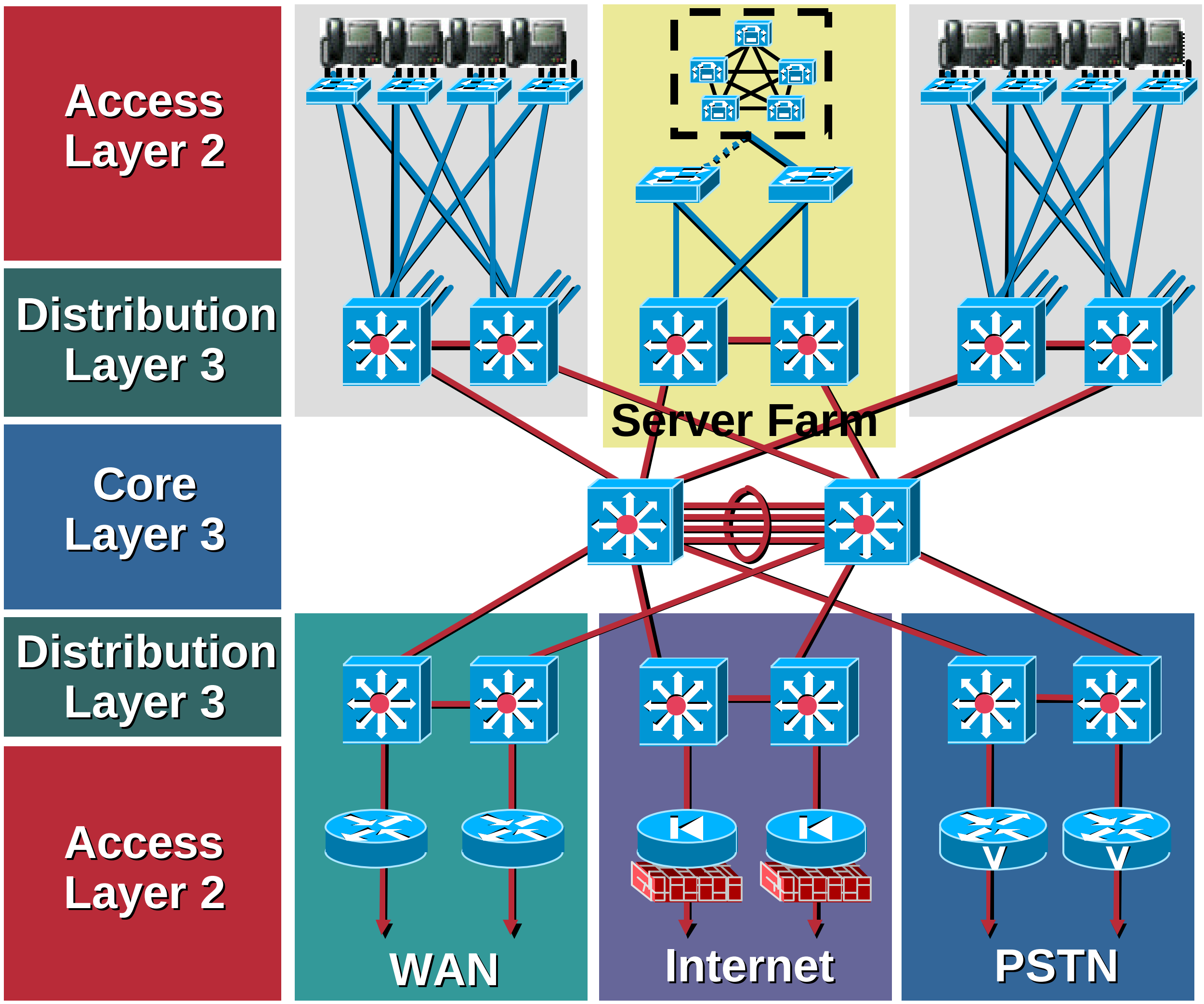
- Each link belongs to its own /30 subnet
- No STP in the core—All routed
- Load balancing to the core/server farm by default
- Tune routing protocol timers for fast convergence



Building a Campus Network Summary

Cisco.com

- Access Layer
  - Per-VLAN spanning-tree
  - Rootguard portfast UplinkFast
- Distribution Layer
  - HSRP with load balancing
  - OSPF/EIGRP configured for fast convergence
- Core
  - OSPF/EIGRP configured for fast convergence



Network Infrastructure Agenda

- Building a Campus Network
- Enabling QoS in the Campus
- Providing Inline Power to IP Phones
- Overlaying Wireless LANs
- Building a WAN
- Enabling QoS in the WAN
- Networks Services

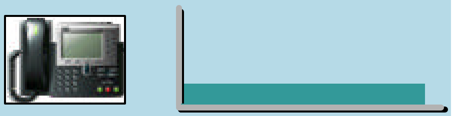
Is Quality of Service (QoS) Needed in the Campus?

"Just throw more bandwidth at it. That will solve the problem!"

Maybe, Maybe Not; Campus Congestion Is a Buffer Management Issue

Network Infrastructure and QoS
Traffic Profiles and Requirements

Voice



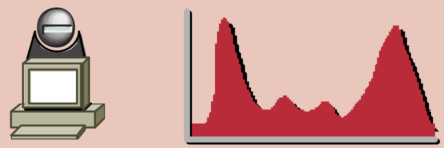
- Smooth
- Benign
- Drop Sensitive
- Delay Sensitive
- UDP Priority

Bandwidth per call depends on codec, sampling-rate, and Layer 2 media

- **Latency = 150 ms**
- **Jitter = 30 ms**
- **Loss = 1%**

One-way requirements

Video-Conf



- Bursty
- Greedy
- Drop Sensitive
- Delay Sensitive
- UDP Priority

IP/VC has the same requirements as VoIP, but has radically different traffic patterns (BW varies greatly)

- **Latency = 150 ms**
- **Jitter = 30 ms**
- **Loss = 1%**

One-way requirements

Data

- Smooth/Bursty
- Benign/Greedy
- Drop Insensitive
- Delay Insensitive
- TCP Retransmits

Traffic patterns for Data vary among applications

Data Classes:

Mission-Critical Apps

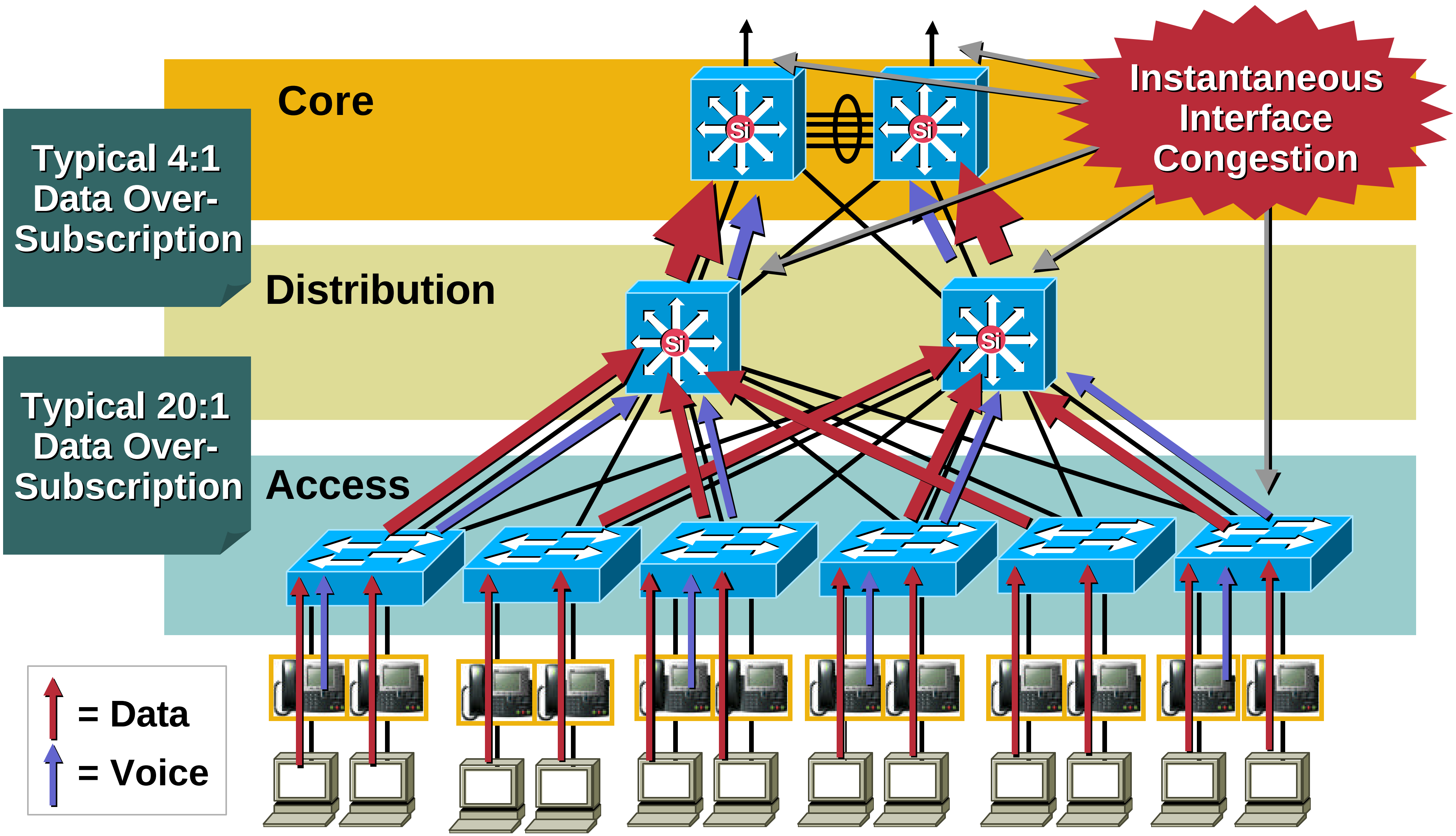
Transactional/Interactive Apps

Bulk Data Apps

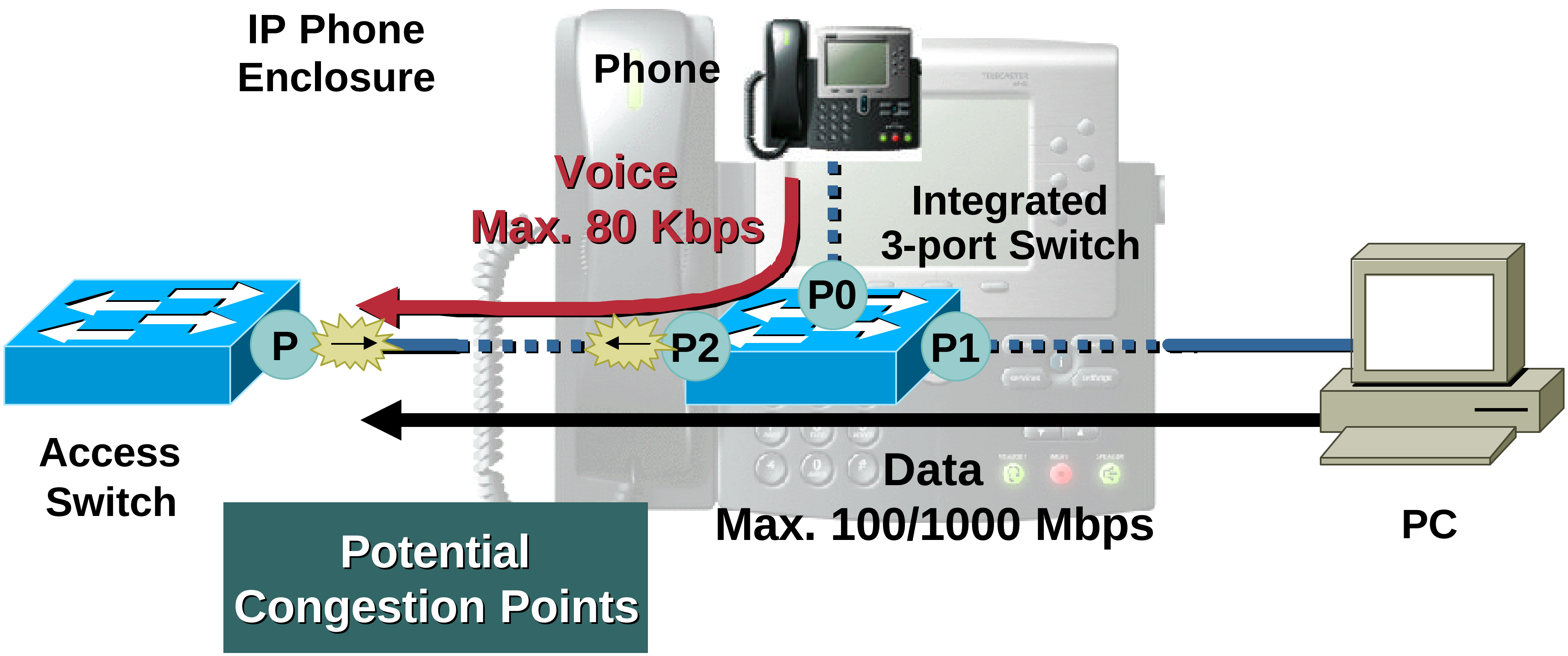
Best Effort Apps (Default)

Enabling QoS in the Campus
Congestion Scenario: TCP Traffic Burst + VoIP

Cisco.com



Enabling QoS in the Campus
Congestion Scenario: Data + VoIP



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

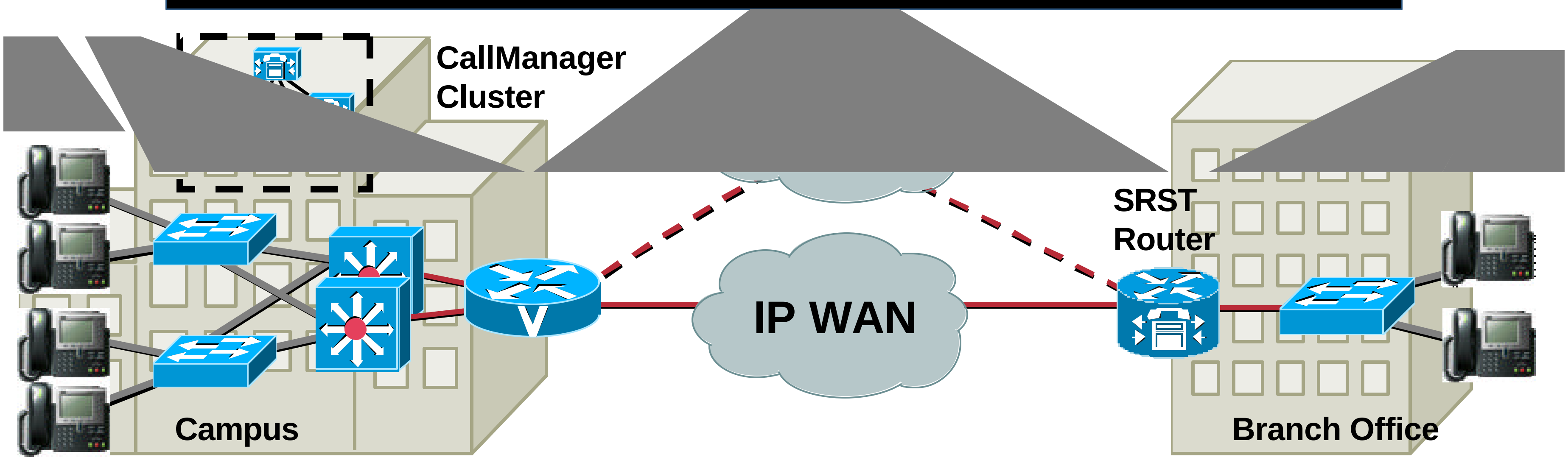
Enabling QoS in the Campus
Cisco's Approach to QoS

Classification: Mark the Packets with a Specific Priority Denoting a Requirement for Class of Service from the Network

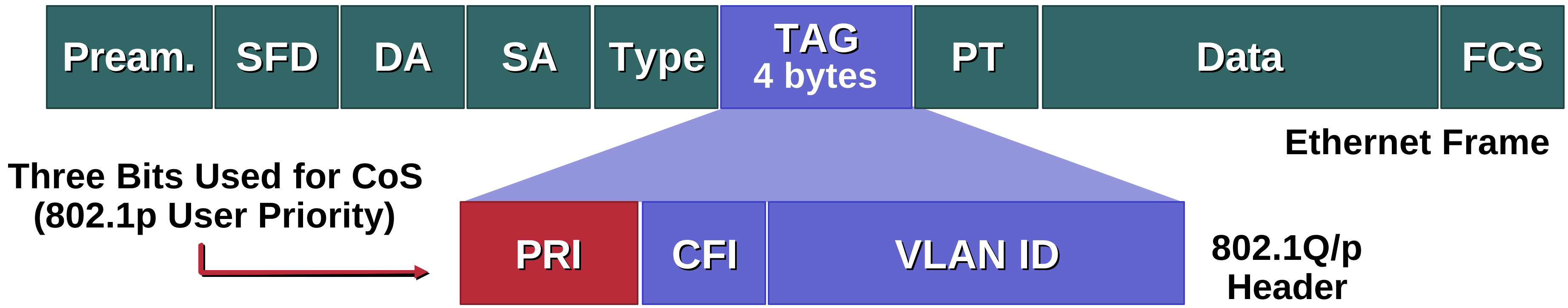
Trust Boundary: Define and Enforce a Trust Boundary at the Network Edge

Scheduling: Assign Packets to One of Multiple Queues (Based on Classification) for Expedited Treatment through the Network

Provisioning: Accurately Calculate the Required Bandwidth for All Applications Plus Element Overhead



Enabling QoS in the Campus
Layer 2 Classification: 802.1p, CoS

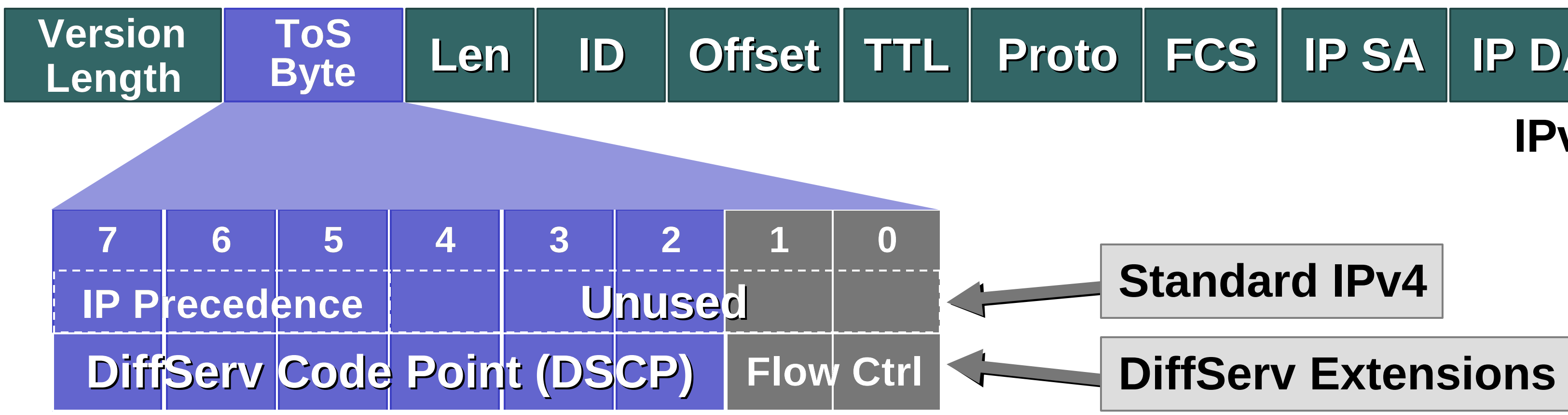


- **802.1p user priority field also called Class of Service (CoS)**
- **Different types of traffic are assigned different CoS values**
- **CoS 6 and 7 are reserved for network use**

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 DiffServ 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

Classification Summary

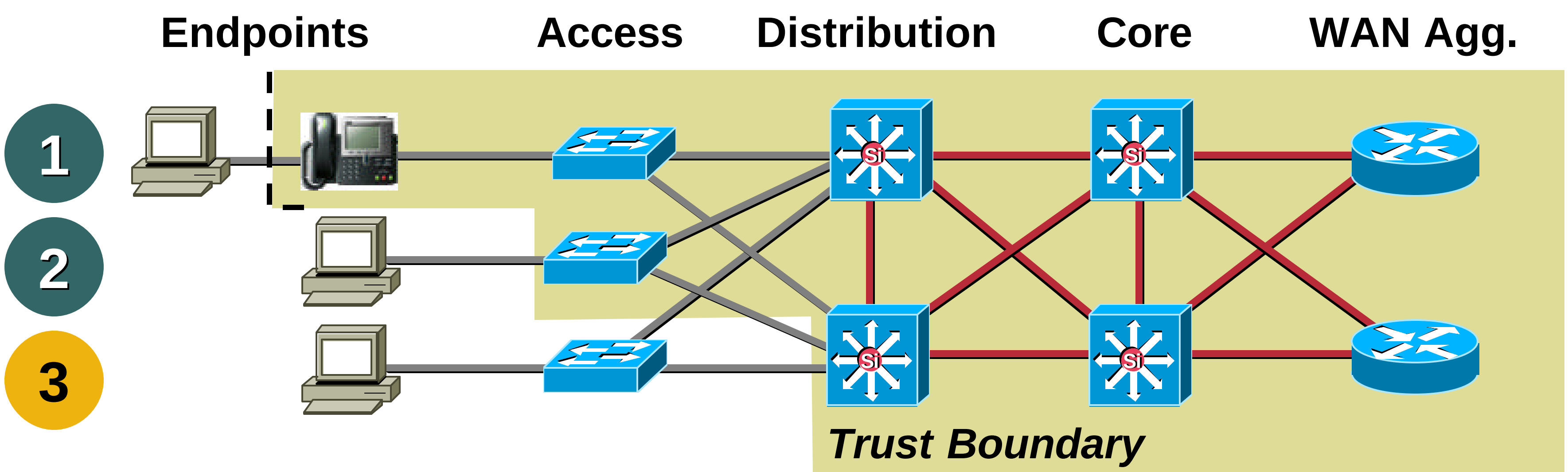
L2 CoS	L3 Classification IP Prec.	PHB	DSCP	Application
7	7	-	56-63	Reserved
6	6	-	48-55	Reserved
5	5	EF	46	Voice Bearer
4	4	AF41	34	Video Conferencing*
3	3	CS3	24	Call Signaling
2	2	AF2y	18,20,22	High Priority Data
1	1	AF1y	10,12,14	Medium Priority Data
0	0	BE	0	Best Effort Data

* Including audio and video

New IETF recommendations

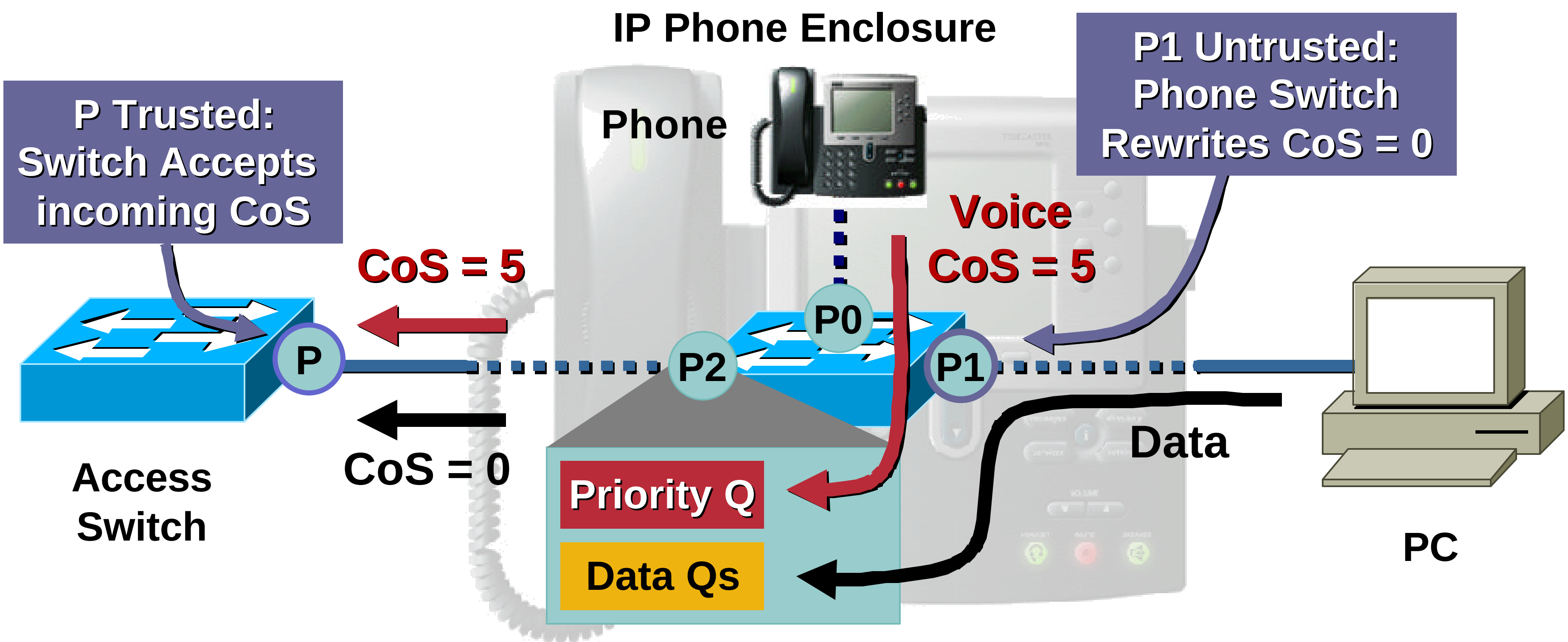
Enabling QoS in the Campus
Trust Boundary

Cisco.com



- A device is trusted if it correctly classifies packets
- For scalability, classification should be done as close to the edge as possible
- The outermost trusted devices represent the trust boundary
- 1 and 2 are optimal, 3 is acceptable (if access switch cannot perform classification)

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 re-marked with CoS 0 (low priority) by the IP phone switch; this occurs if PC tags frames as 802.1p/Q**

Enabling QoS in the Campus
Port Trust Concepts in Catalyst 6K Switches

Cisco.com

- `set port qos <mod/port>` **trust-ext** _____

  Only applies to port trust on the IP phone PC ethernet port

  Un-related to actual cat6k port trust

  `cat6k-a1> (enable) set port qos 2/1 trust-ext untrusted`

- `set port qos <mod/port>` **trust** ____

  Applies to the actual Cat6k port trust rules

  untrusted (default), trust-cos, trust-ipprec, trust-dscp

  Some 10/100 cards (2Q2T non-GigabitEthernet) require an additional ACL to actually enable port trust:

```
cat6k-a1> (enable) set qos enable
cat6k-a1> (enable) set port qos 5/1-48 trust trust-cos
cat6k-a1> (enable) set port qos 5/1-48 vlan-based
cat6k-a1> (enable) set qos acl ip ACL_IP-PHONES trust-cos ip any any
cat6k-a1> (enable) commit qos acl all
cat6k-a1> (enable) set qos acl map ACL_IP-PHONES 110
```

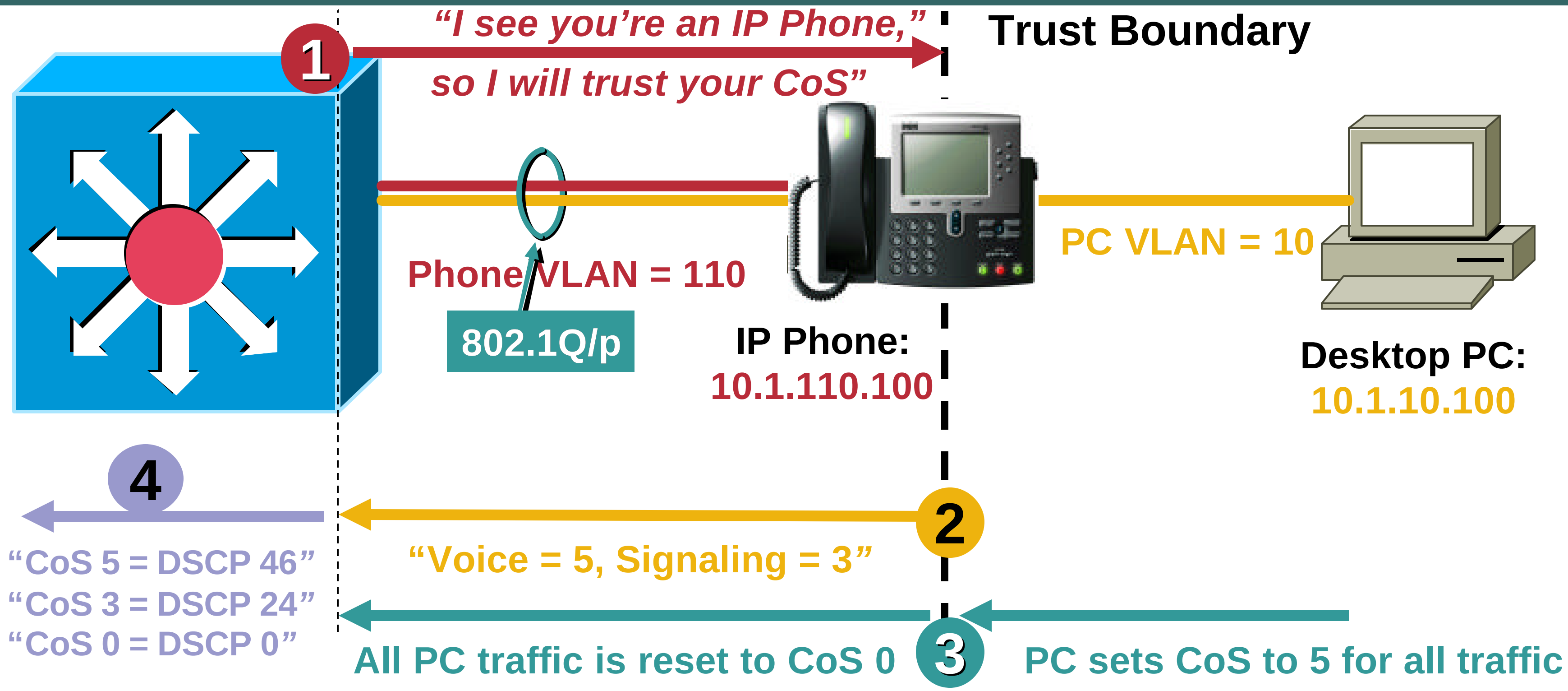
Enabling QoS in the Campus
Conditional Trust and Rate Limiting

- Multiple platforms now allow for extension of trust boundary to be based on detection of IP phone
- Rate limiting is also available to contain traffic flows in any given class
- Platforms include 2950, 2970, 3560, 3750, 4500 and 6500

Campus QoS Considerations

Trust Boundary Extension and Operation

Cisco.com



1. Switch and Phone exchange CDP; trust boundary is extended to IP Phone
2. Phone sets CoS to 5 for VoIP and to 3 for Call-Signaling traffic
3. Phone rewrites CoS from PC port to 0
4. Switch trusts CoS from Phone and maps CoS® DSCP for output queuing

Catalyst 6500 QoS Design

Conditionally Trusted IP Phone + PC Example: Part 1

Cisco.com

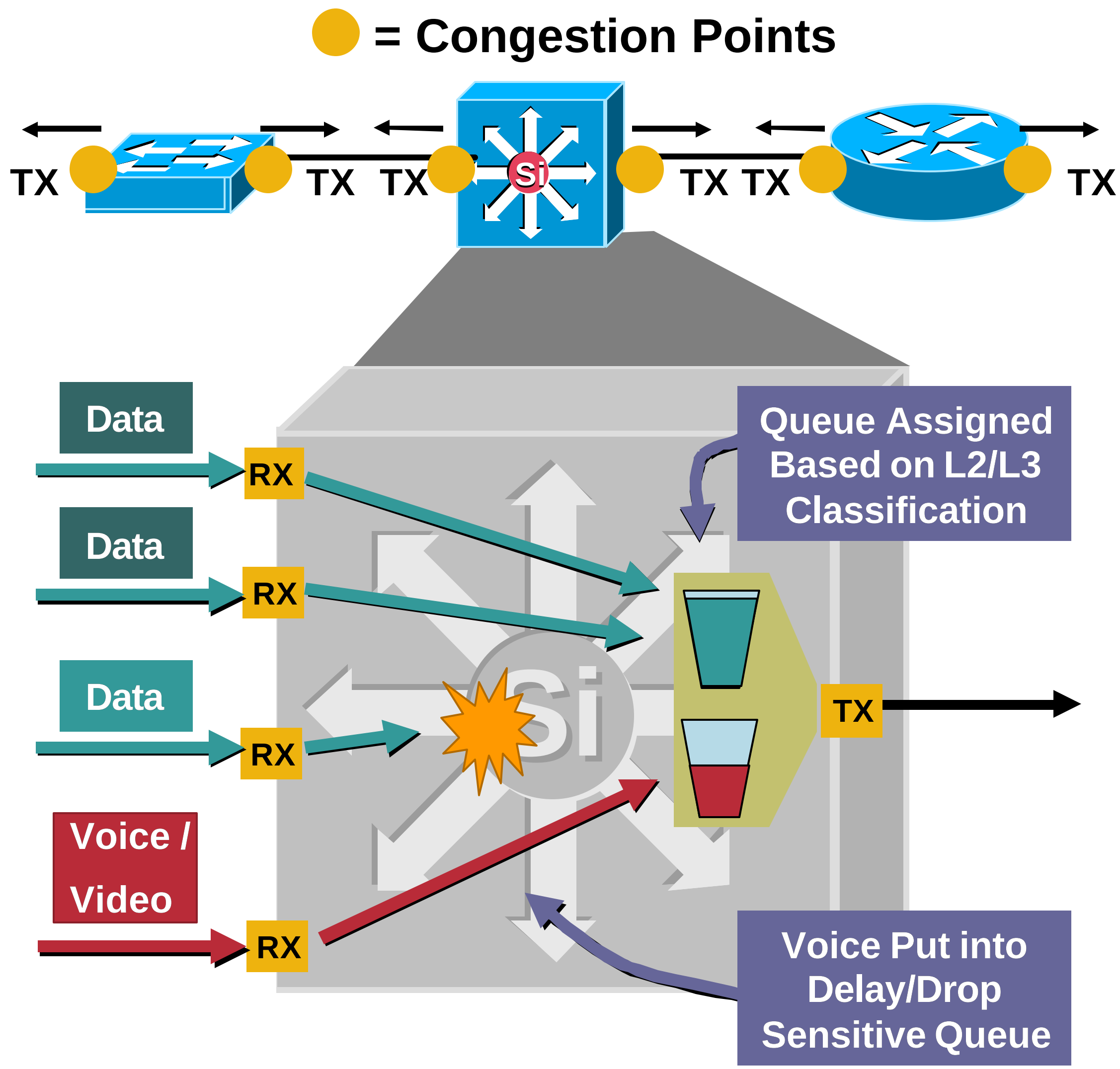
```
CAT6500-PFC2-CATOS> (enable) set qos cos-dscp-map 0 8 16 24 32 46 48 56
        ! Modifies default CoS-DSCP mapping so that CoS 5 is mapped to DSCP EF
CAT6500-PFC2-CATOS> (enable) set qos policed-dscp-map 0,24:8
        ! Excess traffic marked DSCP 0 or CS3 is remarked to CS1
CAT6500-PFC2-CATOS> (enable)


CAT6500-PFC2-CATOS> (enable) set qos policer aggregate VVLAN-VOICE
        rate 128 burst 8000 drop
        ! Defines the policer for IP Phone VoIP traffic
CAT6500-PFC2-CATOS> (enable) set qos policer aggregate VVLAN-SIGNALING
        rate 32 burst 8000 policed-dscp
        ! Defines the policer for IP Phone Call-Signaling traffic
CAT6500-PFC2-CATOS> (enable) set qos policer aggregate VVLAN-ANY
        rate 32 burst 8000 policed-dscp
        ! Defines the policer for any other traffic sourced from the VVLAN
CAT6500-PFC2-CATOS> (enable) set qos policer aggregate PC-DATA
        rate 5000 burst 8000 policed-dscp
        ! Defines the policer for PC Data traffic
CAT6500-PFC2-CATOS> (enable)
```

Catalyst 6500 QoS Design
Conditionally Trusted IP Phone + PC Example: Part 2

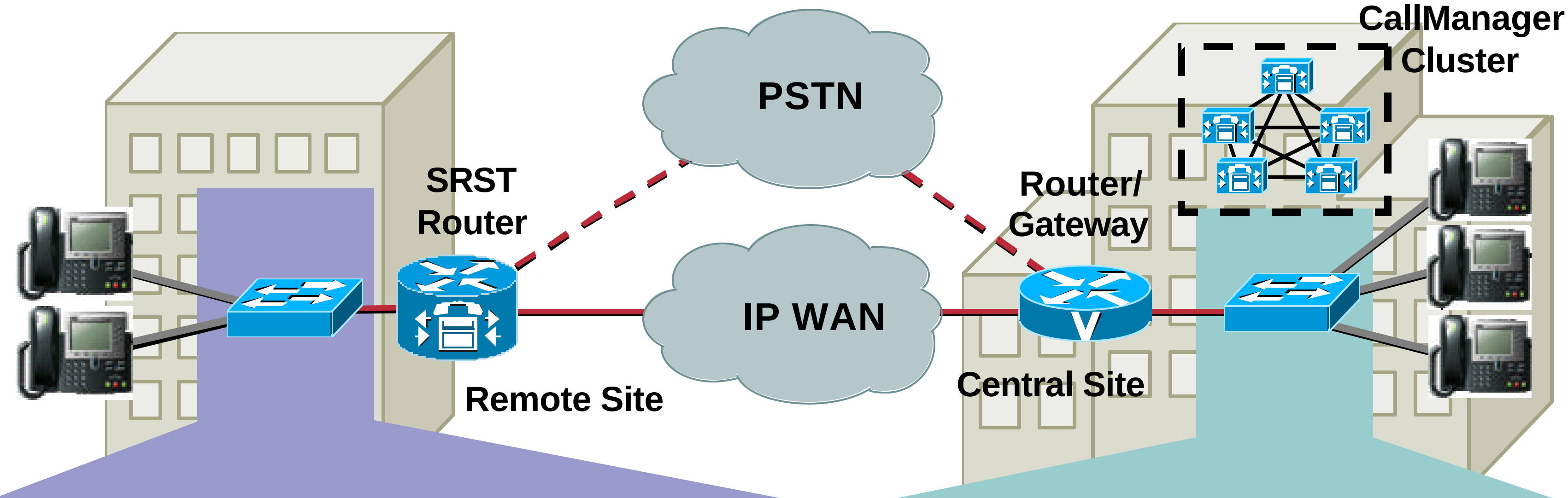

```
CAT6500-PFC2-CATOS> (enable) set qos acl ip IPPHONE-PC-BASIC dscp 46
        aggregate VVLAN-VOICE udp 10.1.110.0 0.0.0.255 any range 16384 32767
        ! Binds ACL to policer and marks in-profile VVLAN VoIP to DSCP EF
CAT6500-PFC2-CATOS> (enable) set qos acl ip IPPHONE-PC-BASIC dscp 24
        aggregate VVLAN-SIGNALING tcp 10.1.110.0 0.0.0.255 any range 2000 2002
        ! Binds ACL to policer marks in-profile VVLAN Call-Signaling to DSCP CS3
CAT6500-PFC2-CATOS> (enable) set qos acl ip IPPHONE-PC-BASIC dscp 0
        aggregate VVLAN-ANY 10.1.110.0 0.0.0.255
        ! Binds ACL to policer and marks all other VVLAN traffic to DSCP 0
CAT6500-PFC2-CATOS> (enable) set qos acl ip IPPHONE-PC-BASIC dscp 0
        aggregate PC-DATA any
        ! Binds ACL to policer and marks in-profile PC Data traffic to DSCP 0
CAT6500-PFC2-CATOS> (enable)


CAT6500-PFC2-CATOS> (enable) commit qos acl IPPHONE-PC-BASIC
        ! Commits ACL to PFC memory
CAT6500-PFC2-CATOS> (enable)
CAT6500-PFC2-CATOS> (enable) set port qos 3/1 trust-device ciscoipphone
        ! Conditional trust (for Cisco IP Phones only)
CAT6500-PFC2-CATOS> (enable) set qos acl map IPPHONE-PC-BASIC 3/1
        ! Attaches ACL to switch port
CAT6500-PFC2-CATOS> (enable)
```

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**
- Cisco switches with multiple queues
  - Catalyst 2950, 2970, 3500, 3560, 3560, 3750, 4000, 4500, 6000



Building a Campus Network Platform Recommendations

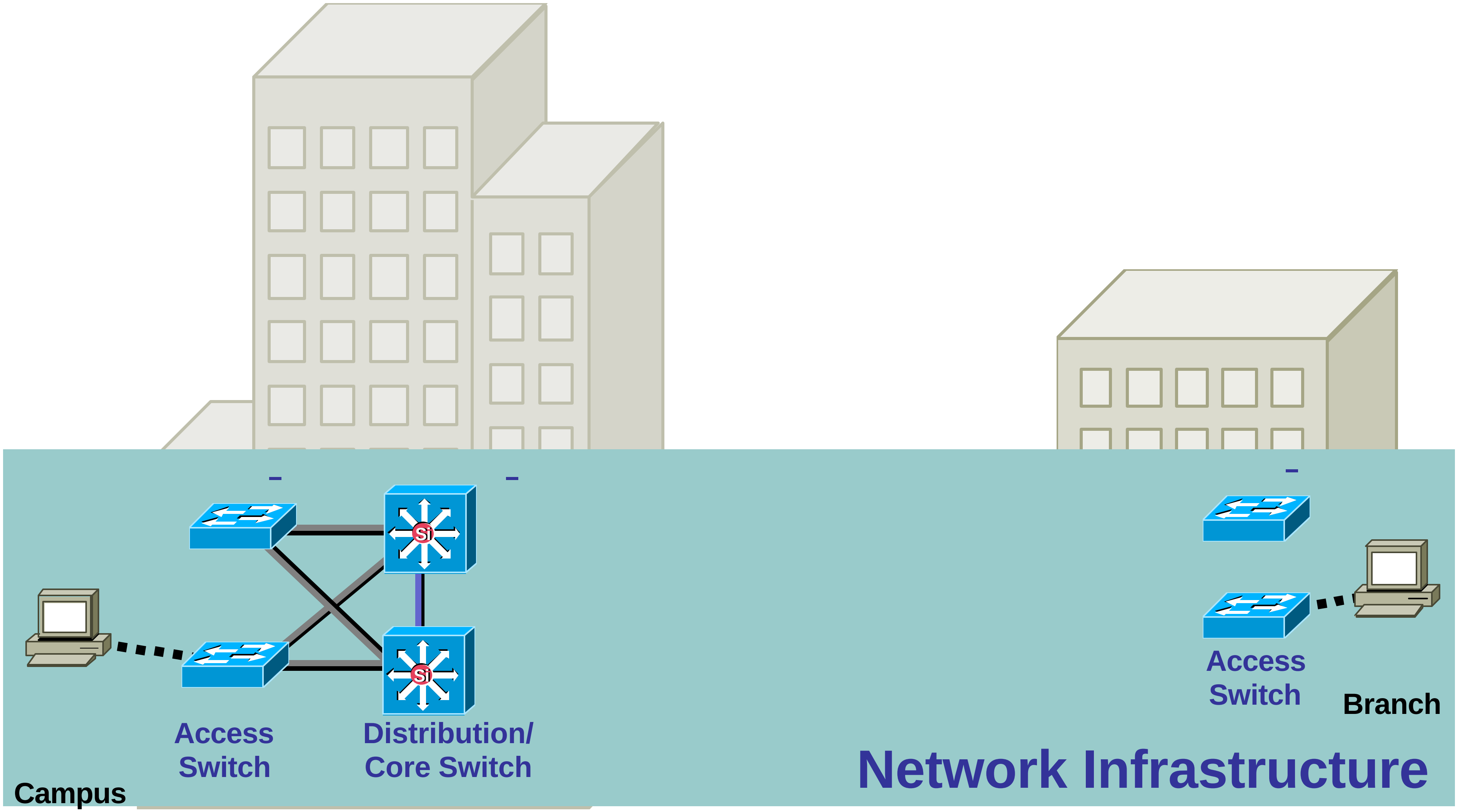


- Catalyst 4x00
- Catalyst 3560, 3750
- Catalyst 2950, 2750
- IOS Router SW NM, HWIC

- Catalyst 6500
- Catalyst 4500
- Catalyst 4000

What We Have Built so Far

Cisco.com



Network Infrastructure Agenda

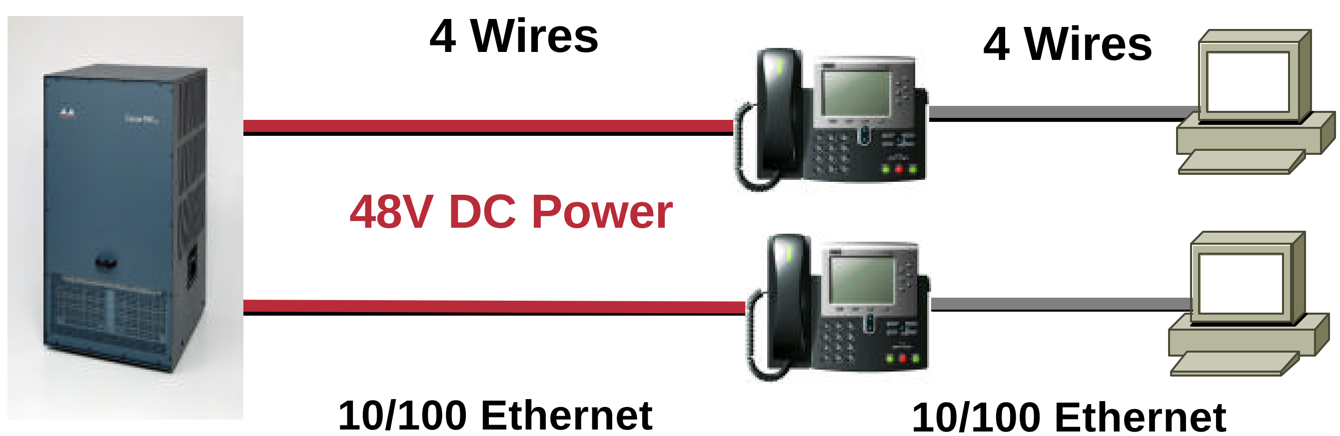
- Building a Campus Network
- Enabling QoS in the Campus
- Providing Inline Power to IP Phones
- Overlaying Wireless LANs
- Building a WAN
- Enabling QoS in the WAN
- Networks Services

Providing Inline Power to IP Phones Automatic Subnet Placement

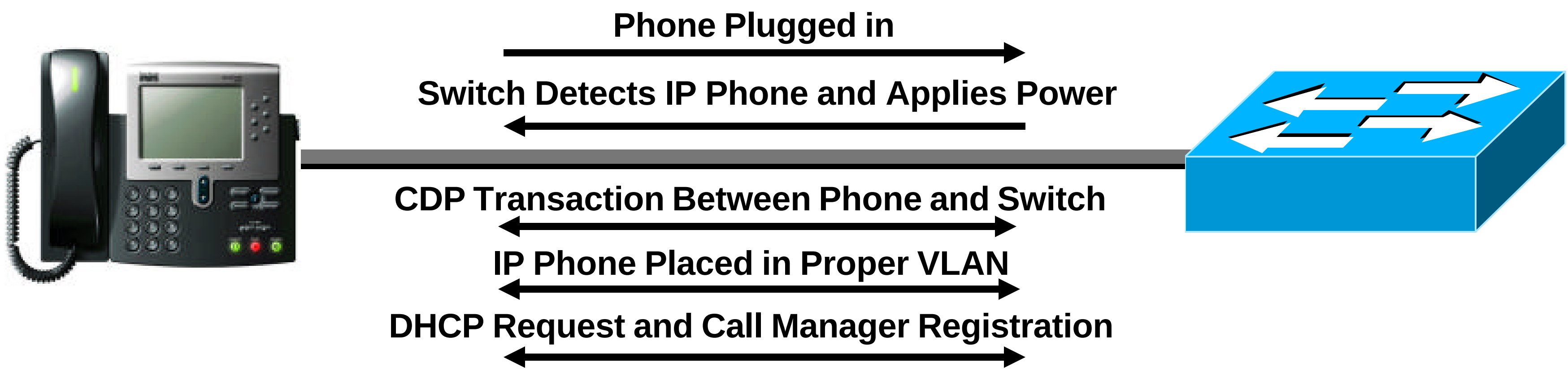
Cisco.com

Catalyst Multiservice Port Provides Automatic Phone VLAN Configuration

Inline Power on Catalyst® Switches



Providing Inline Power to IP Phones
Auto Configuration Process



- **IEEE 802.3af**

  Cisco, Nortel, Avaya, 3com, PowerDsine, HP

- **Standard adopted June 11th, 2003**
- **Cisco is committed to standards has shipped the first IEEE 802.3af compliant phone (the 7970); it is also compatible with Cisco inline power scheme**
- **Catalyst platforms supporting 802.3af: 6500, 4500, 3750, 3560**

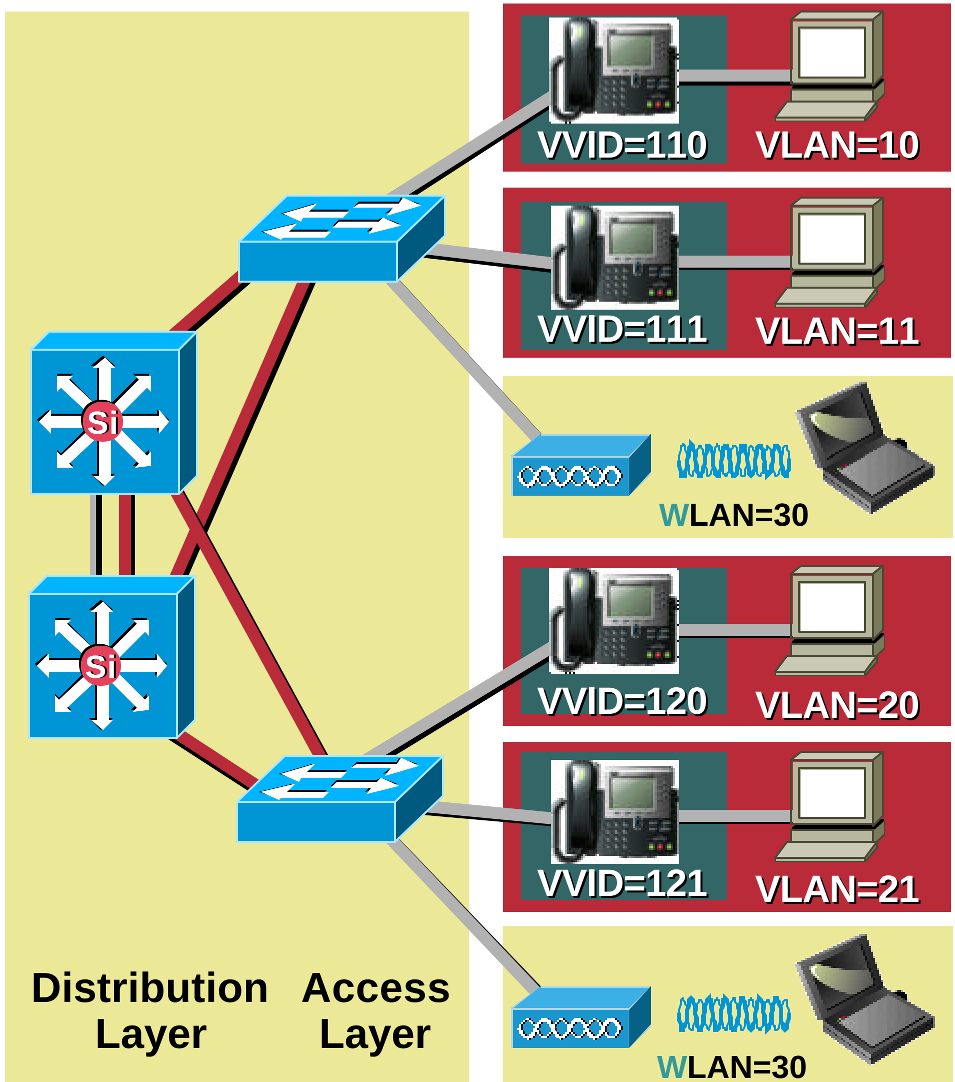
Network Infrastructure Agenda

Cisco.com

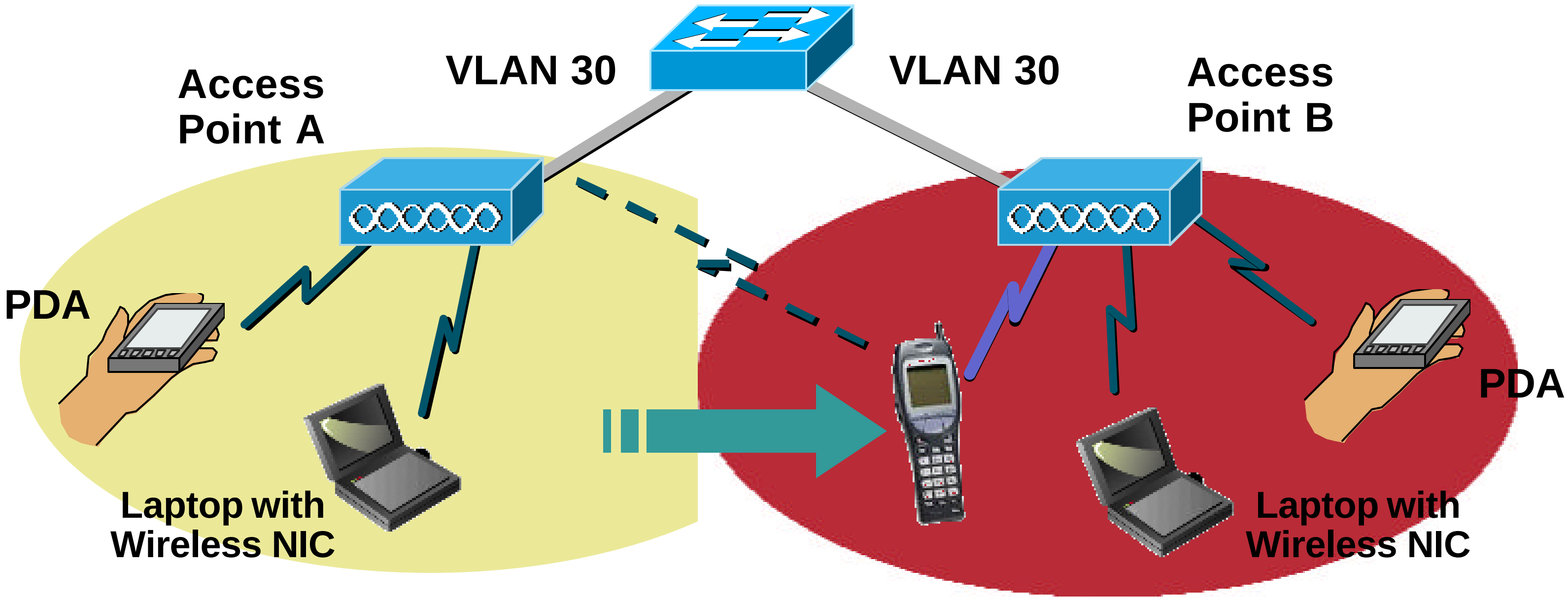
- Building a Campus Network
- Enabling QoS in the Campus
- Providing Inline Power to IP Phones
- Overlaying Wireless LANs
- Building a WAN
- Enabling QoS in the WAN
- Networks Services

Overlaying Wireless LANs
VLAN Design

- Create a single VLAN for the wireless LAN per campus building
- Need a L2 link between distribution switches to carry the wireless VLAN
- Spanning tree convergence only affects the WLAN
- Layer 2 roaming within the building (Layer 2 domain spans multiple wiring closet switches)

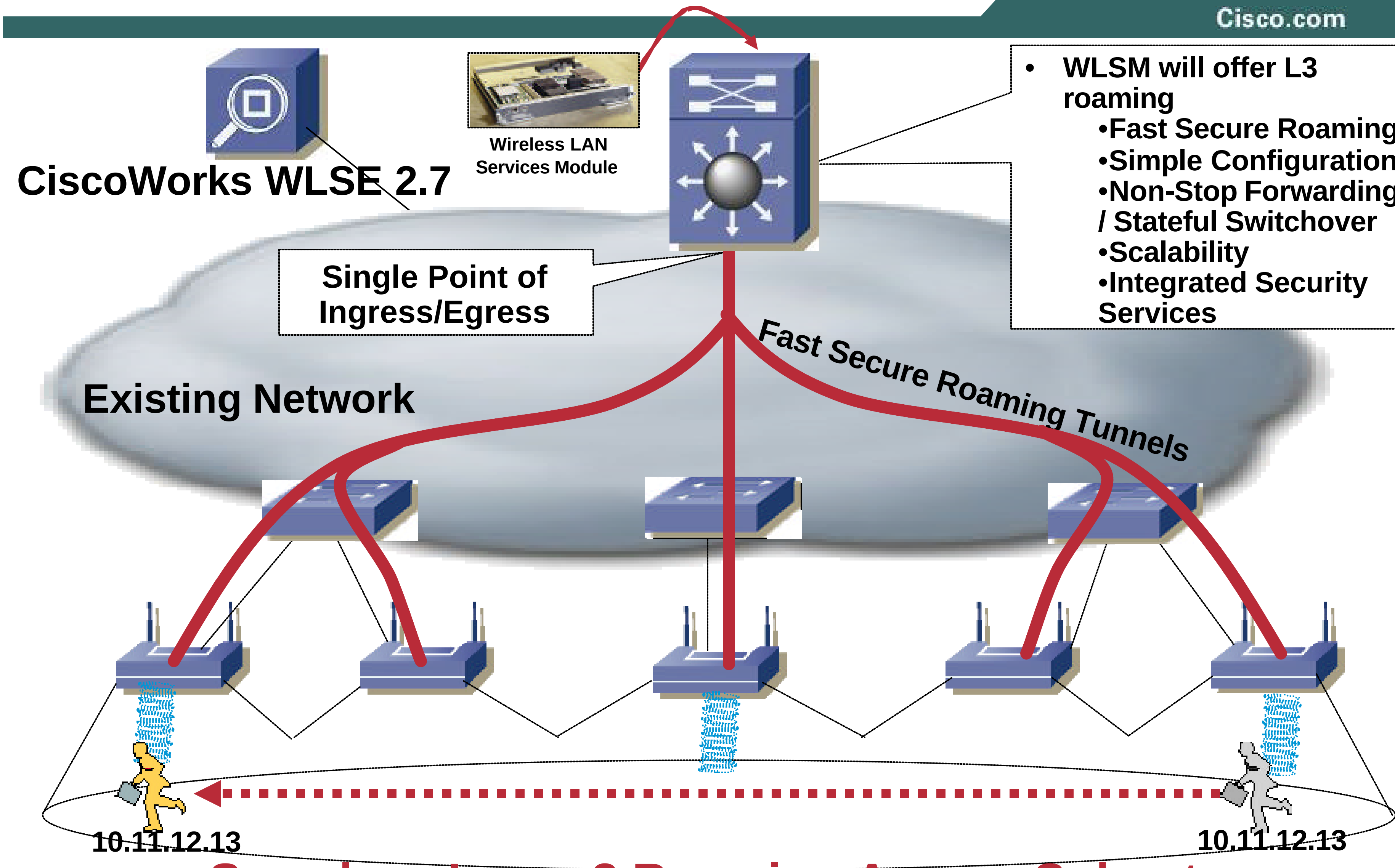


Overlaying Wireless LANs
Layer 2 Roaming



- When client moves into B's coverage area, it re-associates with B
- Handoff typically requires < 500 ms
- Layer 3 roaming will be supported by Wireless LAN Services Module

Overlaying Wireless LANs
Layer 3 Roaming



- WLSM will offer L3 roaming
  - •Fast Secure Roaming
  - •Simple Configuration
  - •Non-Stop Forwarding / Stateful Switchover
  - •Scalability
  - •Integrated Security Services

Seamless Layer 3 Roaming Across Subnets

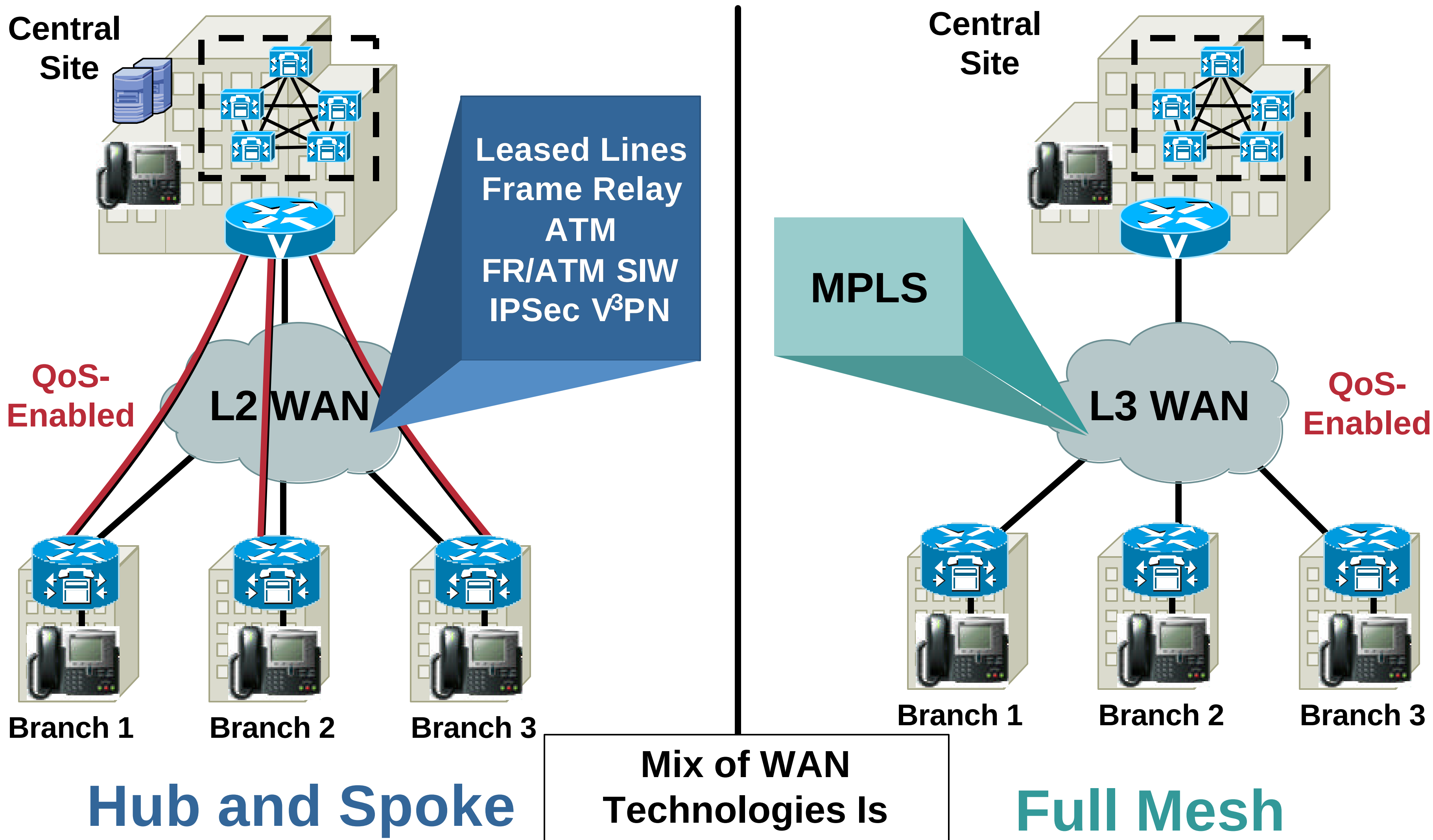
Network Infrastructure Agenda

Cisco.com

- Building a Campus Network
- Enabling QoS in the Campus
- Providing Inline Power to IP Phones
- Overlaying Wireless LANs
- Building a WAN
- Enabling QoS in the WAN
- Networks Services

QoS and WAN Considerations
WAN Topologies and Technologies

Cisco.com



Mix of WAN Technologies Is Supported

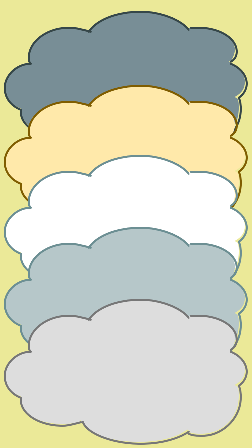
QoS and WAN Considerations

Best Effort vs. Guaranteed Quality

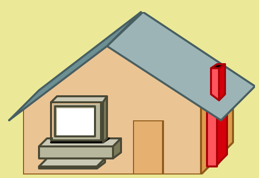
Guaranteed Voice Quality

Call Agents
Business
Critical Calls

- **Leased Lines**
- **Frame Relay**
- **ATM**
- **ATM / Frame Relay**
- **IP-SEC V³PN**
- **MPLS**



- **DSL**
- **Cable**
- **Wireless**
- **Internet**
- **VPN**



Best Effort Voice Quality

Telecommuters
Road Warriors
Intra Company Calls

Network Infrastructure Agenda

Cisco.com

- Building a Campus Network
- Enabling QoS in the Campus
- Providing Inline Power to IP Phones
- Overlaying Wireless LANs
- Building a WAN
- Enabling QoS in the WAN
- Networks Services

Enabling QoS in the WAN

The Evils of Packet-Based Voice/Video

Loss

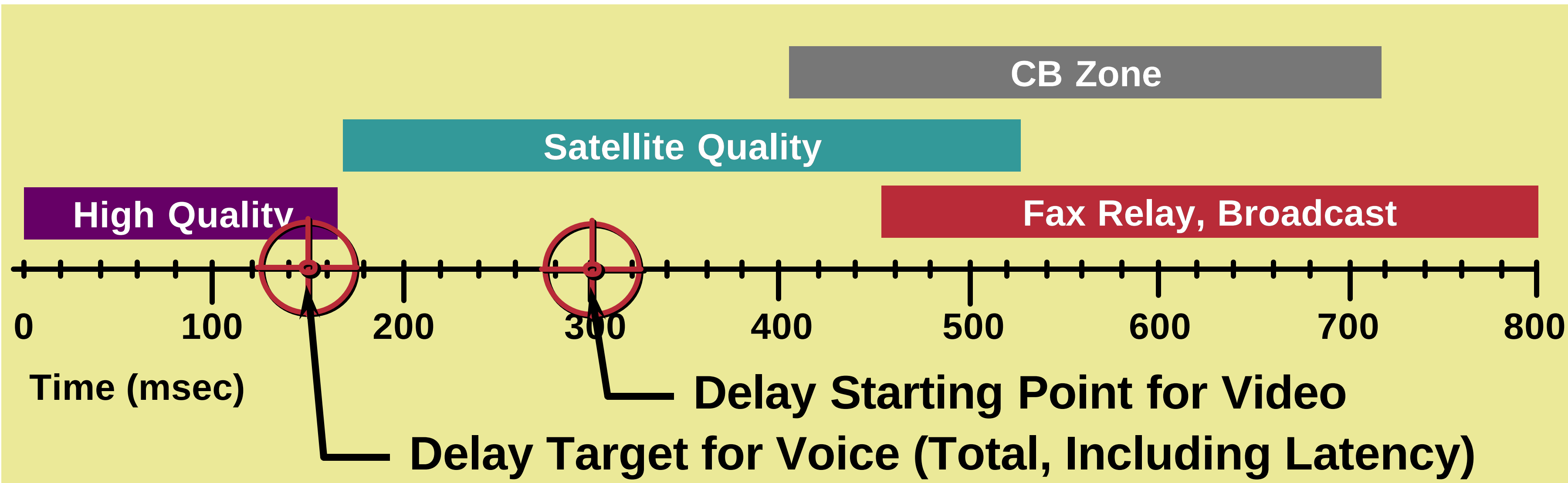
Delay

Delay Variation (Jitter)

Quality of Service
End-to-End Latency or Voice and Video

Cisco.com

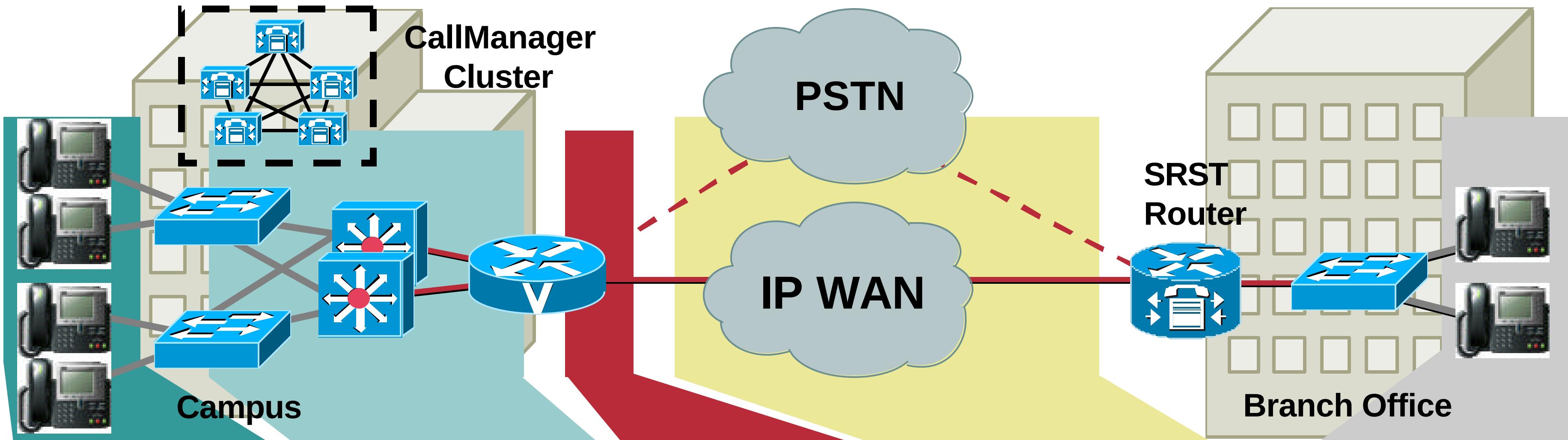
ITU G.114 “Recommendation”: 0–150msec 1-Way Delay



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

Enabling QoS in the WAN

Elements that Affect End-to-End Delay



CODEC	Queuing	Serialization	Propagation and Network	Jitter Buffer
G.729A: 25 ms	Variable (Can Be Reduced Using LLQ)	Variable (Can Be Reduced Using LFI)	6.3 μs/Km + Network Delay (Variable)	20-50 ms

End-to-End Delay (Should Be < 150 ms)

Enabling QoS in the WAN

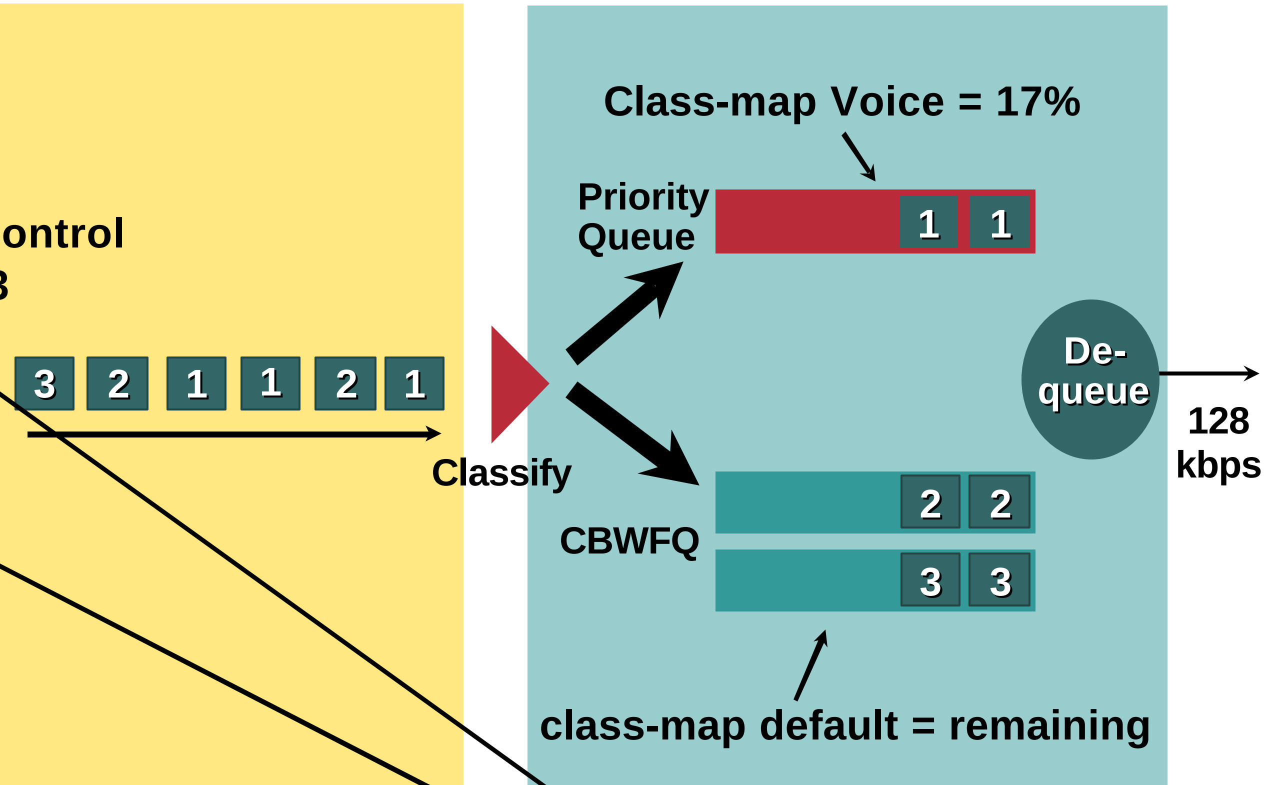
General Guidelines

- Use LLQ anytime VoIP over the WAN is involved
- Traffic shaping is a requirement for Frame Relay/ATM environments
- Use LFI techniques for all links below 768Kbps
  - Don't use LFI for any video over IP applications
- TX-ring sizes may require modifications
- Properly provision the WAN bandwidth
- Call admission control is a requirement where VoIP calls can over-subscribe the provisioned BW
- Use cRTP carefully
- Map QoS from L3 (IP Prec or DSCP) to L2 (802.1p) at remote branches if switch is L2 only

Enabling QoS in the WAN
LLQ Example

Cisco.com

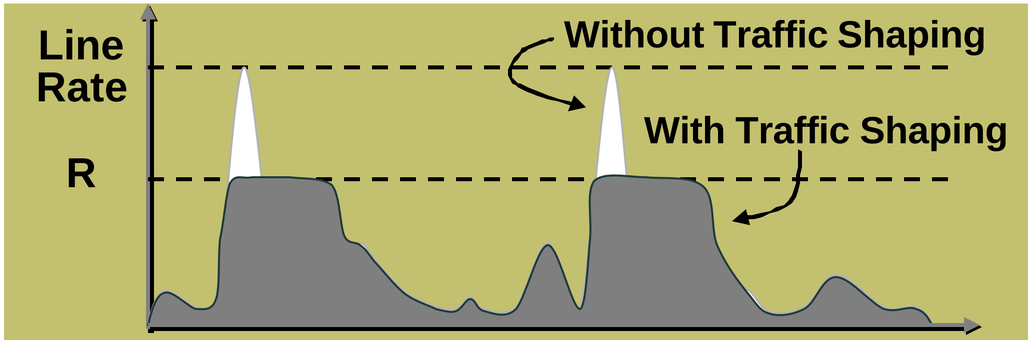
```
class-map class-default
  match any
class-map match-all voice
  match ip dscp ef
Class-map match-all voice-control
  match ip dscp af31 ; or CS3
!
policy-map WAN
 class voice
    priority percent 17
 class voice-control
    bandwidth percent 2
 class class-default
    fair-queue
!
interface Serial0/1
 ip address 10.1.6.2 255.255.255.0
 bandwidth 128
 no ip directed-broadcast
 service-policy output WAN
!
```



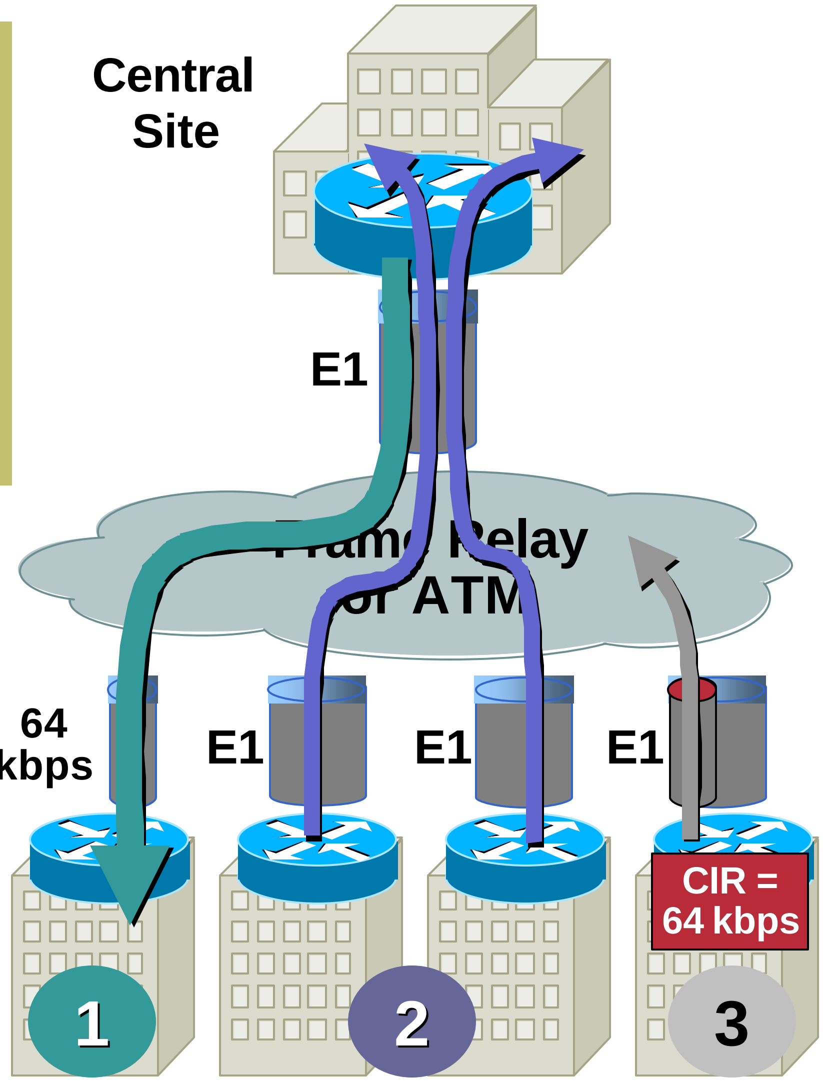
Any Packet with DSCP = 46 (PHB=EF) Gets Assigned to a Class that Will Get a High Priority Queue with 17% Bandwidth

Enabling QoS in the WAN
Traffic Shaping

Cisco.com



Traffic Shaping Limits the Transmit Rate to a Value (R) Lower than Line Rate

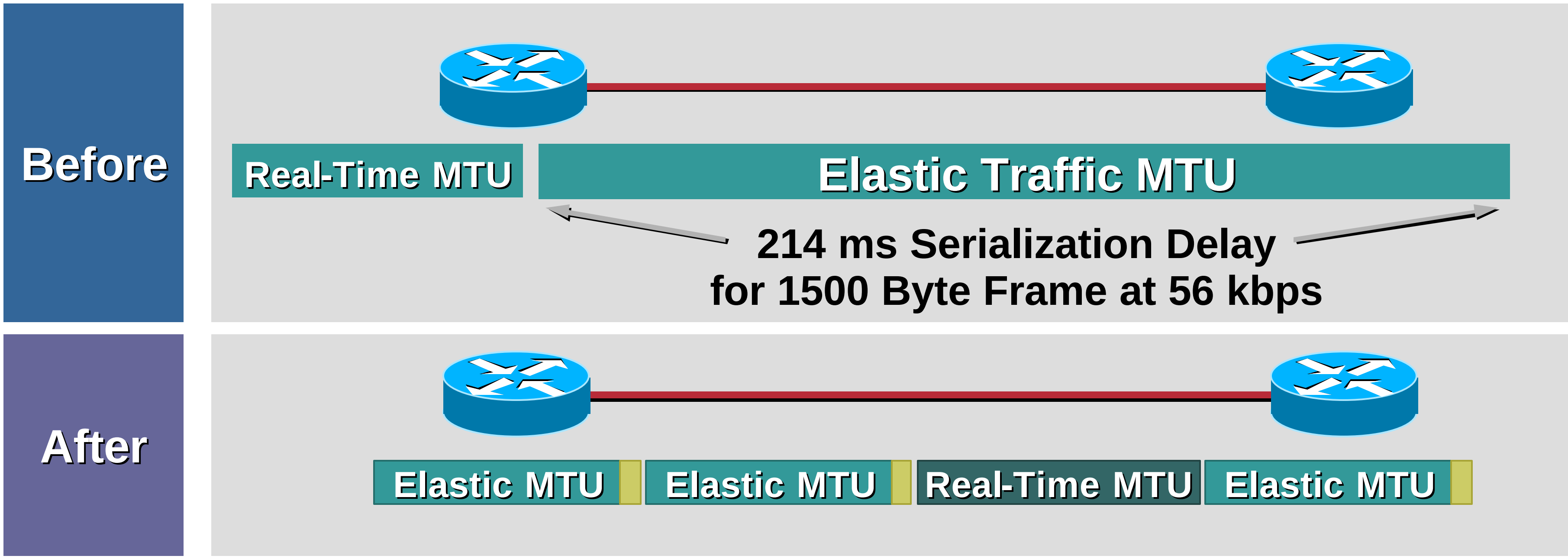


Why Is It Needed?

1. Line speed mismatch
2. Remote to central site over-subscription
3. To prevent bursting above Committed Rate (CIR)

Enabling QoS in the WAN
Link Fragmentation and Interleaving (LFI)

Fragmentation and Interleave Not Needed on Links Greater than 768 kbps



Mechanisms:

Pt to Pt Links:	MLPPP
Frame Relay:	FRF.12
ATM:	MLPPP over ATM
ATM/Frame-Relay SIW:	MLPPP over ATM and FR

Fragment Size Recommendations

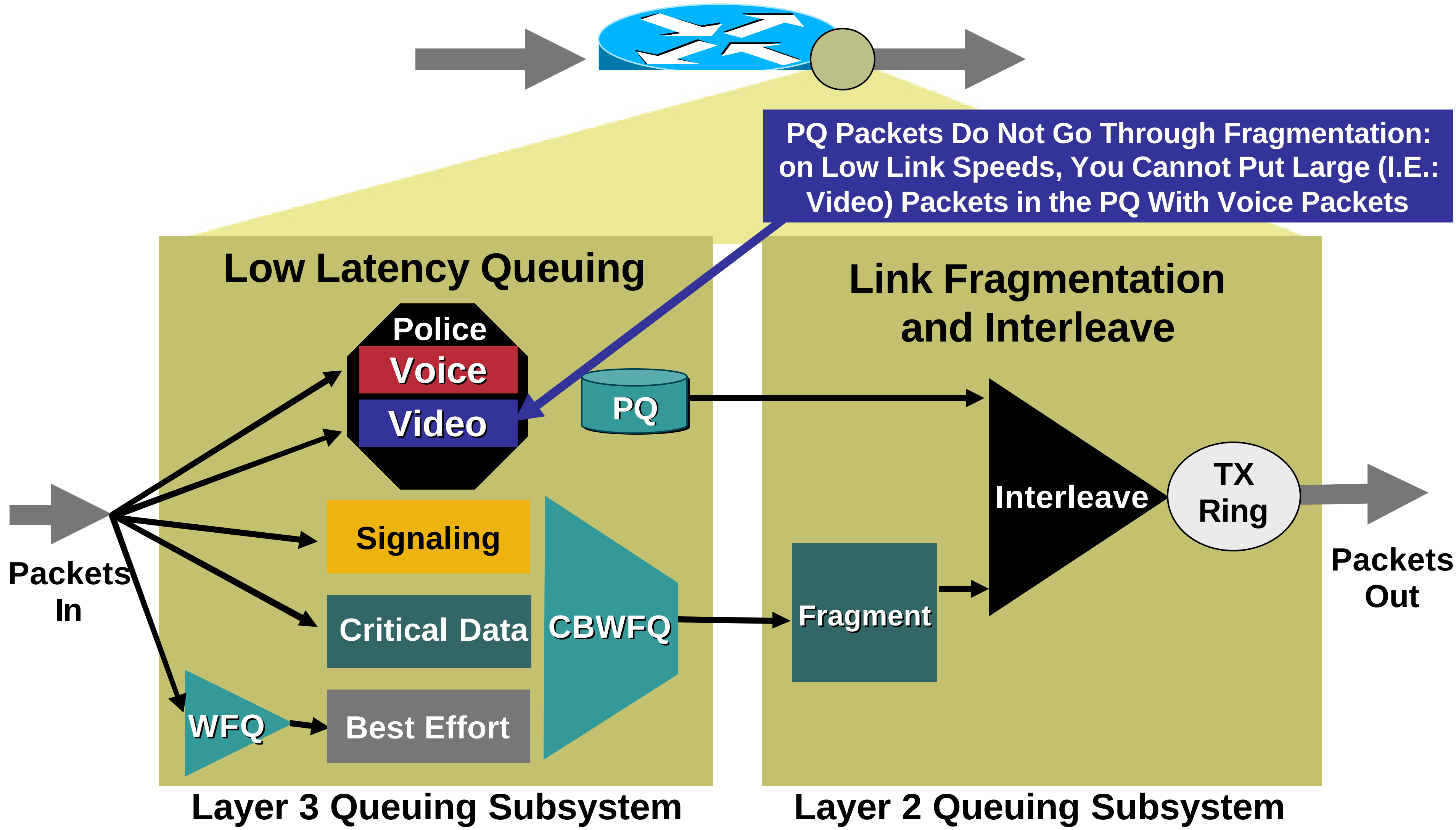
Serialization Delay Matrix

	64 Bytes	128 Bytes	256 Bytes	512 Bytes	1024 Bytes	1500 Bytes
56 kbps	9 ms	18 ms	36 ms	72 ms	144 ms	214 ms
64 kbps	8 ms	16 ms	32 ms	64 ms	128 ms	187 ms
128 kbps	4 ms	8 ms	16 ms	32 ms	64 ms	93 ms
256 kbps	2 ms	4 ms	8 ms	16 ms	32 ms	46 ms
512 kbps	1 ms	2 ms	4 ms	8 ms	16 ms	23 ms
768 kbps	640 used	1.2 ms	2.6 ms	5 ms	10 ms	15 ms

Fragmentation Size Matrix
(Based on 10 msec Delay)

PVC Speed	Frag Size
56 kbps	70 Bytes
64 kbps	80 Bytes
128 kbps	160 Bytes
256 kbps	320 Bytes
512 kbps	640 Bytes
768 kbps	1000 Bytes
1536 kbps	~~2000 Bytes~~

Network Infrastructure and QoS
Scheduling in the WAN



Enabling QoS in the WAN
Scheduling: TX-Ring Sizing

- **TX-Ring (TX-Queue on 7500 RSP) is an un-prioritized FIFO buffer which holds packets just before media transmission**
- **Used to make sure enough packets are queued in order to maximize available BW**
- **Will add to E-2-E delay numbers because serialization delay really equals:**

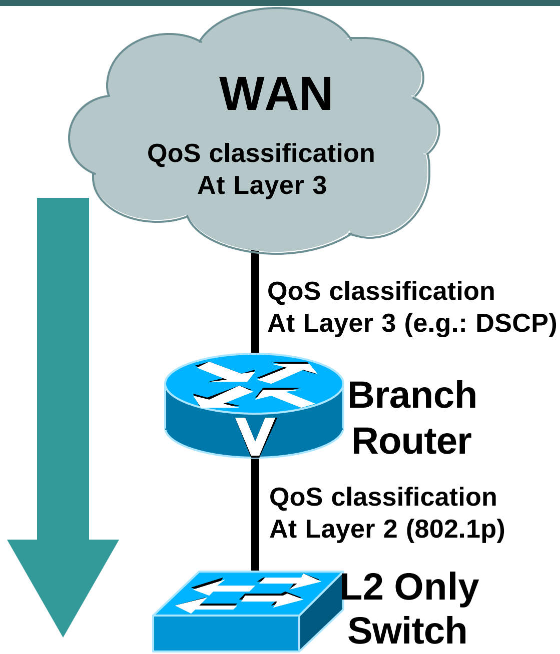
Serialization delay * number of packets in the TX-Ring buffer

Media	Default TX-Ring Buffer Sizing (Packets)
PPP	6
MLPPP	2
ATM	8192—Must Be Changed for Low Speed Vcs
Frame Relay	64 (Per Main E1 Interface)

Link Speed/ CIR/PVC	Default TX-Ring Buffer Sizing (Packets)
128 kbps	3
192 kbps	3
256 kbps	3
512 kbps	4
768 kbps	6

Gateways

QoS Settings for L3-to-L2 (L2-Only Switch)

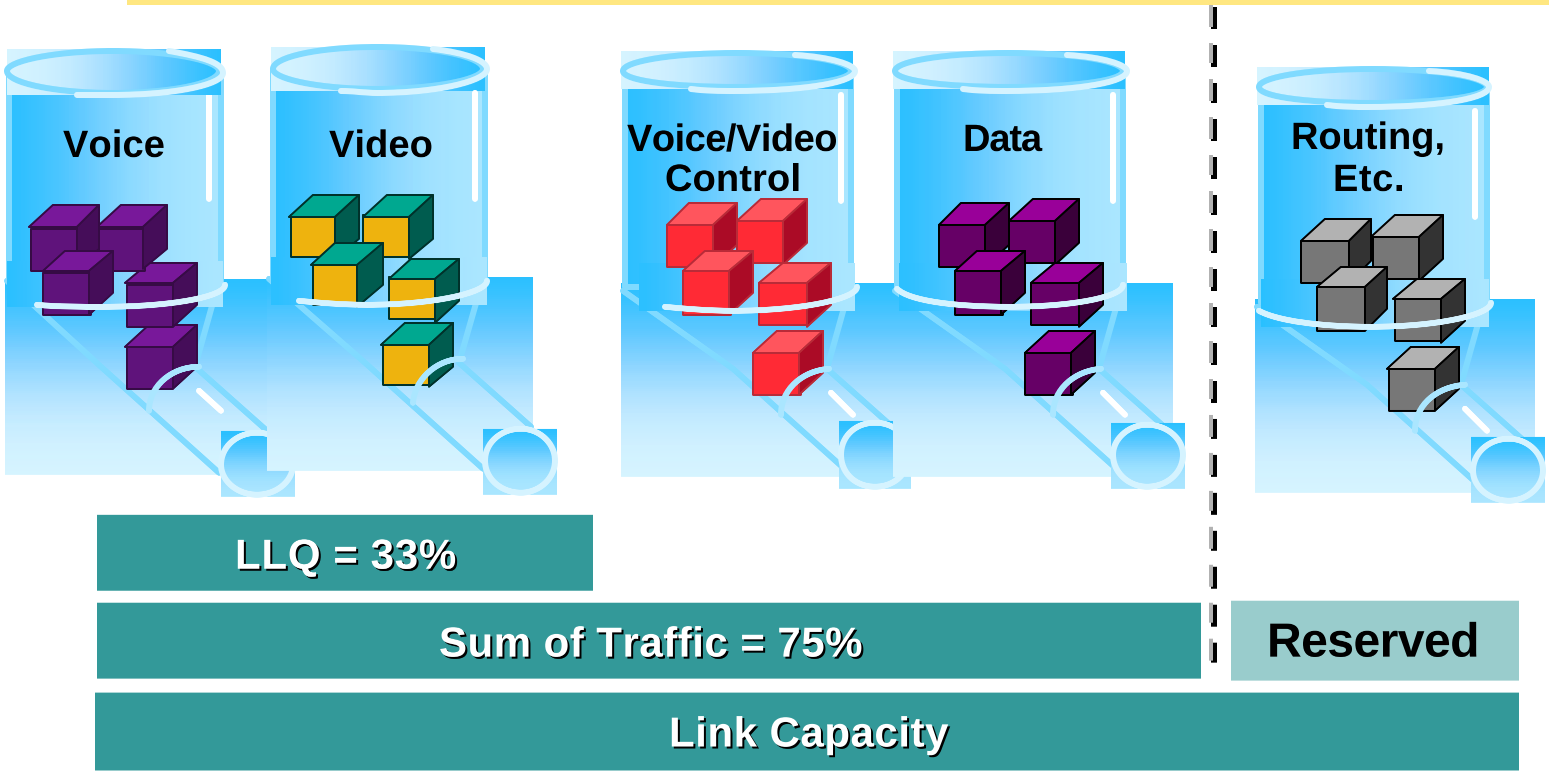



```
class-map match-all L3-2-L2-VoIP-RTP
  match ip dscp EF

class-map match-all L3-2-L2-VoIP-Control
  match ip dscp AF31; or CS3

policy-map output-L3-2-L2
  class L3-2-L2-VoIP-RTP
    set cos 5

   class L3-2-L2-VoIP-Control
    set cos 3
```

- Provides mapping of the DSCP in the IP header to the layer 2 CoS in the 802.1p ethernet header
- Applies to both H.323 and MGCP gateways
- Example based on Cisco IOS release 12.2 T

Enabling QoS in the WAN
Provisioning

**Voice Is Not Free—Especially on Low Speed Links—
Engineer the Network for Data, Voice, and Video**



Link Capacity = (Min BW for Voice + Min BW for Video + Min BW for Data)/0.75

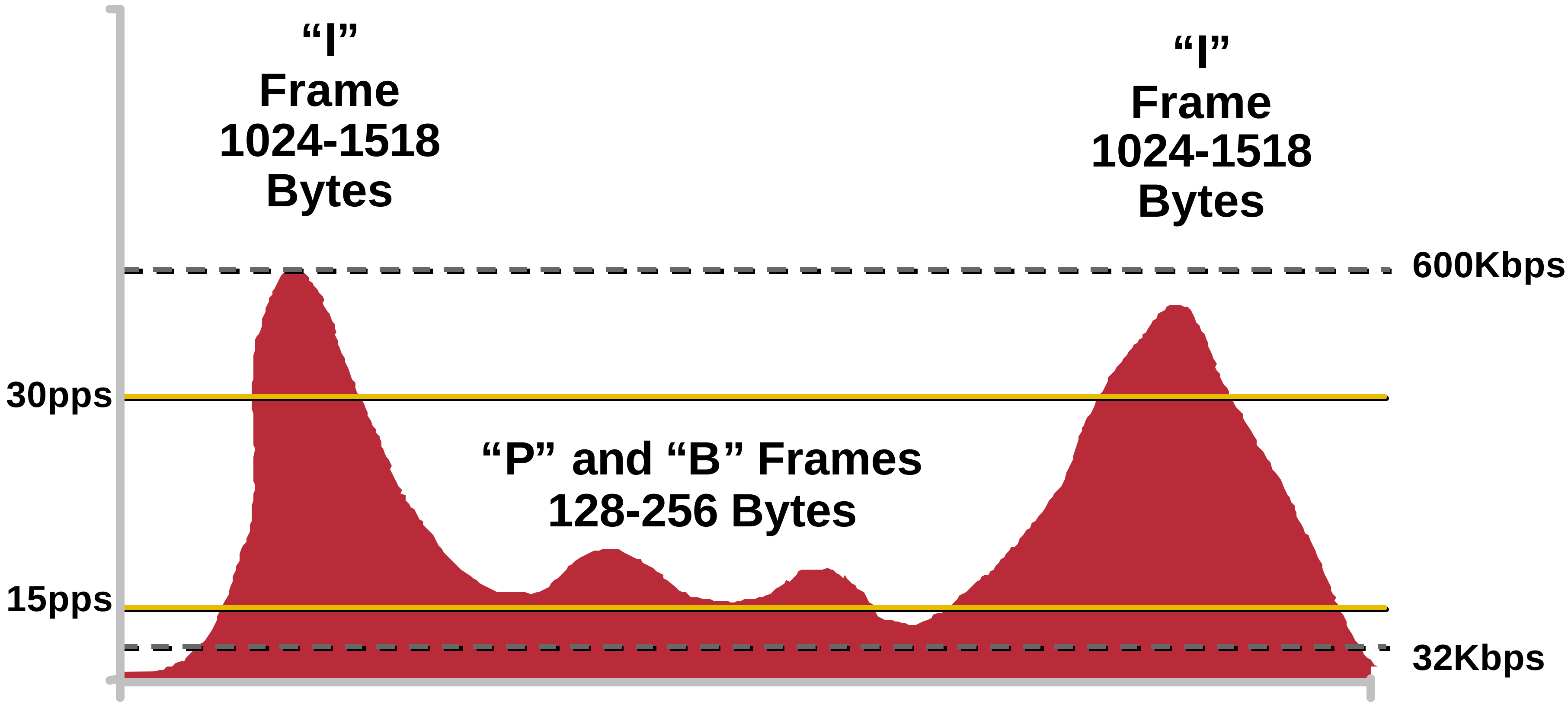
Enabling QoS in the WAN
Provisioning Tables for Voice Bearer Traffic

CODEC	Sampling Rate	Voice Payload in Bytes	Packets per Second	Bandwidth per Conversion
G.711	20 msec	160	50	80 kbps
G.711	30 msec	240	33	74 kbps
G.729A	20 msec	20	50	24 kbps
G.729A	30 msec	30	33	18 kbps

A More Accurate Method for Provisioning Is to Include the Layer 2 Headers into the Bandwidth Calculations:

CODEC	Ethernet 14 Bytes of Header	PPP 6 Bytes of Header	ATM 53 Bytes Cells with a 48 Byte Payload	Frame Relay 4 Bytes of Header
G.711 at 50 pps	85.6 kbps	82.4 kbps	106 kbps	81.6 kbps
G.711 at 33 pps	77.6 kbps	75.5 kbps	84 kbps	75 kbps
G.729A at 50 pps	29.6 kbps	26.4 kbps	42.4 kbps	25.6 kbps
G.729A at 33 pps	22.2 kbps	20 kbps	28 kbps	19.5 kbps

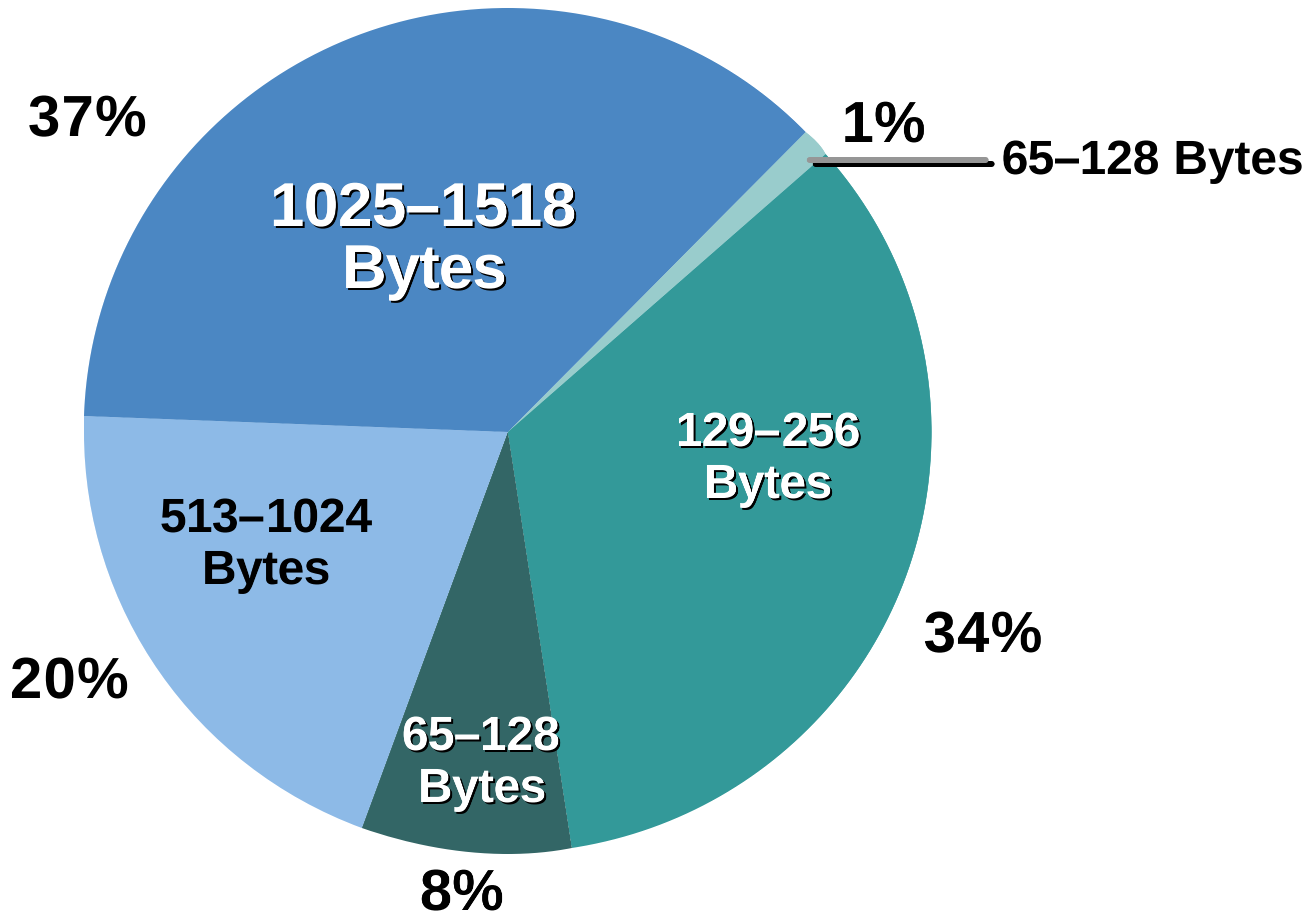
Bandwidth Requirements
Variability of Video Coders



- "I" frame is a full sample of the video
- "P" and "B" frames use quantization via motion vectors and prediction algorithms

Bandwidth Requirements
Average Packet Size

Video Conferencing Traffic Packet Size Breakdown



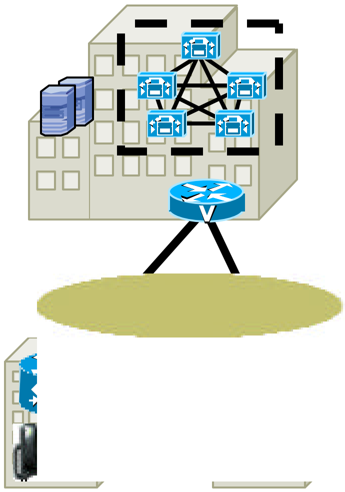
Bandwidth Requirements
Calculating Layer 2/3 Overhead

- Harder to calculate video because payload size is variable (Video is bursty!)
- General rule of thumb is to add 20% for all layer 2/ layer 3 overhead
- Call speed is typically the "maximum" transmission of the call. Average is usually much less

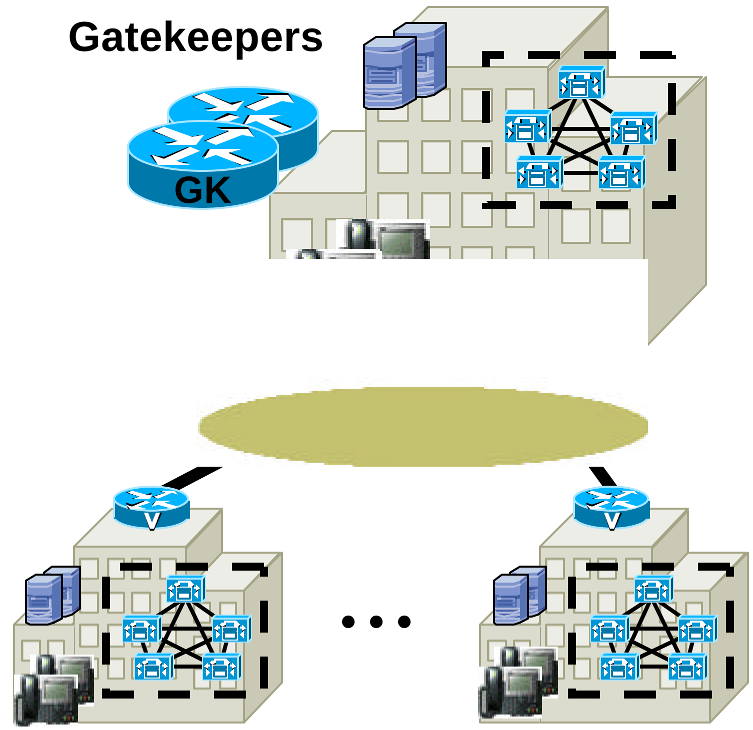
Video Data Rate and Bandwidth Required

128k = 153k
384k = 460k
512k = 614k
768k = 921k
1.5M = 1.8M

Enabling QoS in the WAN
Provisioning Tables for Signaling Traffic



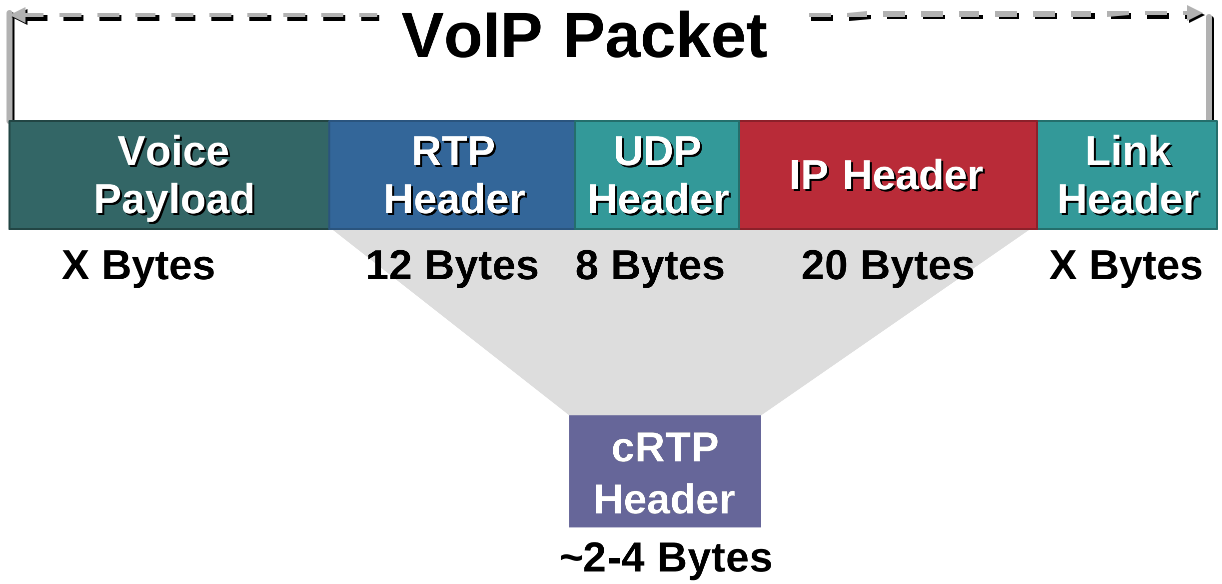
Centralized Call Processing	
# of IP Phones, Gateways	Bandwidth
1 to 30	8 kbps
50	11 kbps
100	23 kbps
150	34 kbps



Distributed Call Processing	
# of Virtual Tie Lines	Bandwidth
1 to 70	8 kbps

Enabling QoS in the WAN
Provisioning with Compressed RTP (cRTP)

- **Compresses RTP+ UDP+ IP headers (40 bytes) down to 2-4 bytes**
- **Enabled on a per-link basis**



CODEC	PPP 6 Bytes of Header	ATM 53 Bytes Cells with a 48 Byte Payload	Frame-Relay 4 Bytes of Header
G.711 at 50 pps	68 kbps	85 kbps	67 kbps
G.711 at 33 pps	66 kbps	84 kbps	65.5 kbps
G.729A at 50 pps	12 kbps	21.2 kbps	11.2 kbps
G.729A at 33 pps	10.5 kbps	14 kbps	10 kbps

For more information: http://cco/en/US/partner/tech/tk543/tk762/technologies_tech_note09186a0080108e2c.shtml

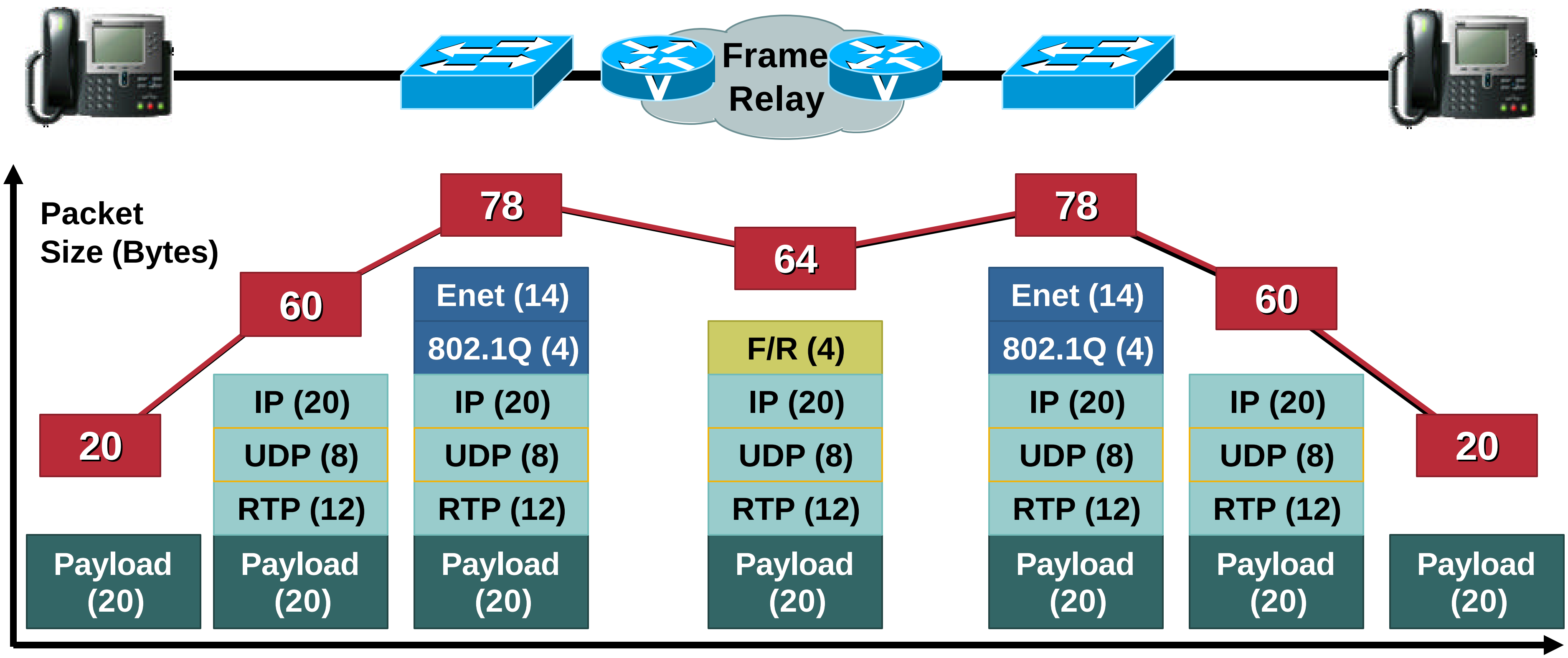
Enabling QoS in the WAN

A Day in the Life of a VoIP Packet: Without cRTP

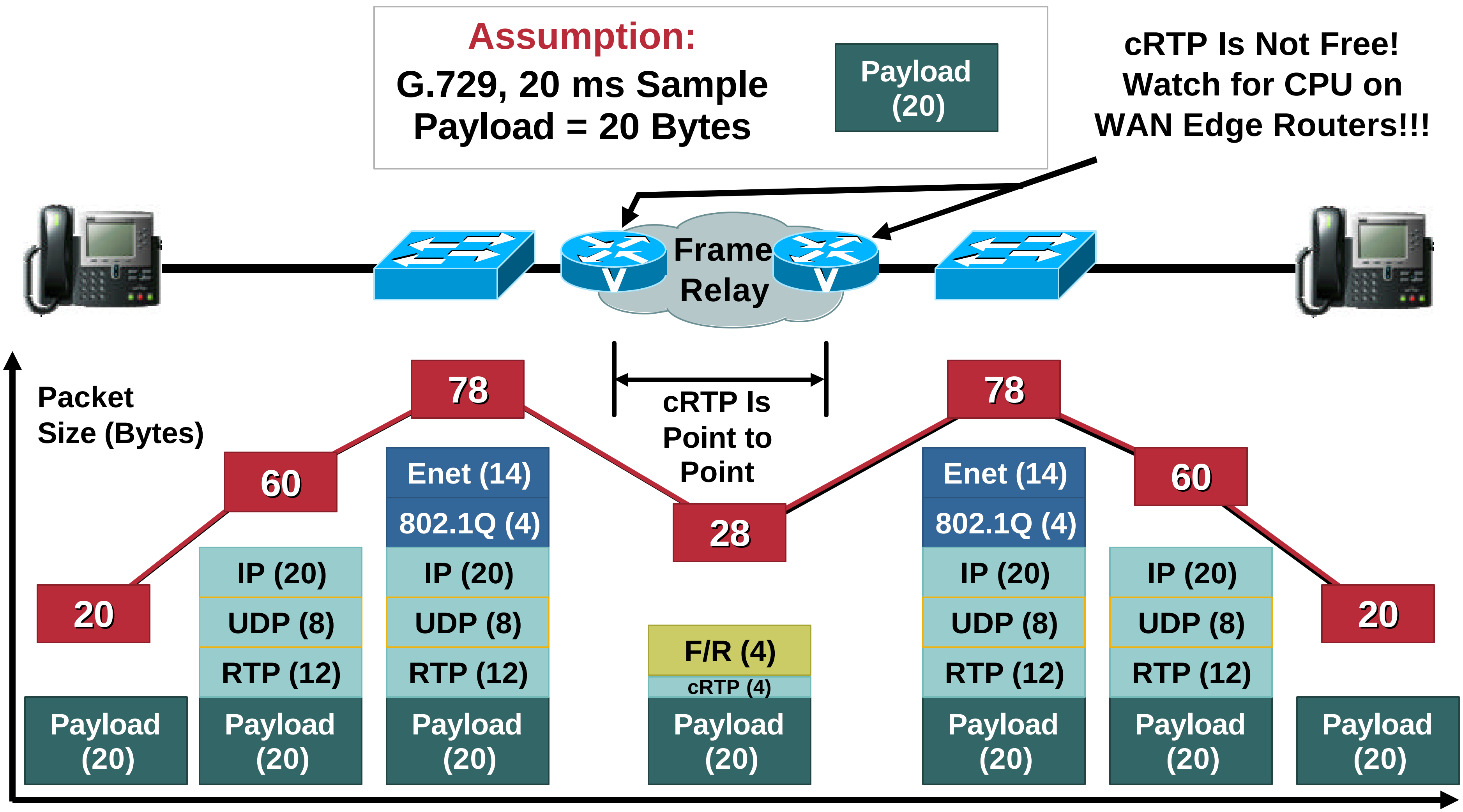
Assumption:

G.729, 20 ms Sample
Payload = 20 Bytes

Payload (20)



Enabling QoS in the WAN
A Day in the Life of a VoIP Packet: With cRTP



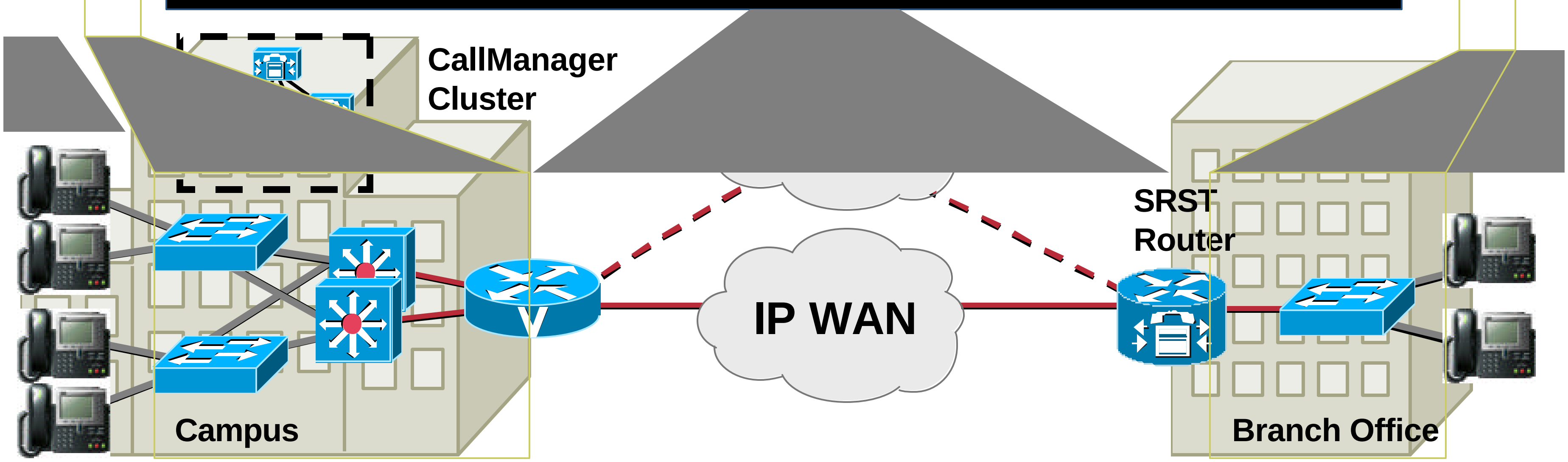
Enabling QoS in the WAN
QoS Approach Summary

Classification: Mark the Packets with a Specific Priority Denoting a Requirement for Class of Service from the Network

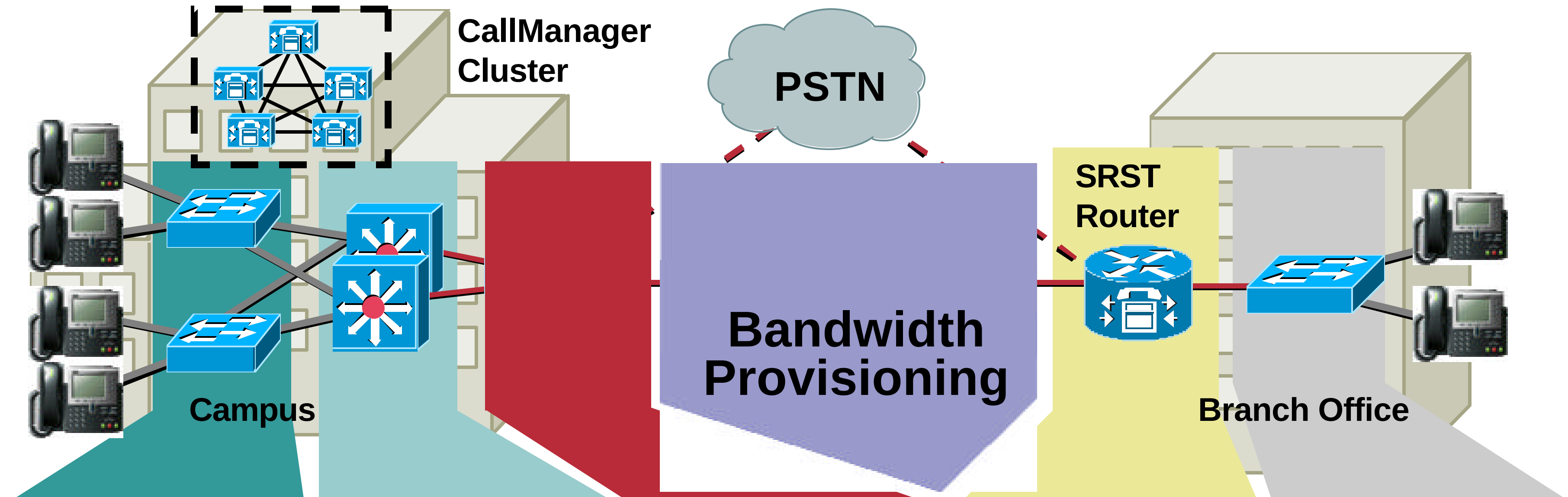
Trust Boundary: Define and Enforce a Trust Boundary at the Network Edge

Scheduling: Assign Packets to One of Multiple Queues (Based on Classification) for Expedited Treatment through the Network

Provisioning: Accurately Calculate the Required Bandwidth for All Applications Plus Element Overhead



Enabling QoS in the WAN
Overall QoS Design Summary



Campus Access

- Inline power
- Multiple Q's
- 802.1p/Q
- Fast link convergence

Campus Distribution

- Multiple Q's
- 802.1p/Q
- Classification
- Reclassification

WAN Aggregation

- Multiple Q's
- 802.1p/Q
- Traffic shaping
- Link efficiency (LFI, cRTP)
- Classification
- Reclassification

Branch Router

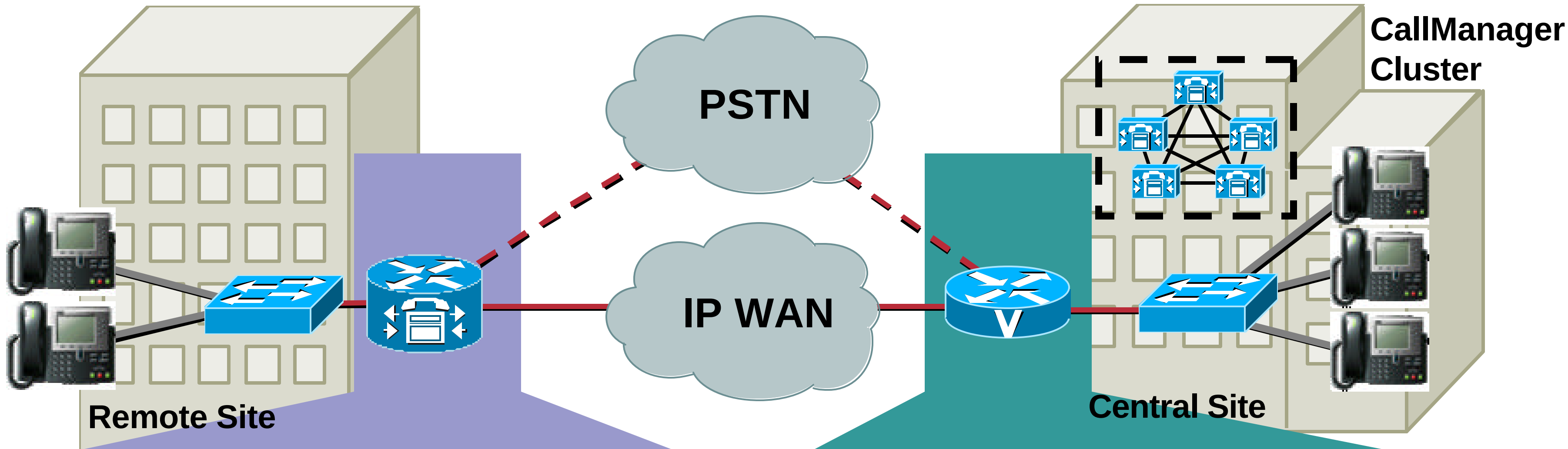
- Multiple Q's
- 802.1p/Q
- Link efficiency (LFI, cRTP)
- Classification
- Reclassification

Branch Switch

- Inline power
- Multiple Q's
- 802.1p/Q

Building a WAN
Platform Recommendations

Cisco.com



- Cisco 38xx
- Cisco 28xx
- Cisco 18xx

- Cisco 75xx
- Cisco 72xx
- Cisco 38xx

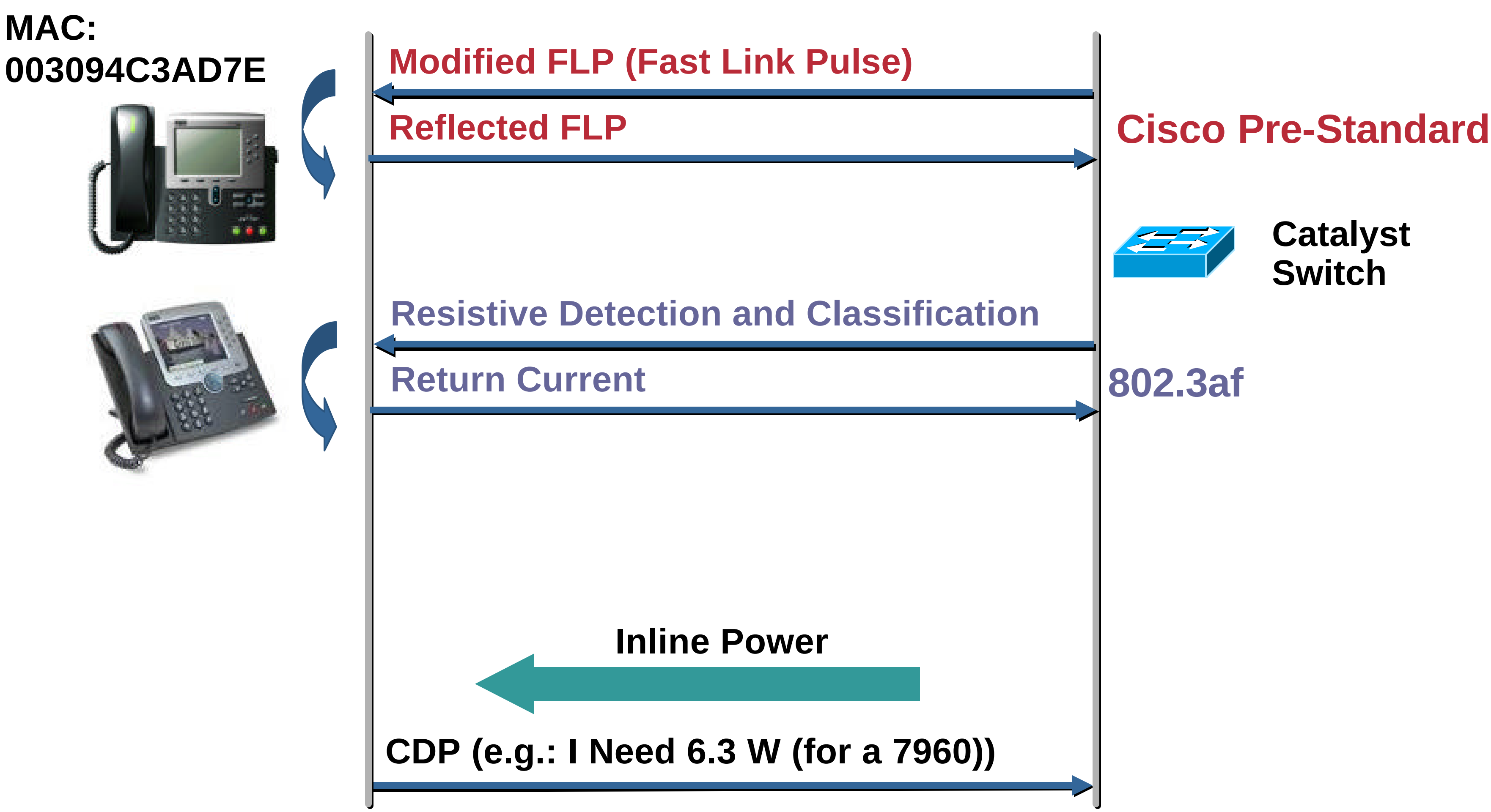
Network Infrastructure Agenda

- Building a Campus Network
- Enabling QoS in the Campus
- Providing Inline Power to IP Phones
- Overlaying Wireless LANs
- Building a WAN
- Enabling QoS in the WAN
- Networks Services

Networks Services

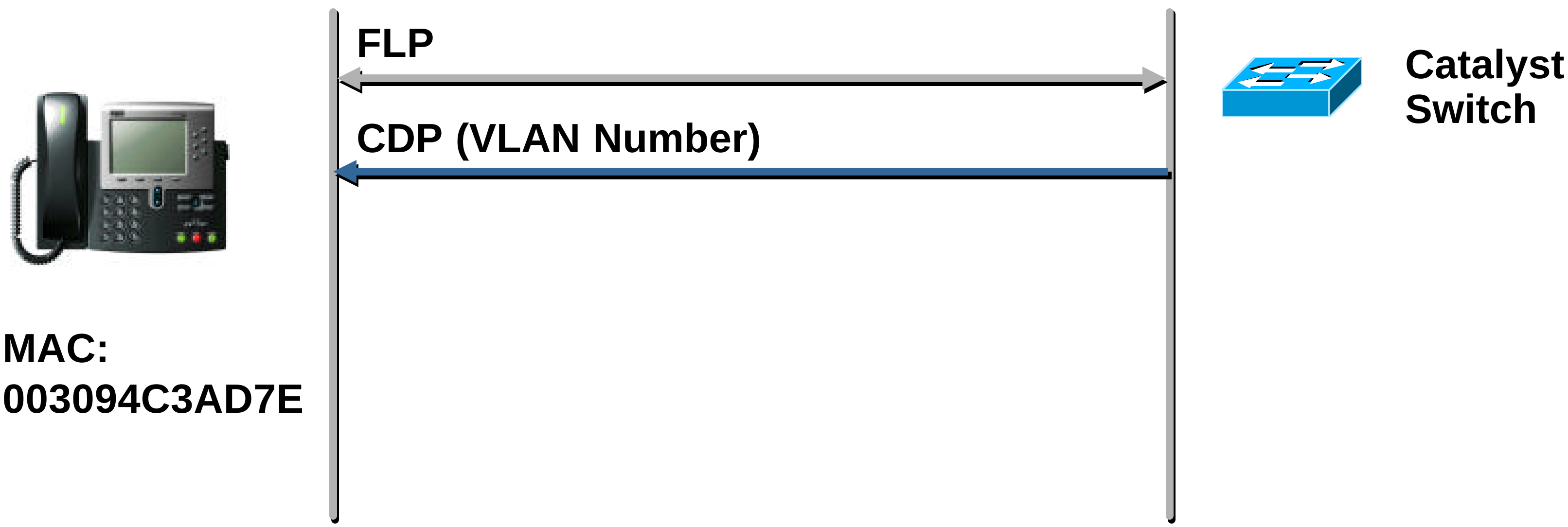
- **CDP puts phone in correct VLAN/Subnet and allows for proper power computation**
- **DHCP used to automate network access**
  - **DHCP server needs to provide the following:**
    - **IP Address and network mask**
    - **Default Gateway**
    - **Option 150, TFTP server**
    - **DNS Server (optional)**
  - **Can be centrally managed (IP helper address)**
  - **Can be locally implemented (e.g.: IOS DHCP server function)**
- **TFTP server provides configuration file and phone s/w distribution to endpoints (e.g.: phones)**
- **DNS server is optional: try to not use, unless NAT is used**

IP Phone Initialization: Inline Power



Phone: Mute, Headset, Speaker Buttons Illuminated

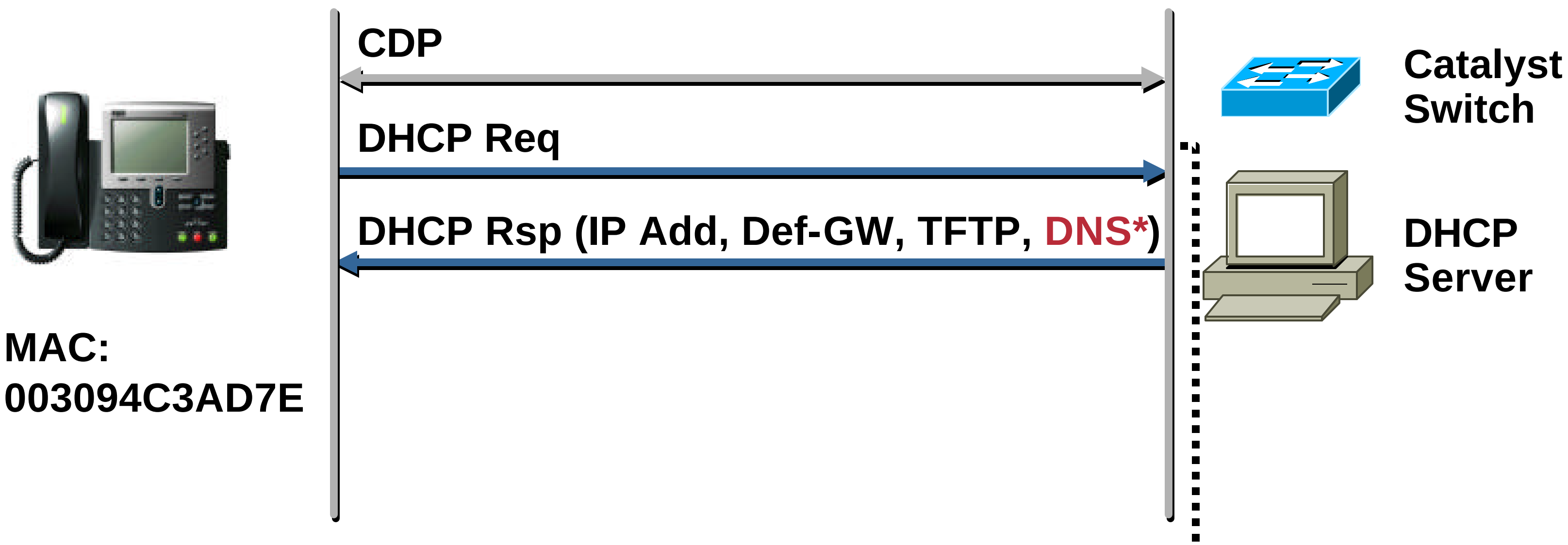
IP Phone Initialization: AUX VLAN



Phone Displays: Configuring VLAN

Check Settings: NetCfg->19 Operational VLAN ID

IP Phone Initialization: IP Configuration



DHCP Request Must Be Made in the Correct VLAN to Place the Phone in the Correct Subnet!!

Phone Displays: Configuring IP

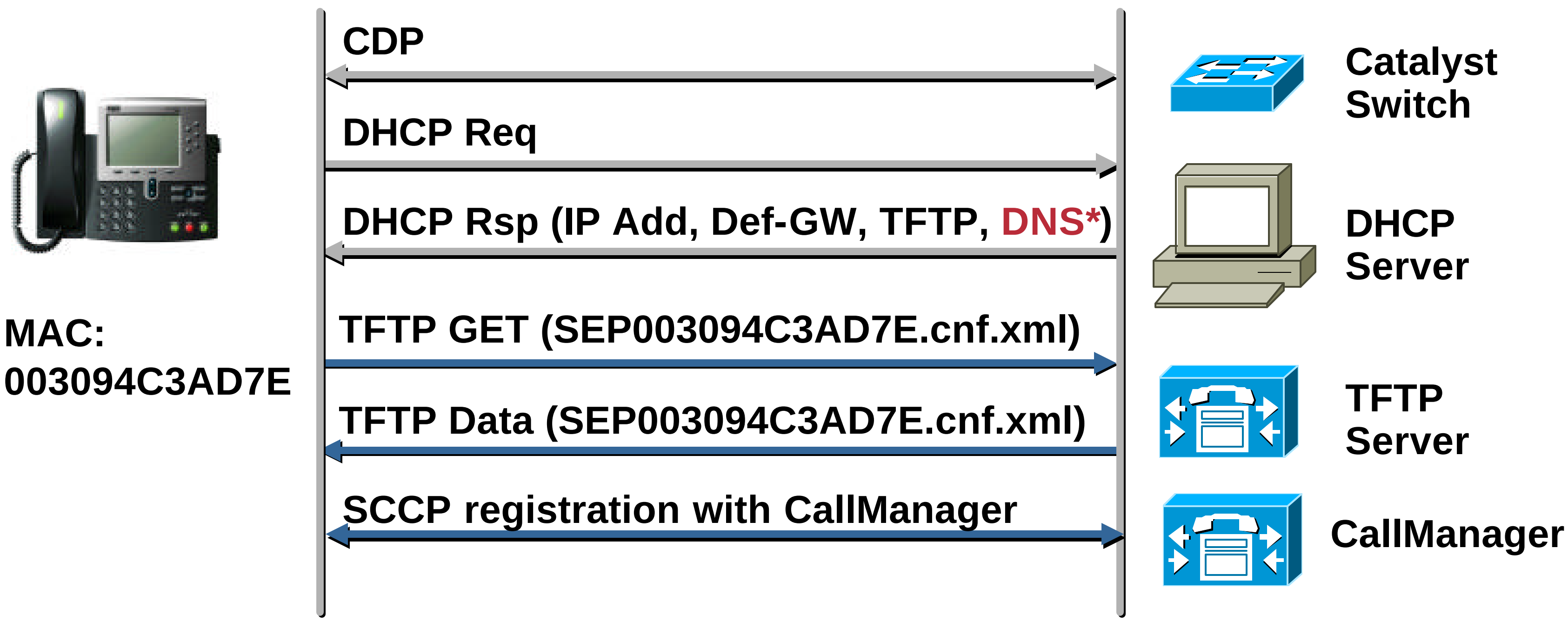
***DNS Is Optional**

Check Settings: NetCfg-> 1 DHCP Server

NetCfg-> 6 IP Address

IP Phone Initialization: TFTP and SCCP

Cisco.com

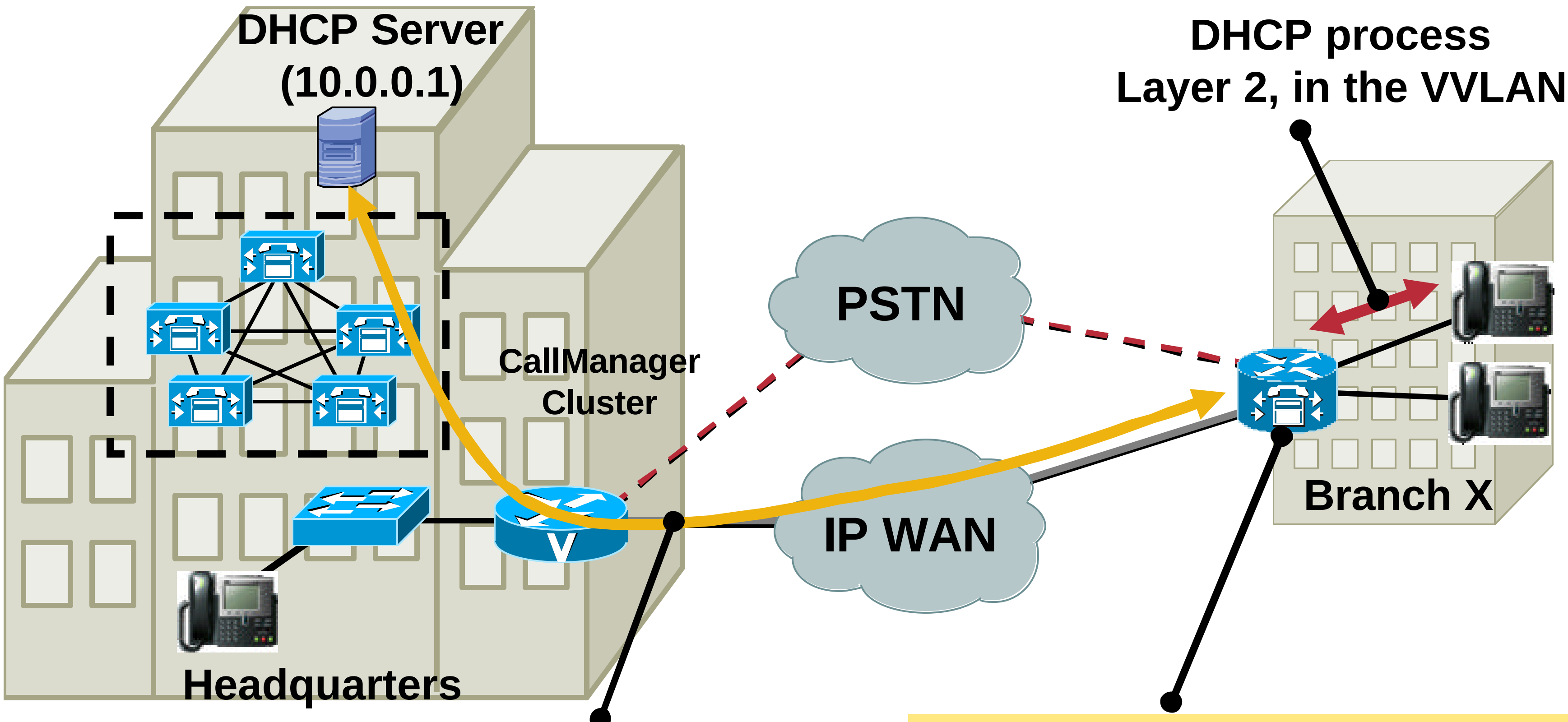


Phone Displays: Configuring IP

Error Verifying Config Info

Check settings: NetCfg-> 8 TFTP Server

Networks Services: DHCP

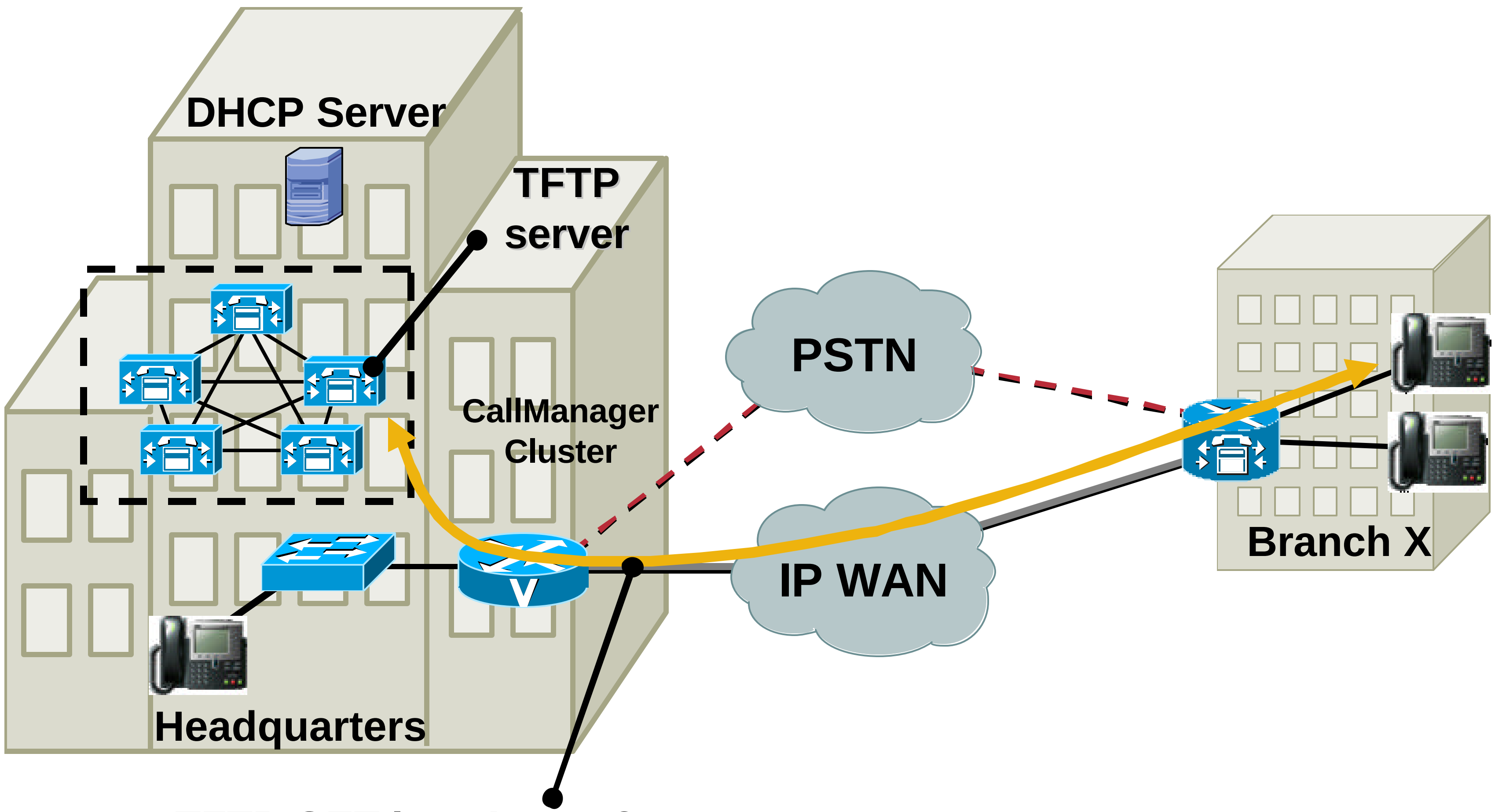


- **DHCP process tunneled at Layer 3**
- **DHCP relay agent (ip helper-address)**
- **Identification of scope relies on router ID (typically the default gateway's IP address)**

```
(under VVLAN interface)
ip address 10.1.1.1 255.255.255.0
ip helper-address 10.0.0.1
```

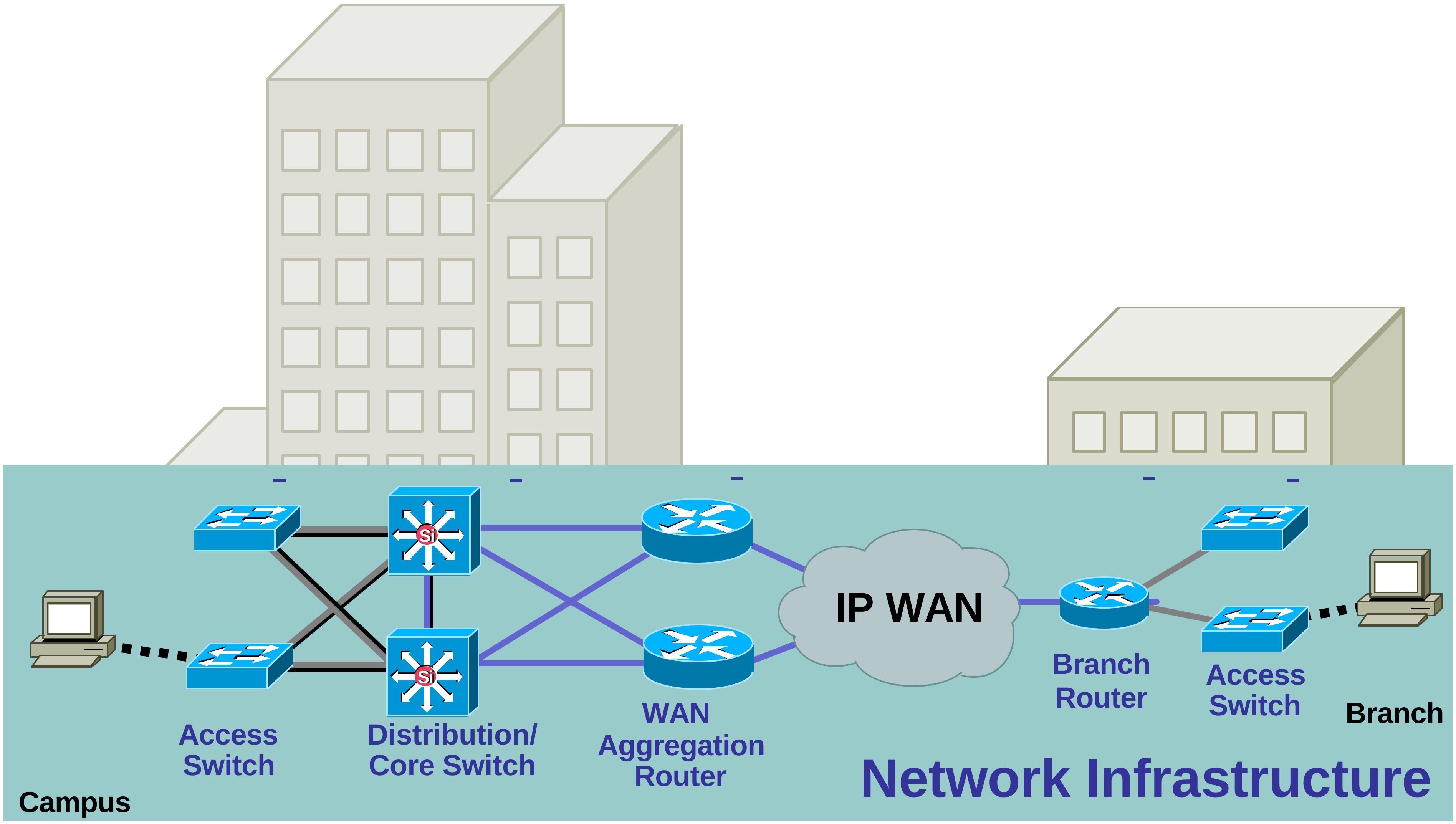
Networks Services: TFTP

Cisco.com



TFTP GET Is at Layer 3
Ubiquitous, Just Requires IP Connectivity

What We Have Built So Far



Agenda

- Introduction
- Network Infrastructure
- Telephony Infrastructure
- Legacy Migration and Integration

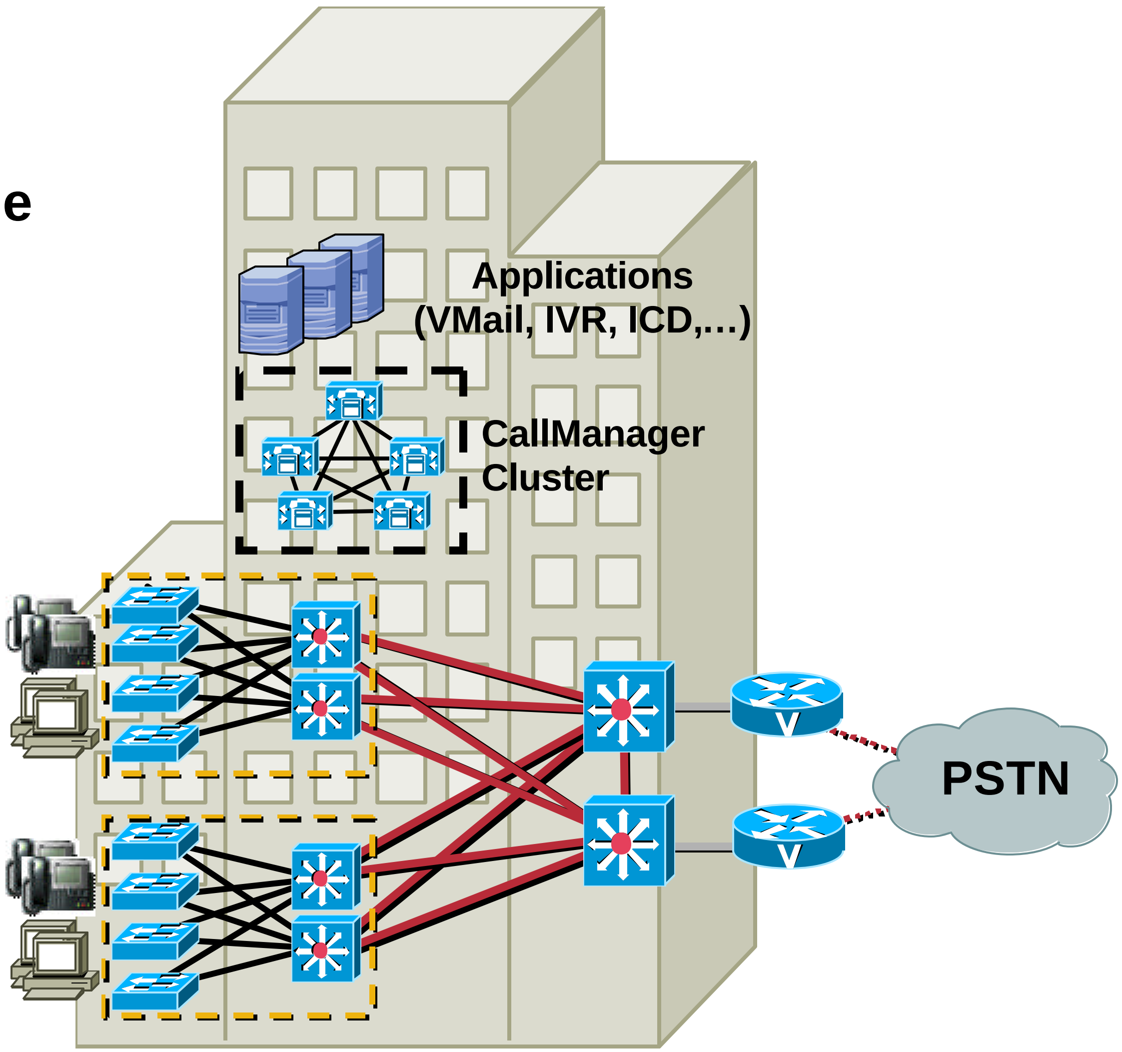
Telephony Infrastructure Agenda (1/2)

- Deployment Models
- Basic Call Processing
- Signaling Protocols
- Gateways
- Media Resources
- Call Processing

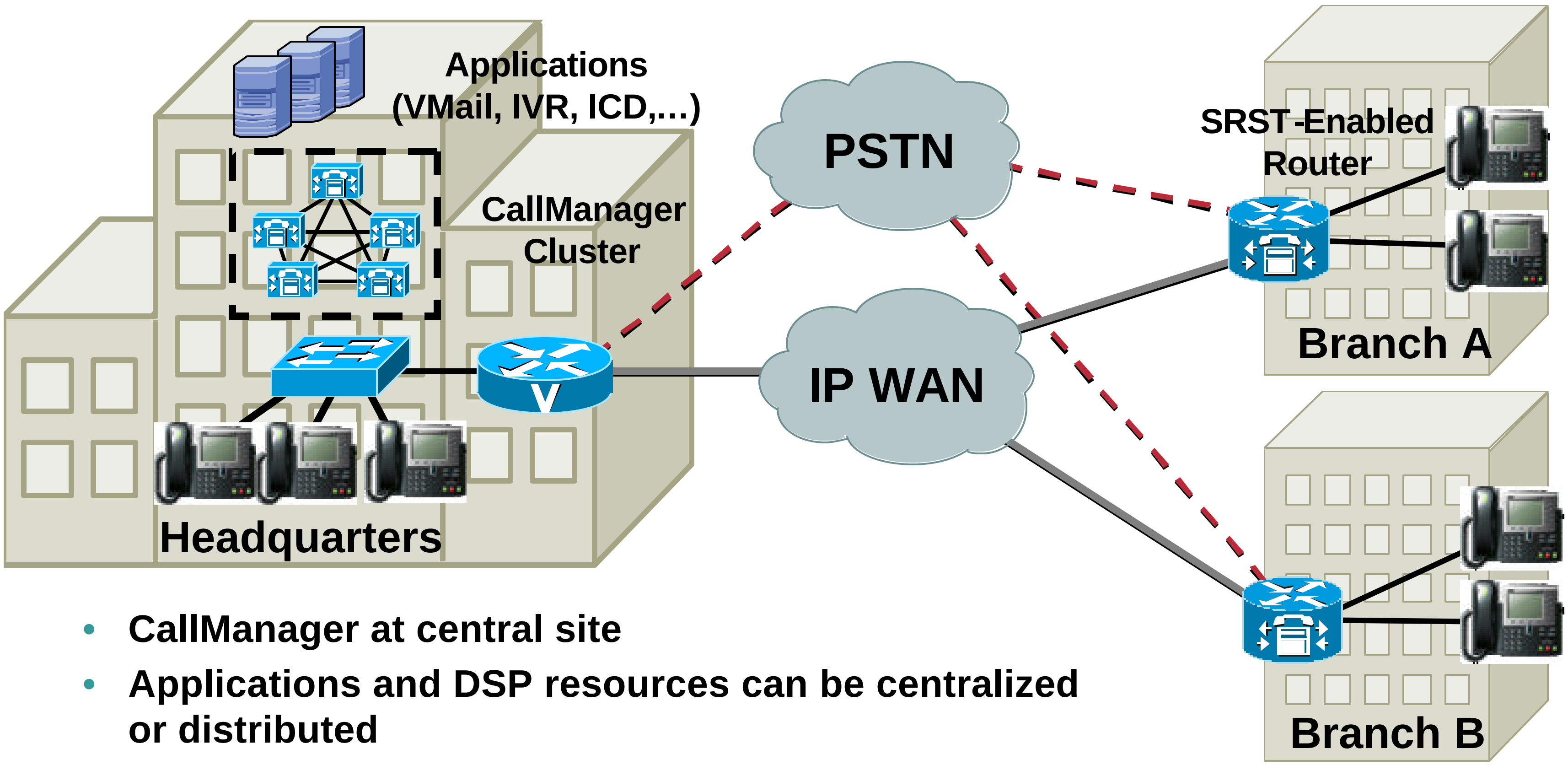
Deployment Models
Single Site

Cisco.com

- Cisco CallManager, applications and DSP resources at same physical location
- Supports up to 30,000 lines per cluster
- Multiple clusters can be interconnected via inter-cluster trunks
- PSTN used for all external calls



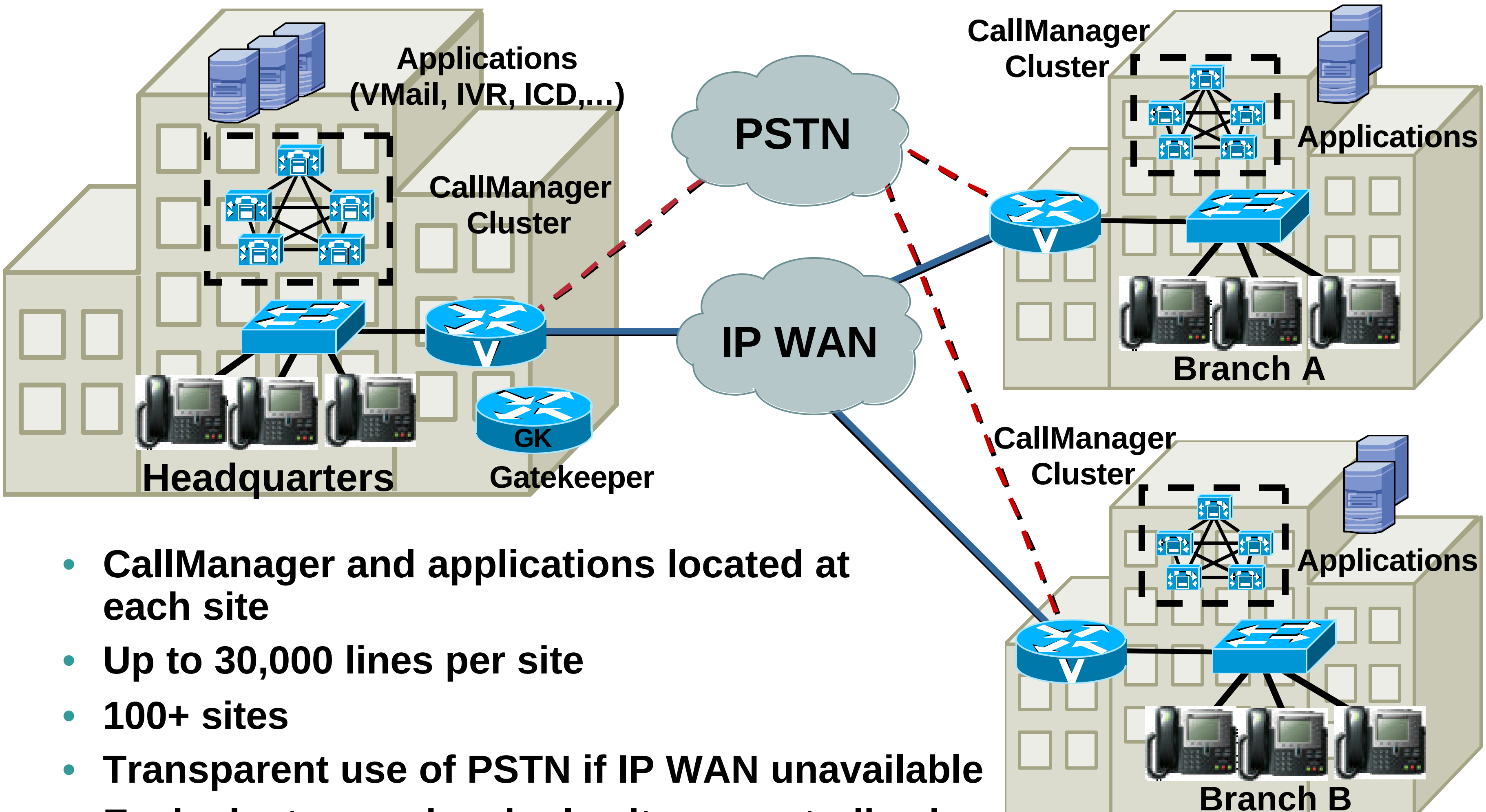
Deployment Models
Centralized Call Processing



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

Deployment Models
Distributed Call Processing

Cisco.com



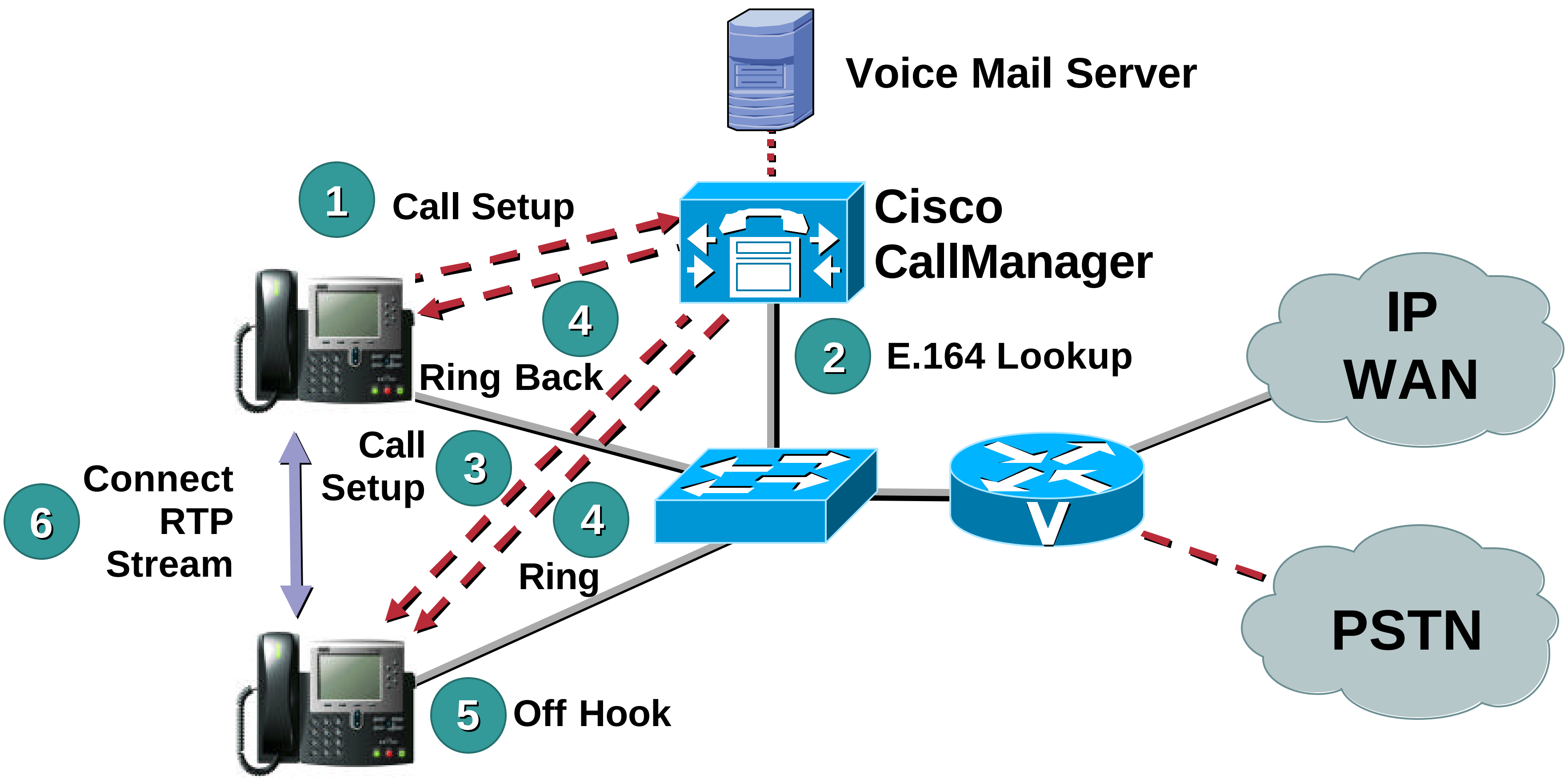
- CallManager and applications located at each site
- Up to 30,000 lines per site
- 100+ sites
- Transparent use of PSTN if IP WAN unavailable
- Each cluster can be single site or centralized call processing topology

Telephony Infrastructure Agenda (1/2)

- Deployment Models
- Basic Call Processing
- Signaling Protocols
- Gateways
- Media Resources
- Call Processing

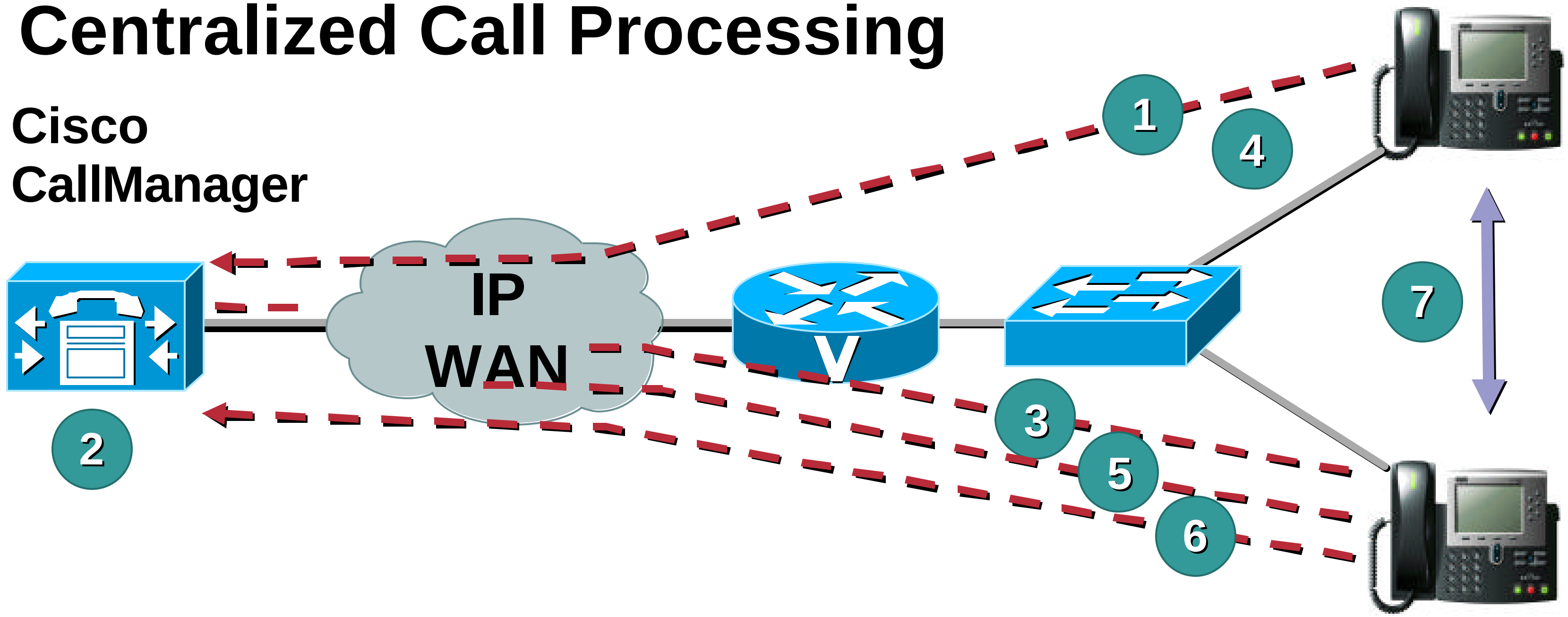
Basic Call Processing

Single Site



Basic Call Processing

Centralized Call Processing

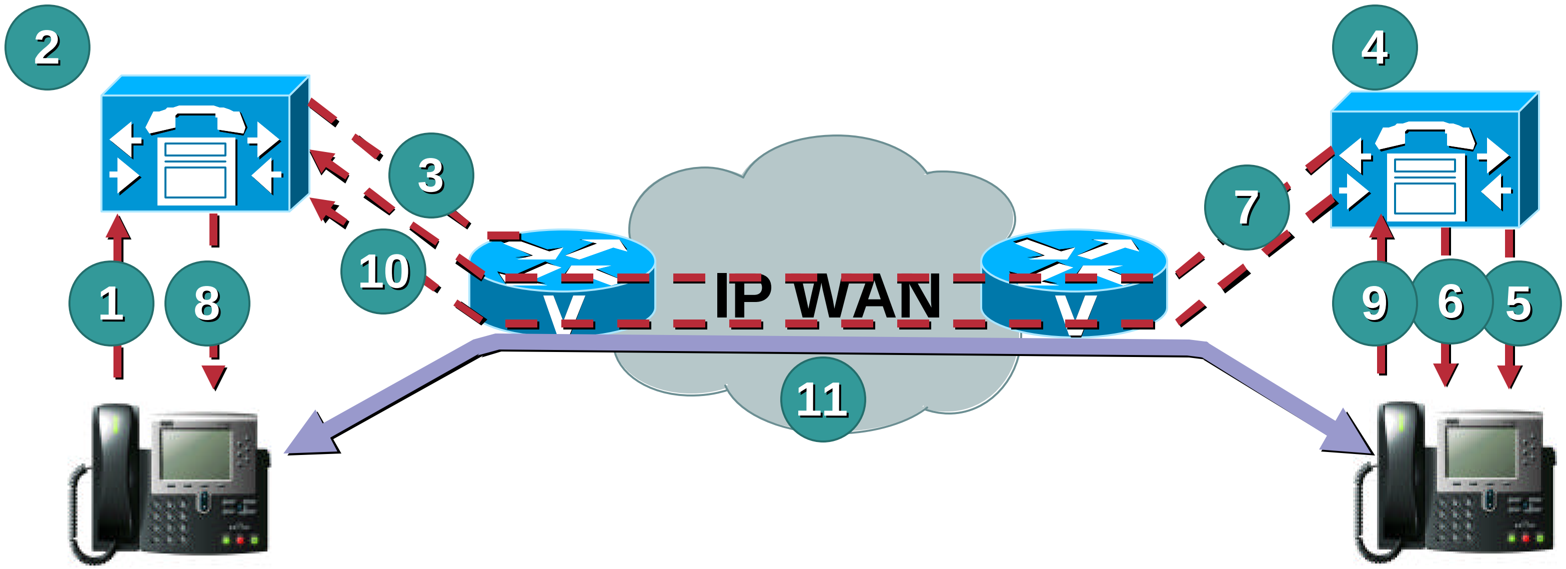


1. Call Setup
2. E.164 Lookup
3. Call Setup
4. Ring Back
5. Ring
6. Off Hook
7. Connect RTP Stream

Call Processing Is Essentially the Same in this Deployment Model as in the Single Site Case; IP Makes the Technology More Topology Independent

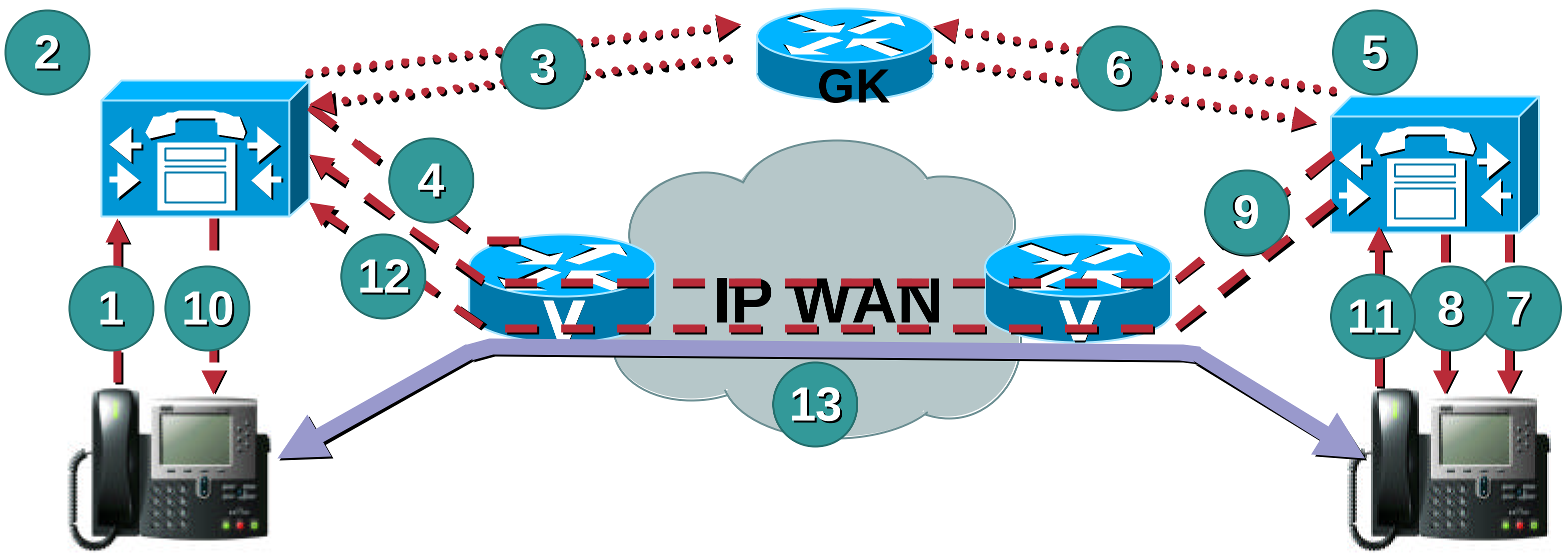
Basic Call Processing
Distributed Call Processing

Cisco.com



1	Call Setup	5	Call Setup	9	Off Hook
2	E.164 Lookup	6	Ring	10	Call Connect
3	Call Setup	7	Alerting	11	Connect RTP Stream
4	E.164 Lookup	8	Ringback		

Basic Call Processing
Distributed Call Processing with Gatekeeper

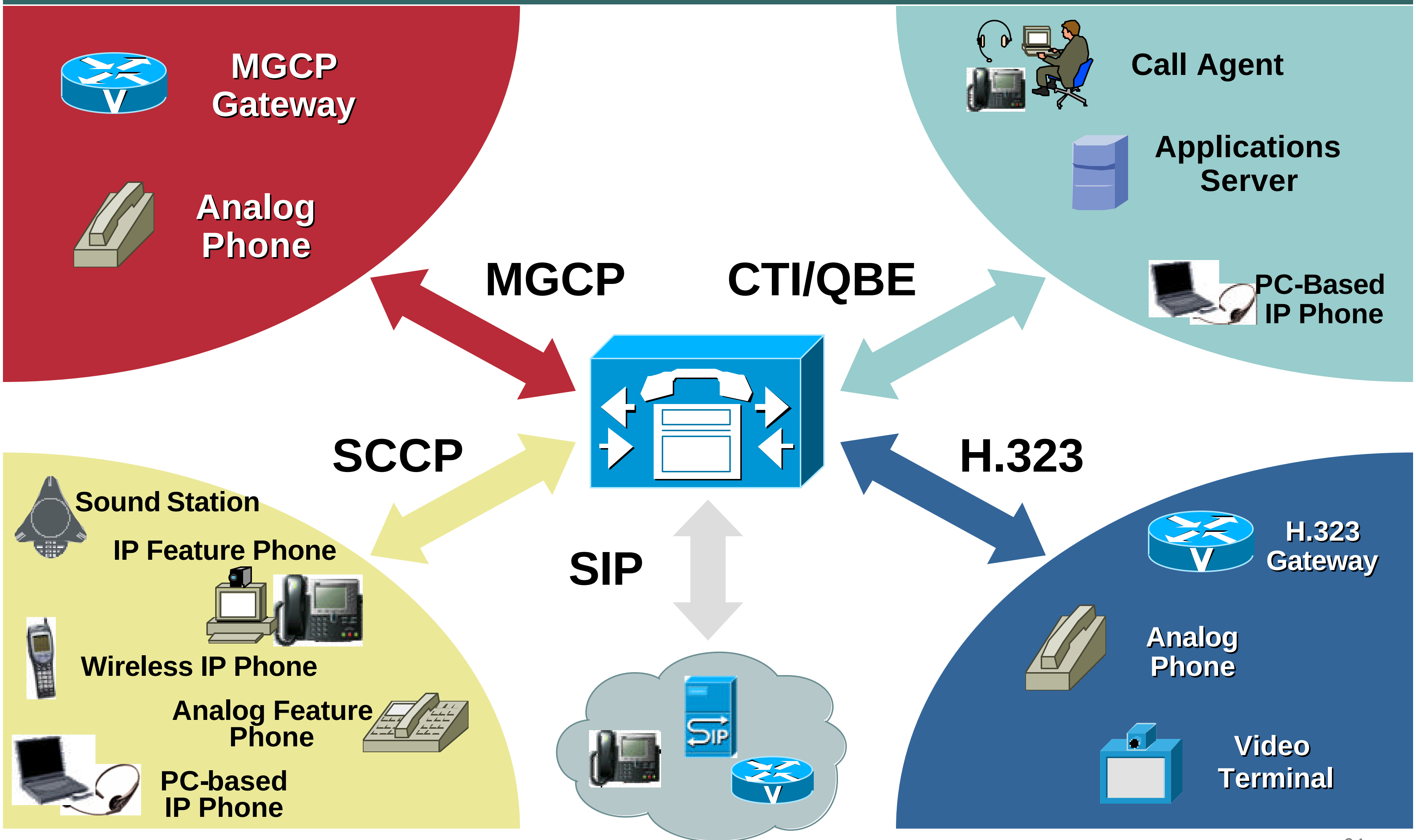


1	Call Setup	6	Call Admission				
2	E.164 Lookup	7	Call Setup				
3	Call Admission/ Dial Plan resolution	8	Ring	11	Off Hook		
4	Call Setup	9	Alerting	12	Connect		
5	E.164 Lookup	10	Ringback	13	Connect RTP Stream		

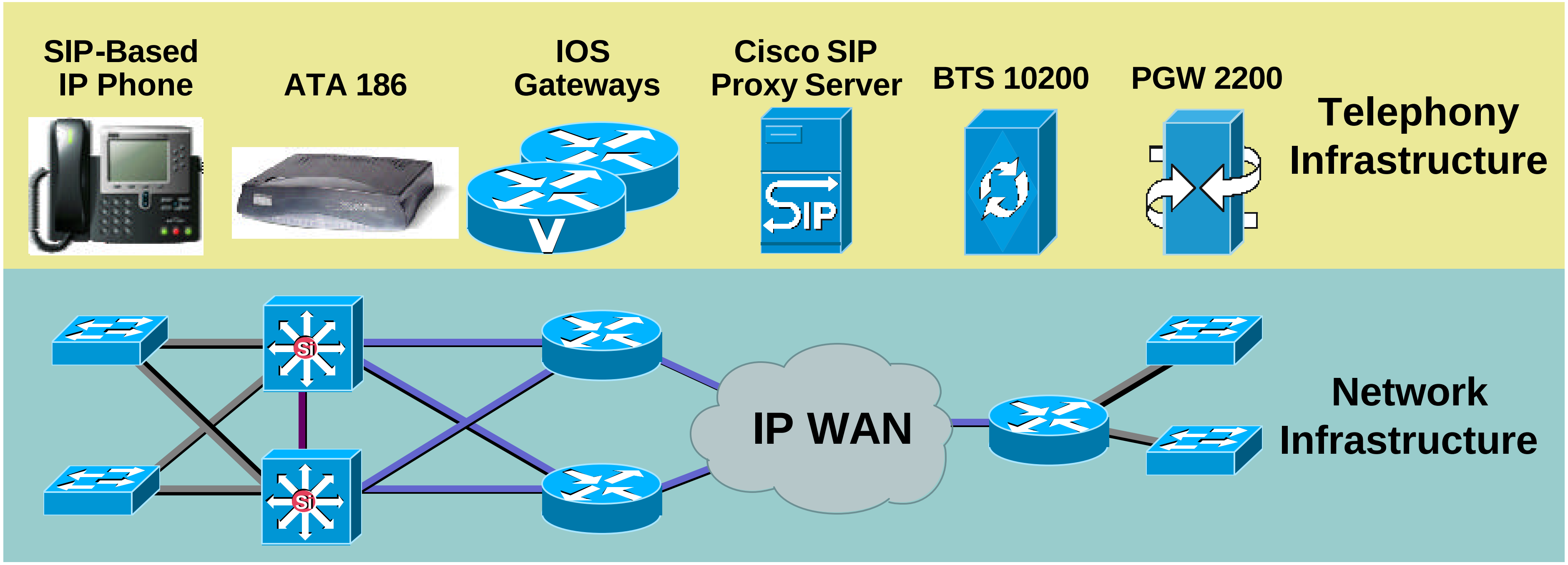
Telephony Infrastructure Agenda (1/2)

- Deployment Models
- Basic Call Processing
- Signaling Protocols
- Gateways
- Media Resources
- Call Processing

Signaling Protocols
CallManager as a "Protocol Translator"



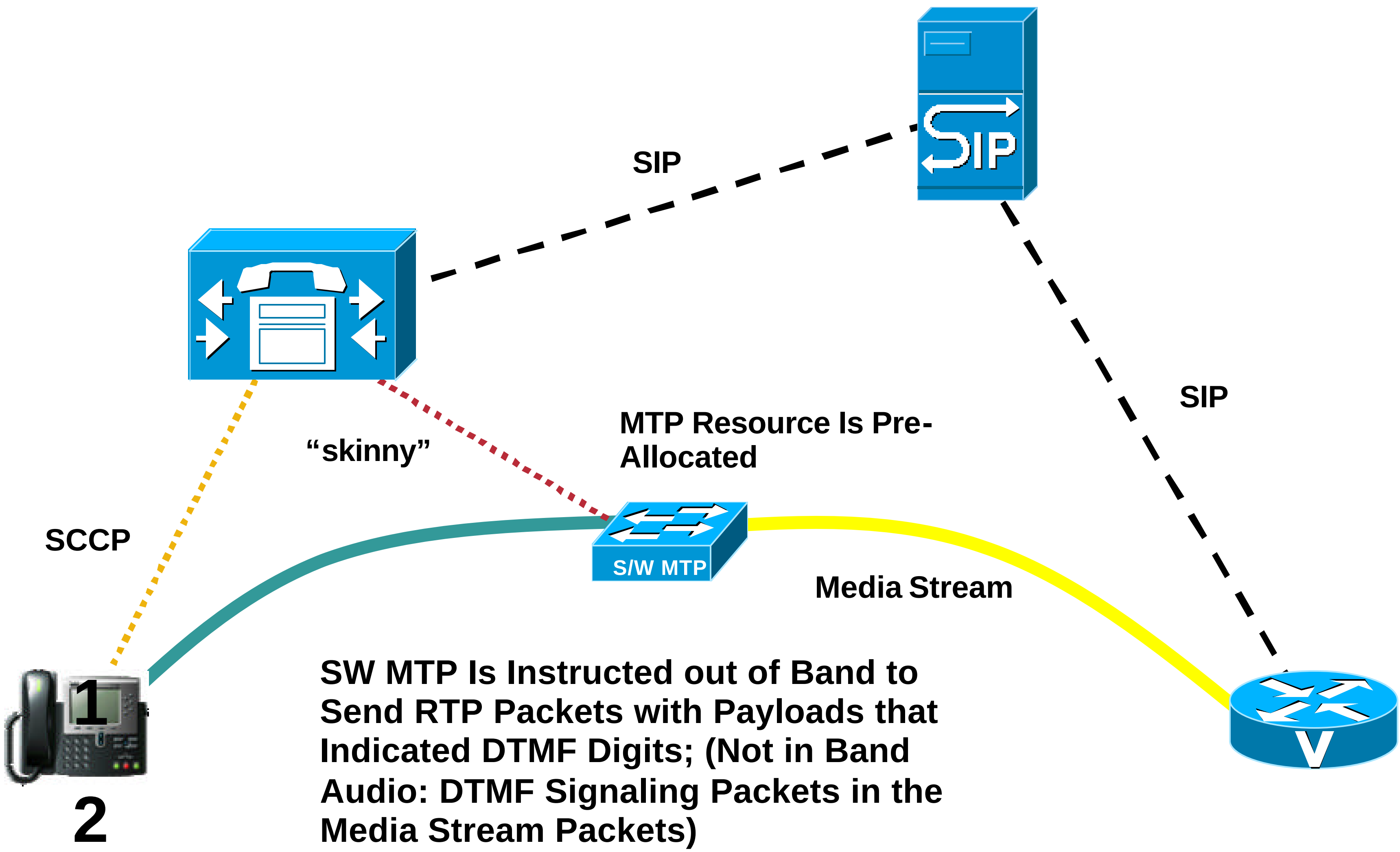
Signaling Protocols
More about SIP



- Several Cisco voice products already support SIP
- The network infrastructure is independent of the signaling protocol
- Many PBX features cannot be delivered natively using SIP today
- SIP trunk available today in CallManager

SIP Trunk
RFC 2833 DTMF Relay

Cisco.com



SW MTP Is Instructed out of Band to Send RTP Packets with Payloads that Indicated DTMF Digits; (Not in Band Audio: DTMF Signaling Packets in the Media Stream Packets)

SIP Trunk

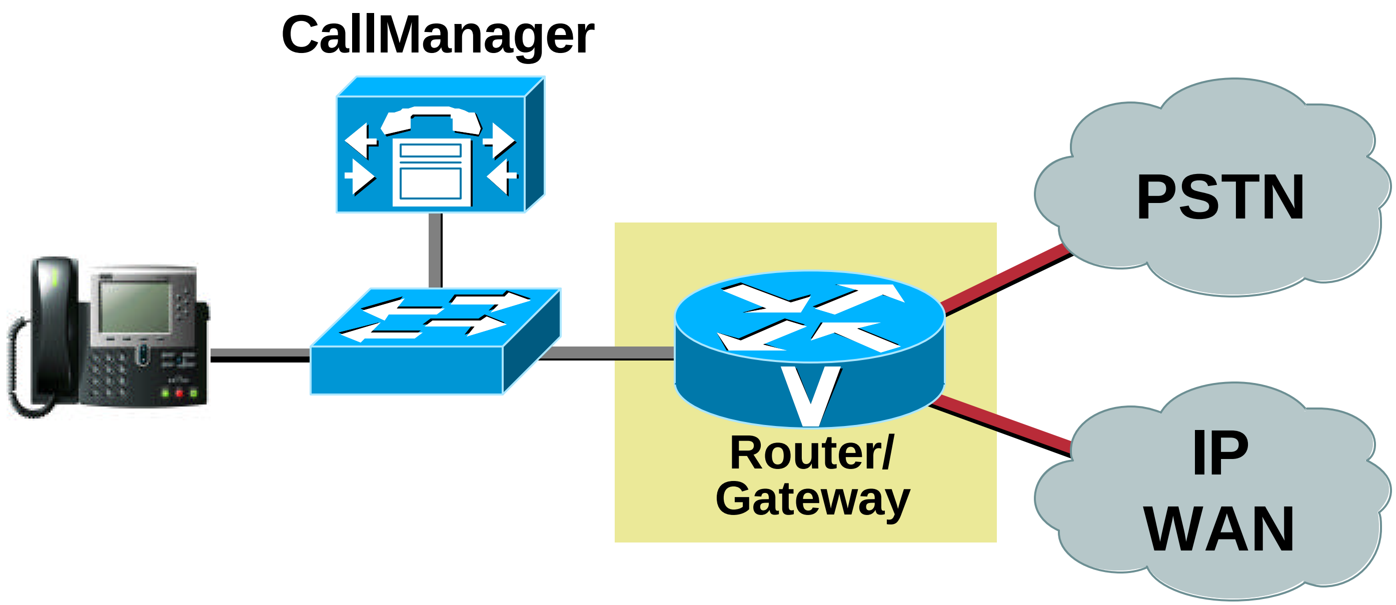
- Provides voice connectivity to SIP from H.323, SCCP, CTI/QBE and MGCP voice devices
- Must use a software MTP (hardware support to follow)
- Does not support video
- DTMF is relayed using RFC2833
- SIP Trunk does not register with Proxy/Registrar
- Subset of SIP messages supported (e.g., no MWI using Subscribe/Notify)

Telephony Infrastructure Agenda (1/2)

- Deployment Models
- Basic Call Processing
- Signaling Protocols
- Gateways
- Media Resources
- Call Processing

Gateways
Gateway Selection Criteria

Cisco.com

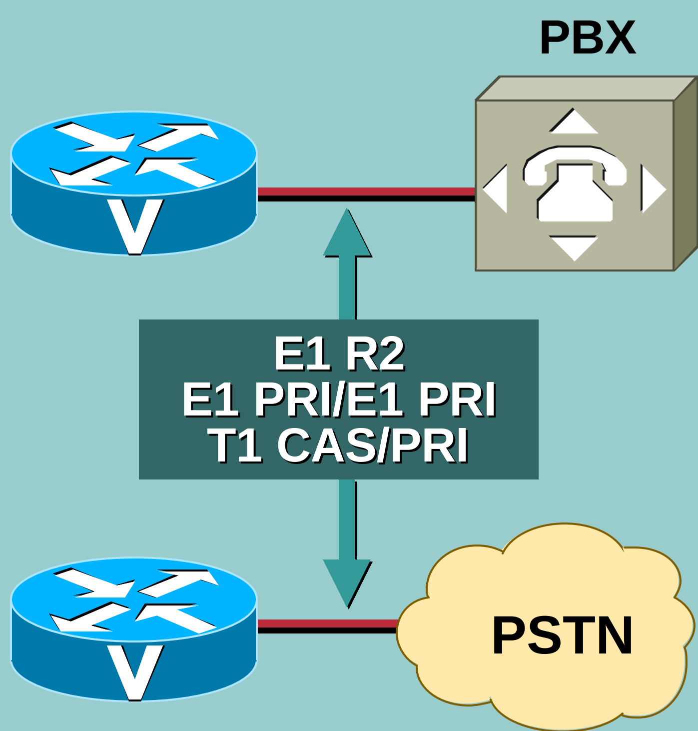


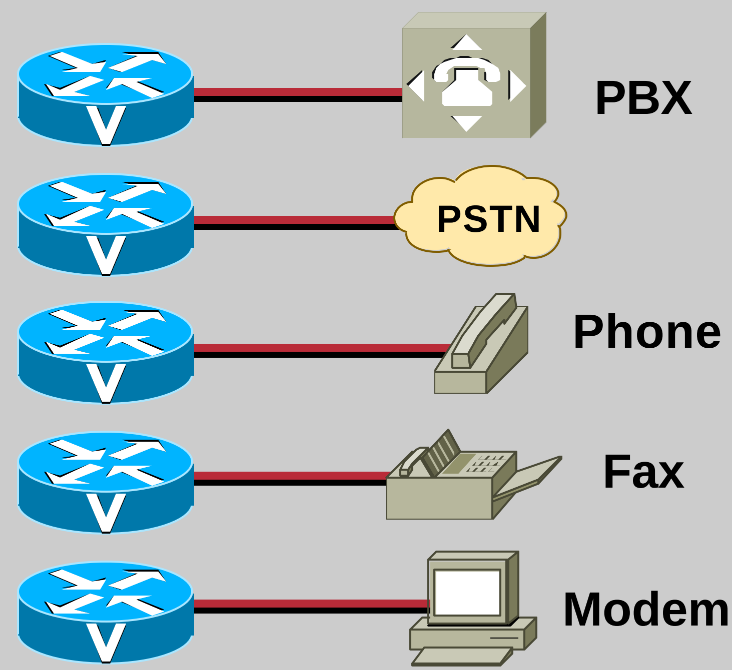
- Voice port density requirements
- Signaling protocol (H.323, MGCP, etc.)
- Support for required PSTN signaling types
- Support for required WAN interfaces and QoS

Gateways
Digital vs. Analog

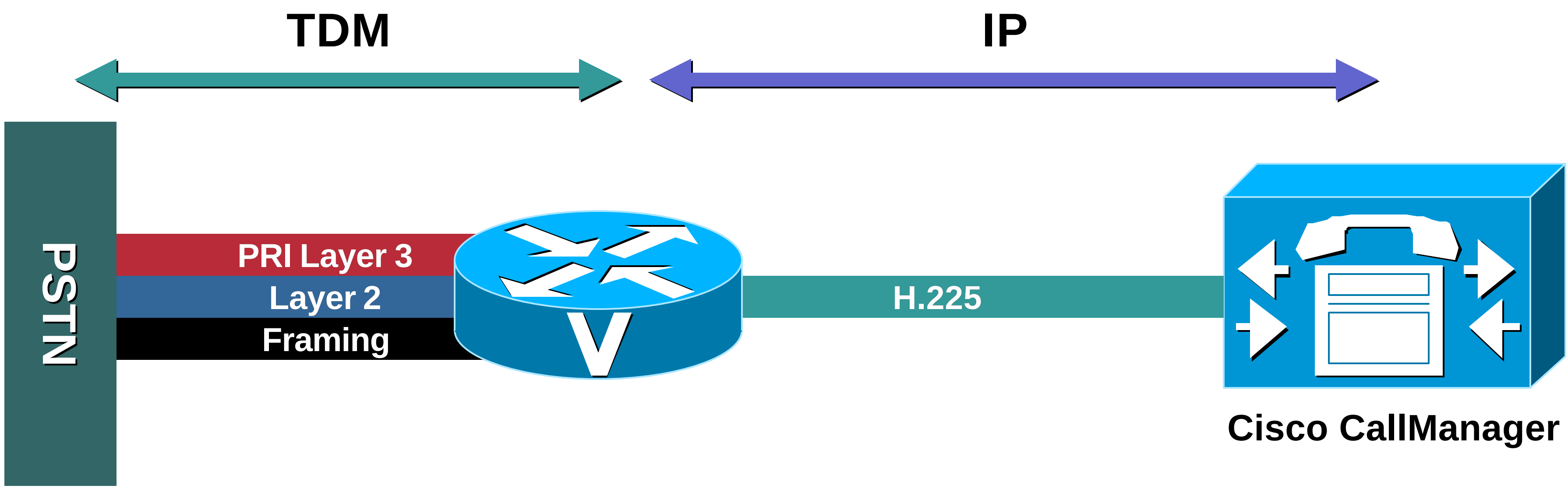
Cisco.com

Digital Gateways	Analog Gateways





Gateways
H.323



- All PSTN signaling terminates on gateway
- H.225 communication between gateway and CallManager
- H.323 is a “peer-to-peer” protocol

Gateways
H.323: Cisco IOS Configuration

Cisco.com

Interface Configuration

```
isdn switch-type primary-5ess
!
controller E1 1/0
 framing crc
 clock source line primary
 linecode hdb3
 pri-group timeslots 1-31
!
interface Loopback0
 ip address 10.1.1.1 255.255.255.0
 h323-gateway voip interface
 h323-gateway  voip bind srcaddr 10.1.1.1
!
interface Ethernet0/0.300
 encapsulation doE1q
 ip address 10.10.10.1 255.255.255.0
 service-policy output output-L3-2-L2
!
interface Serial1/0:15
 isdn switch-type primary-net5
 isdn incoming-voice modem
```

Dial Peer Configuration

```
dial-peer voice 1 voip
 destination-pattern 1…
! Set our preference for the dial-peer
 preference 1
! Set target to the CallManager Address
 session target ipv4:10.10.10.10
! Configure QoS for the dial-peer
 ip qos dscp af31 signaling ;or CS3
 ip qos dscp ef media
! Set DTMF relay
 dtmf-relay h245-alpha
!
dial-peer voice 408 pots
 destination-pattern 9T
 port 1/0:15
```

Gateways
H.323: Pros and Cons

Pros

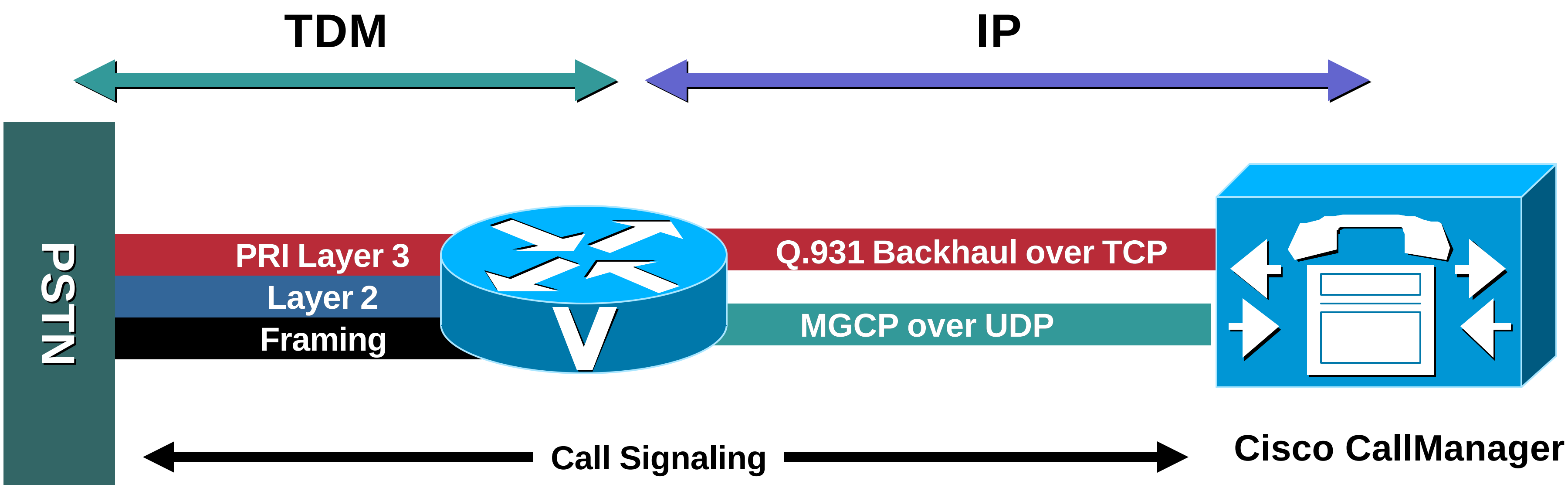
- Interoperability
- Breadth of product and interface choice
- Support for survivable remote site telephony
- Gateway intelligence

Cons

- Higher administration required
- No call preservation (yet) on CCM switchover

Gateways
MGCP: PRI Backhaul

Cisco.com



- Framing and layer 2 signaling terminates at the gateway
- Layer 3 signaling is backhauled to the CallManager
- MGCP is a “client-server” protocol
- MGCP 0.1 with CallManager only

Gateways
MGCP: Cisco IOS Gateway Configuration

Cisco.com

```
hostname GW1
mgcp
mgcp call-agent 10.10.10.10
mgcp dtmf-relay codec all mode out-of-band
mgcp ip qos dscp ef media
mgcp ip qos dscp af31 signaling; or cs3
ccm-manager redundant-host 10.10.10.11
ccm-manager mgcp
controller E1 1/0
 linecode b8zs
 framing esf
 pri-group timeslots 1-24 service mgcp
!
interface Serial1/0:23
 no ip address
 no logging event link-status
 isdn incoming-voice voice
 isdn bind-l3 ccm-manager
!
dial-peer voice 101 pots
 application mgcpapp
 port 1/0:23
```

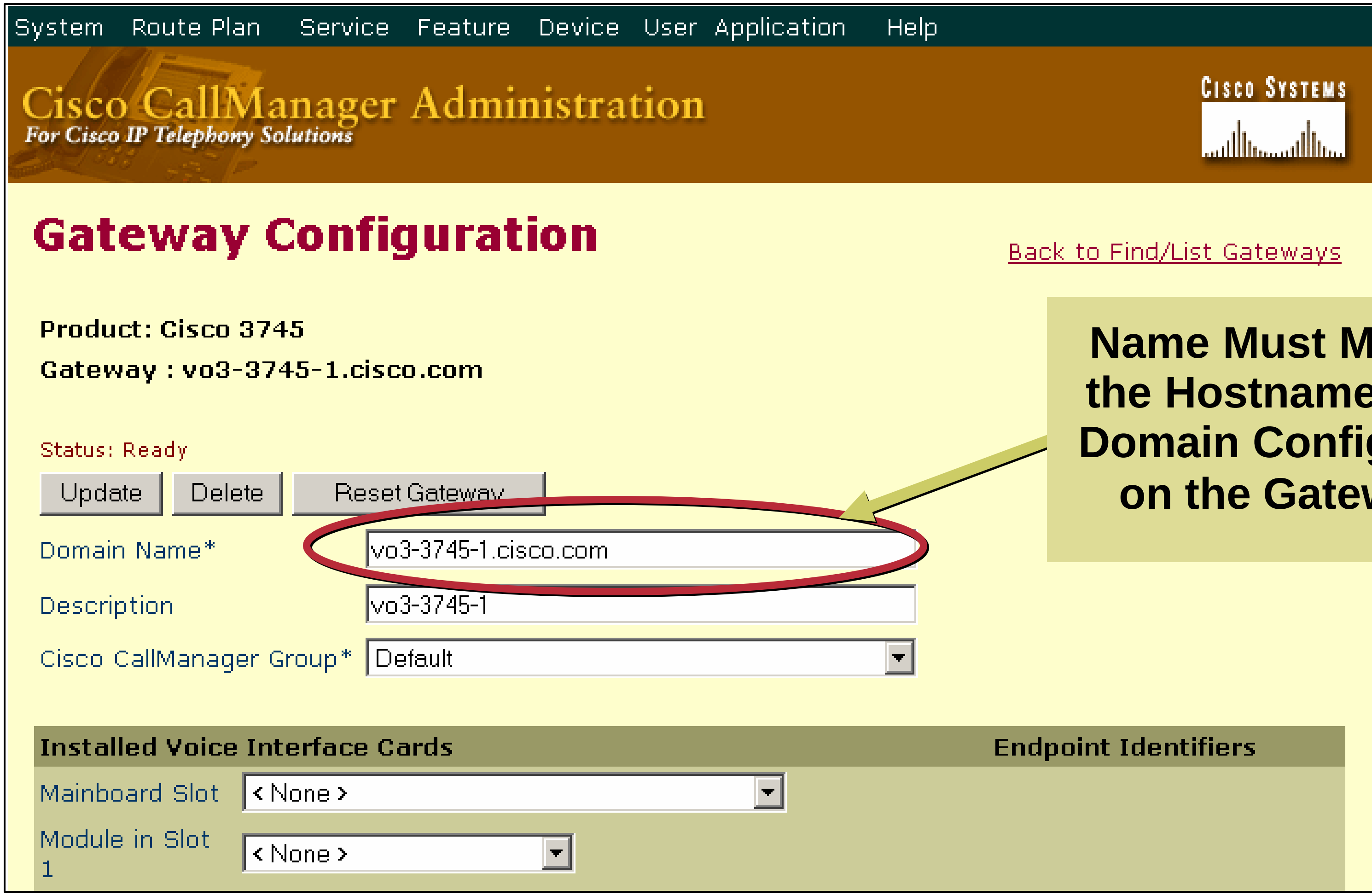
NOTE:

DSCP Support added in Cisco IOS 12.2(11)T

IP Prec Support Added in Cisco IOS 12.1(5)XM and 12.2(2)T

```
mgcp ip-tos rtp 5
mgcp ip-tos signaling 3
```

Gateways
MGCP: CallManager Configuration



Name Must Match the Hostname and Domain Configured on the Gateway

Gateways
MGCP: Pros and Cons

Pros

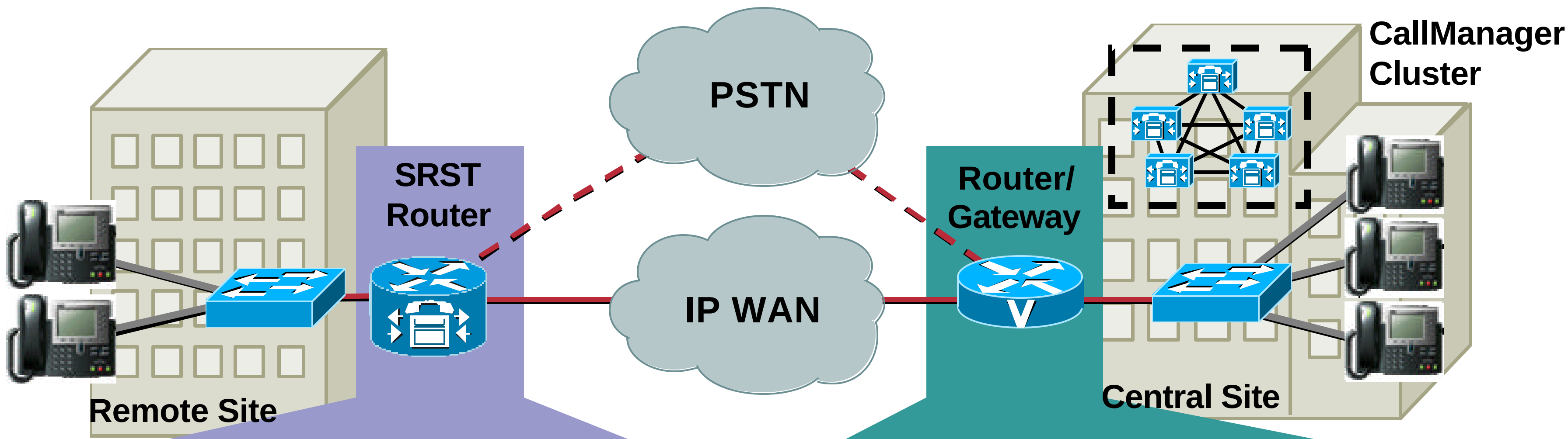
- Ease of dial plan administration
- Call (audio) preservation
- Port-level control (required for voice mail integration)

Cons

- Dependency on connectivity to call agent

Gateways
Protocol and Platform Recommendations

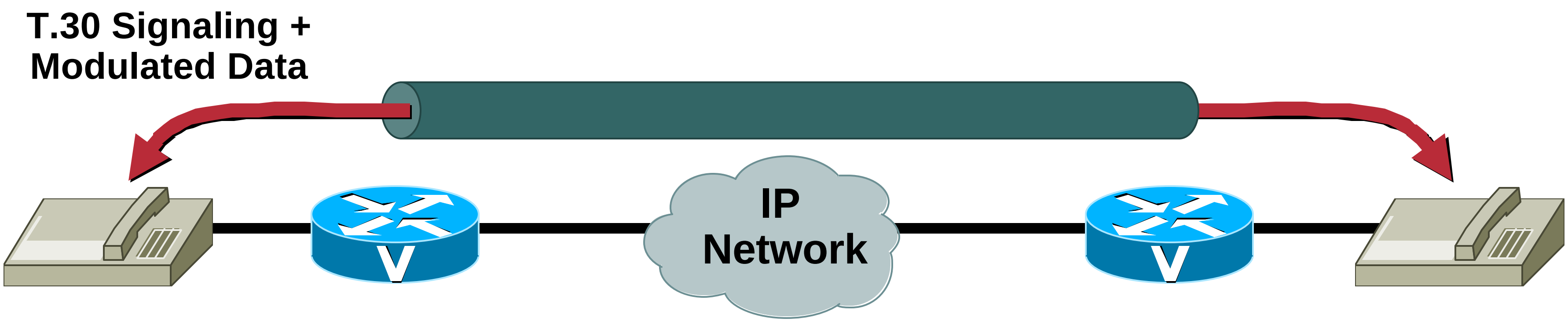
Cisco.com



- H.323, MGCP fallback to H.323
- Standalone, router-integrated
- Platforms:
  - 1751, 1760
  - 28xx, 26xx
  - 38xx, 37xx, 36xx

- MGCP, H.323
- Standalone, router-integrated
- Platforms:
  - WS-X6608
  - CMM
  - 38xx, 36xx, 37xx
  - AS5x00

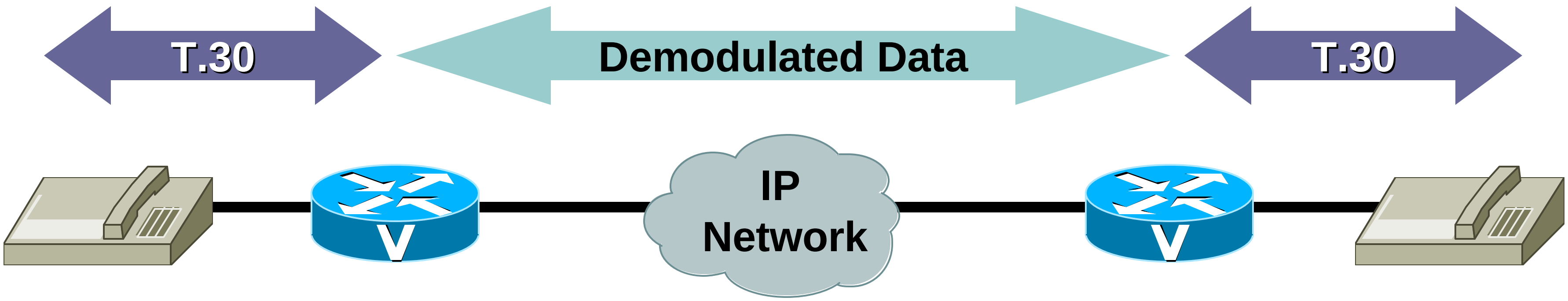
Gateways
Fax Pass-Through



- **No demodulation of fax traffic (Like a VoIP call)**
- **Recommendation: Hard-code codec to G.711 for call admission control**
- **When a fax call is detected:**
  - **Echo cancellation is disabled**
  - **Jitter is disabled**
  - **VAD is disabled**
- **Group 3 (9,600 kbps)—Best case 14,400 kbps**

Gateways
Cisco Fax Relay

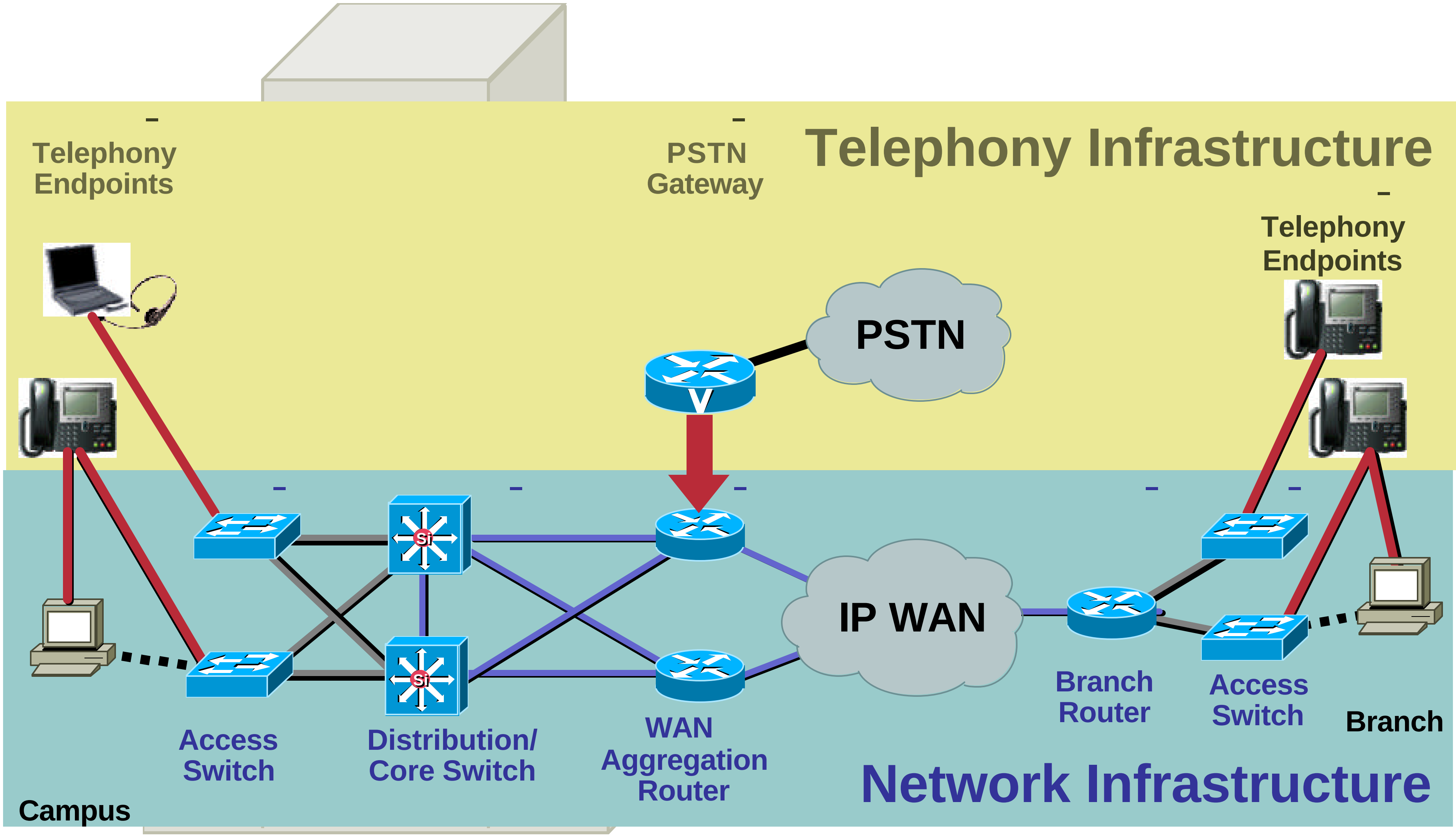
Cisco.com



- Cisco fax relay is negotiated over the media stream "in-band"—CallManager handles it like a voice call
- T.30 is demodulated at the inbound gateway
- Demodulated data is sent to the outbound gateway for modulation
- Maximum speed: 14,400 kbps with G.711

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_access/fxmdmnt.htm#xtocid5

What We Have Built so Far



Telephony Infrastructure Agenda (1/2)

Cisco.com

- Deployment Models
- Basic Call Processing
- Signaling Protocols
- Gateways
- Media Resources
- Call Processing

Media Resources
Conferencing, Transcoding, Music on Hold

- **Conferencing**

  DSPs needed for multi-party conferences

- **Transcoding**

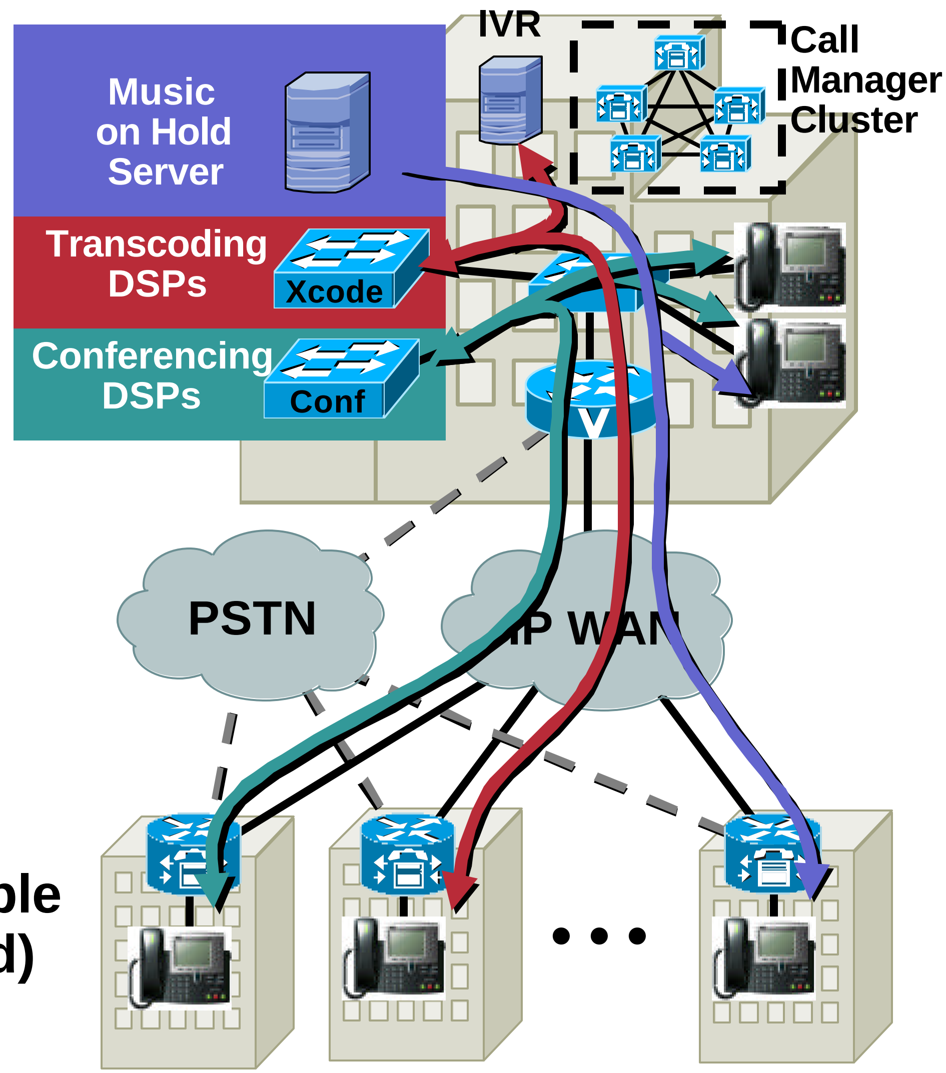
  Multiple CODEC support (e.g., G.711 to G.729)

  Automatic CODEC selection

  DSPs needed in presence of single-CODEC endpoints

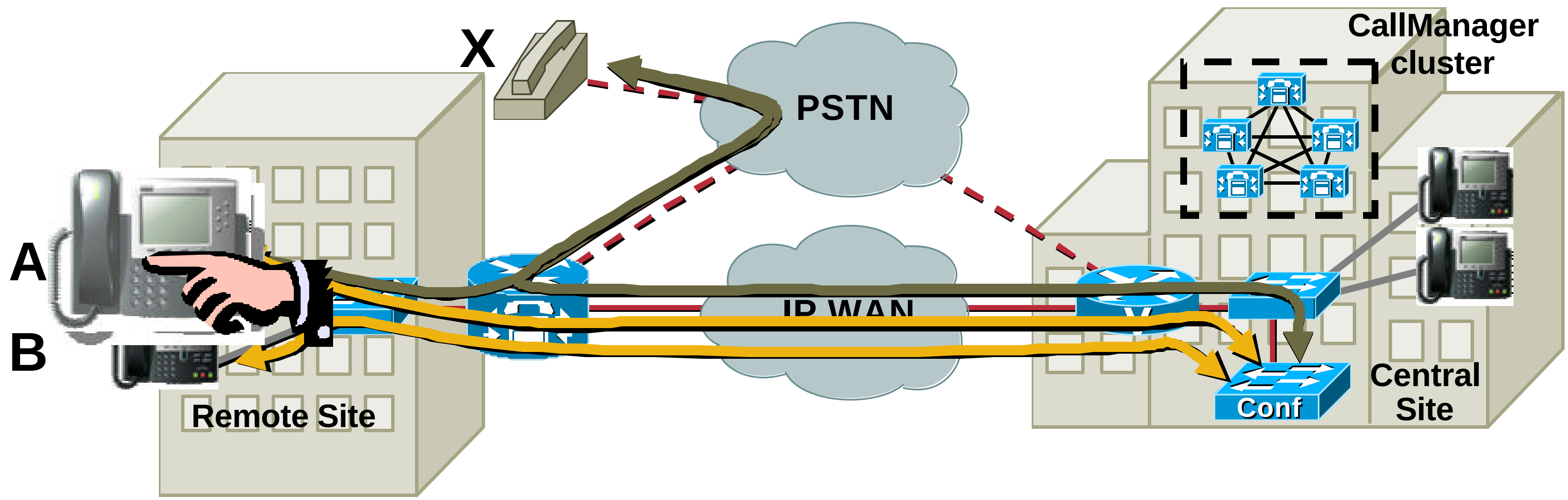
- **Music on hold**

  Multiple source types possible (centralized or branch-based)



Media Resources
Centralized Conferencing Resources

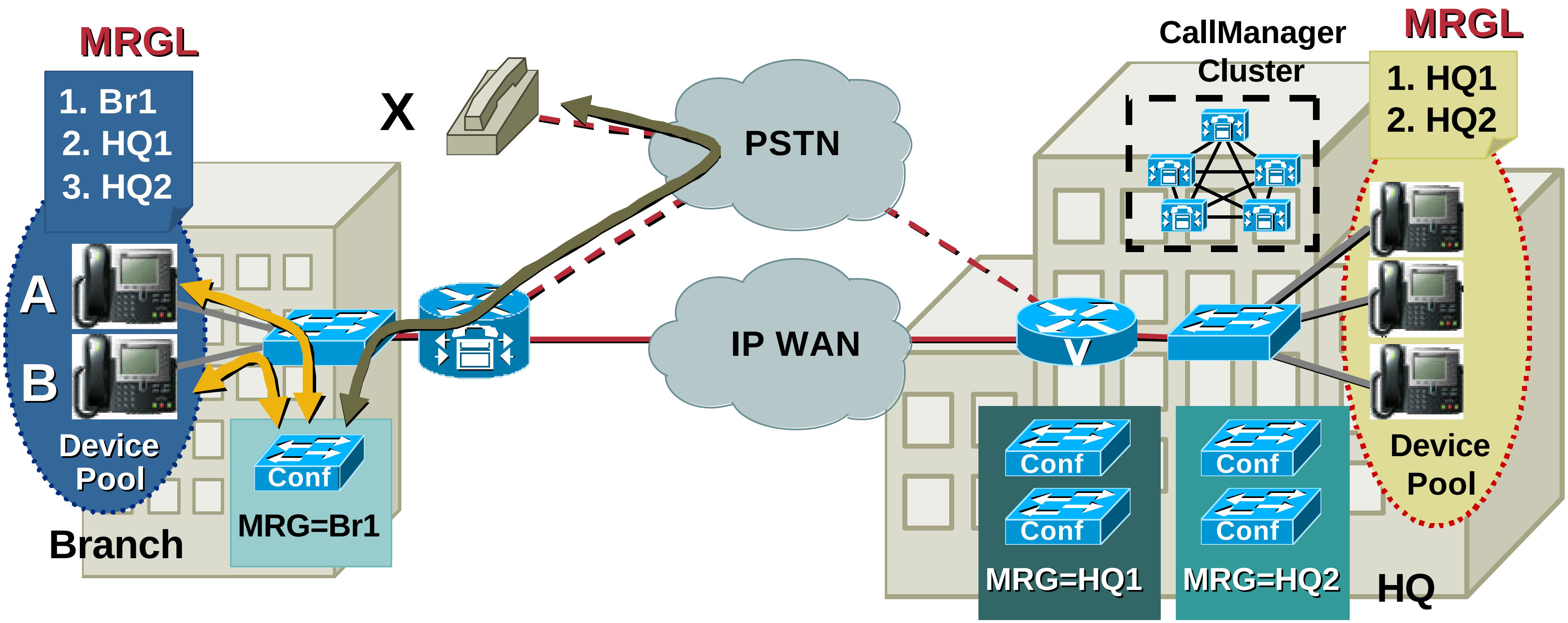
Cisco.com



- External caller X calls A—No voice across WAN
- A conferences B in
- 3 voice streams across WAN
- No conferencing during WAN failures

Media Resources
Distributed Conferencing Resources

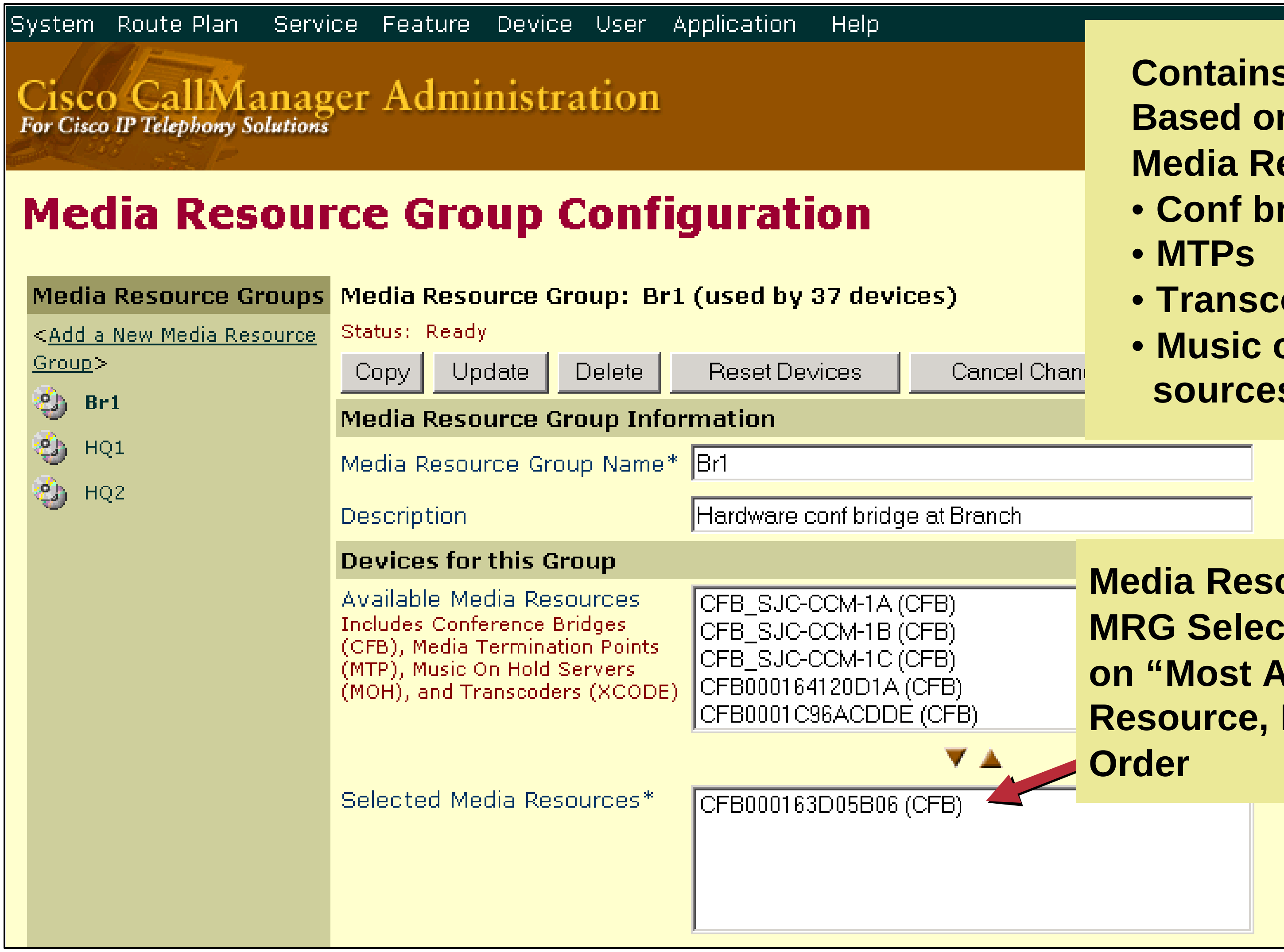
Cisco.com



- Conference between A, B and X—No voice across WAN
- Requires extra hardware at branch
- No conferencing during WAN failures

MRG = Media Resource Group
MRGL = Media Resource Group List

Media Resources
Configuration Example: MRG



Contains Actual SW-Based or HW-Based Media Resources:
- **Conf bridges**
- **MTPs**
- **Transcoders**
- **Music on hold sources**

Media Resource within MRG Selected Based on “Most Available” Resource, Not in List’s Order

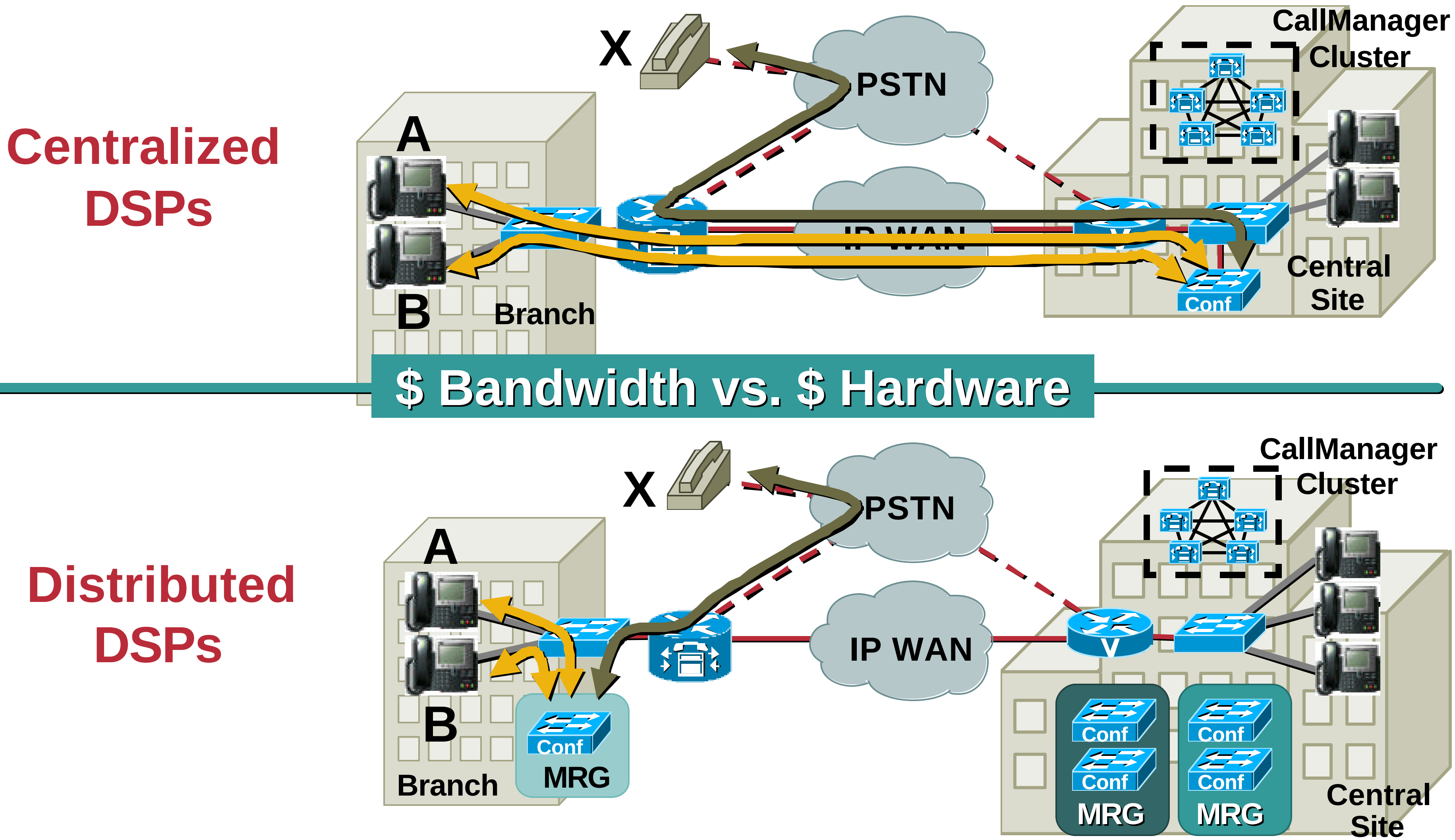
Media Resources
Configuration Example: MRGL

Cisco.com

Prioritized List of MRGs: Branch Devices Will Use Local Conf Bridge First

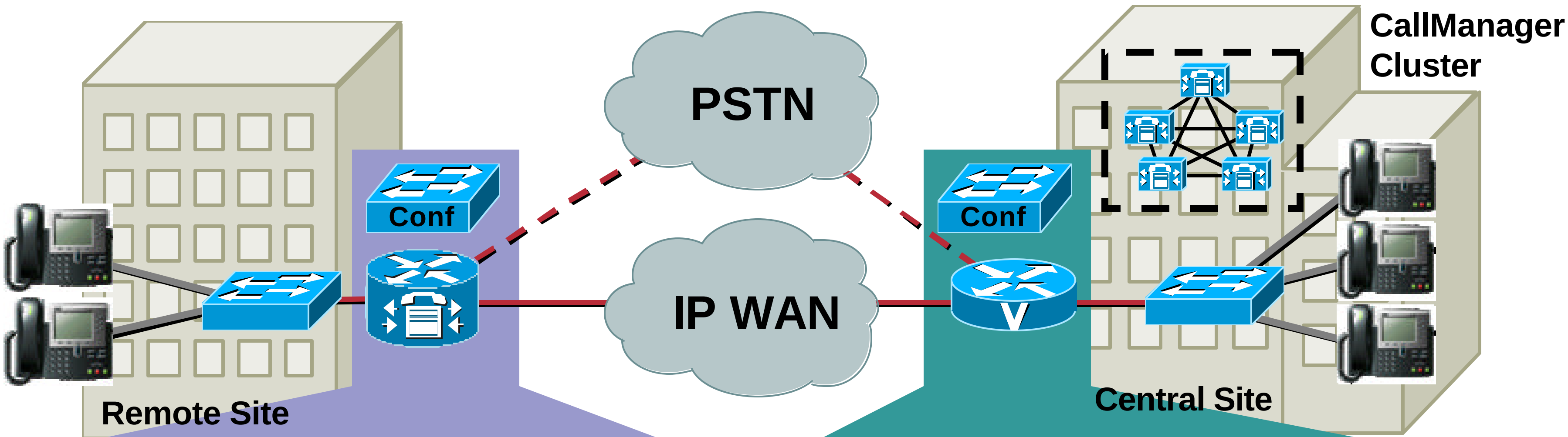
Media Resources
Centralized vs. Distributed DSPs

Cisco.com



Media Resources
DSP Platform Recommendations

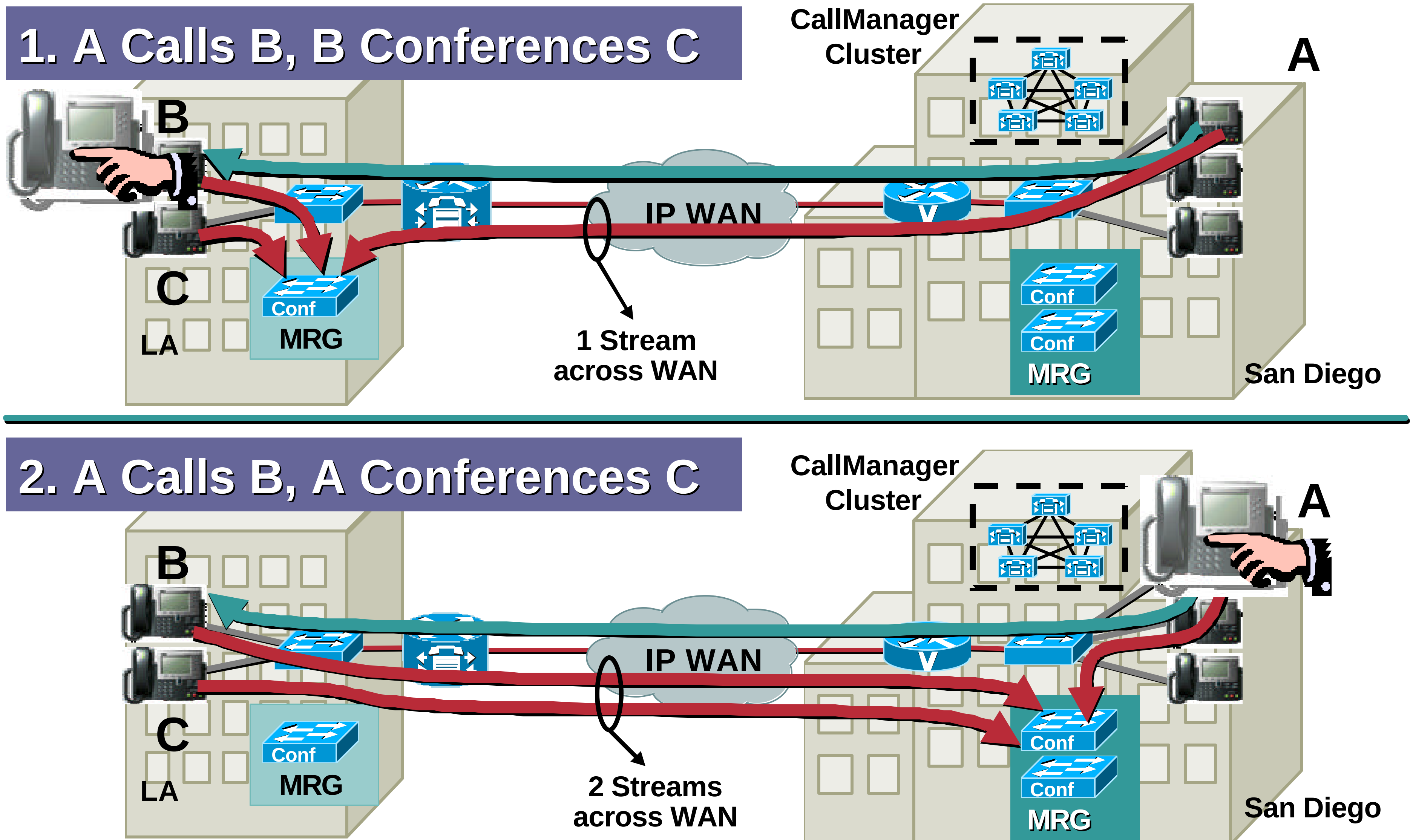
Cisco.com



- Cisco IOS HDV

- WS 6608 (6 parties)
- CMM (64 parties)
- NM-HDV2 (8 parties)
- Software CFB

Media Resources
“Conference Initiator” Concept



MoH Configuration
Audio Source and Server Selection

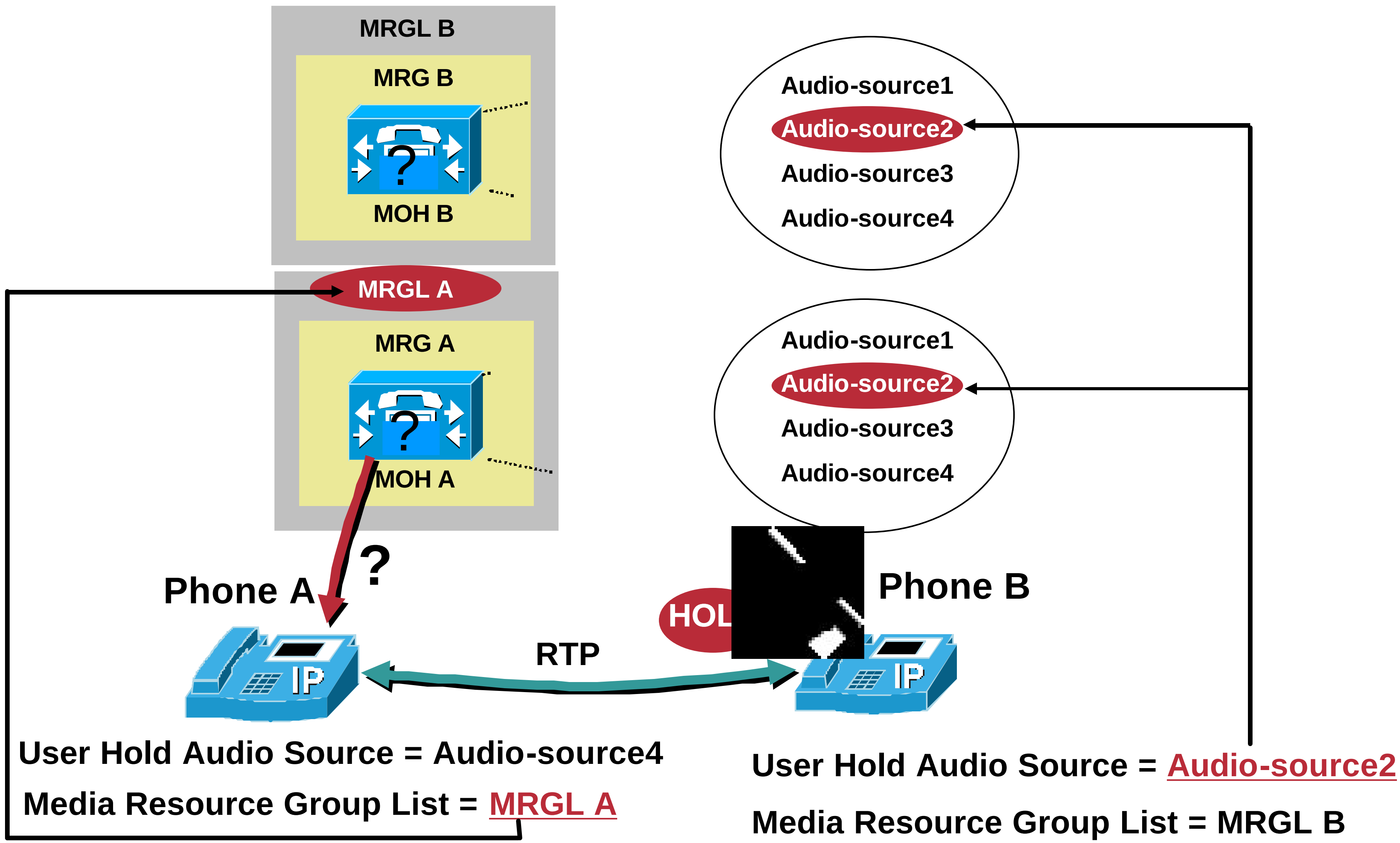
The MoH Stream that an Endpoint Receives Is Determined by a Combination of the Following:

The Configured User/Network Hold Audio Source of the Endpoint/Network Resource Initiating the Hold Event

AND

The Configured Media Resource Group List of the Endpoint Being Placed on Hold

MoH Configuration
Audio Source and Server Selection: Example



MoH Configuration
Multicast Addressing

- Configure multicast MoH sources to use multicast group addresses in the range:

  239.1.1.1 to 239.255.255.255

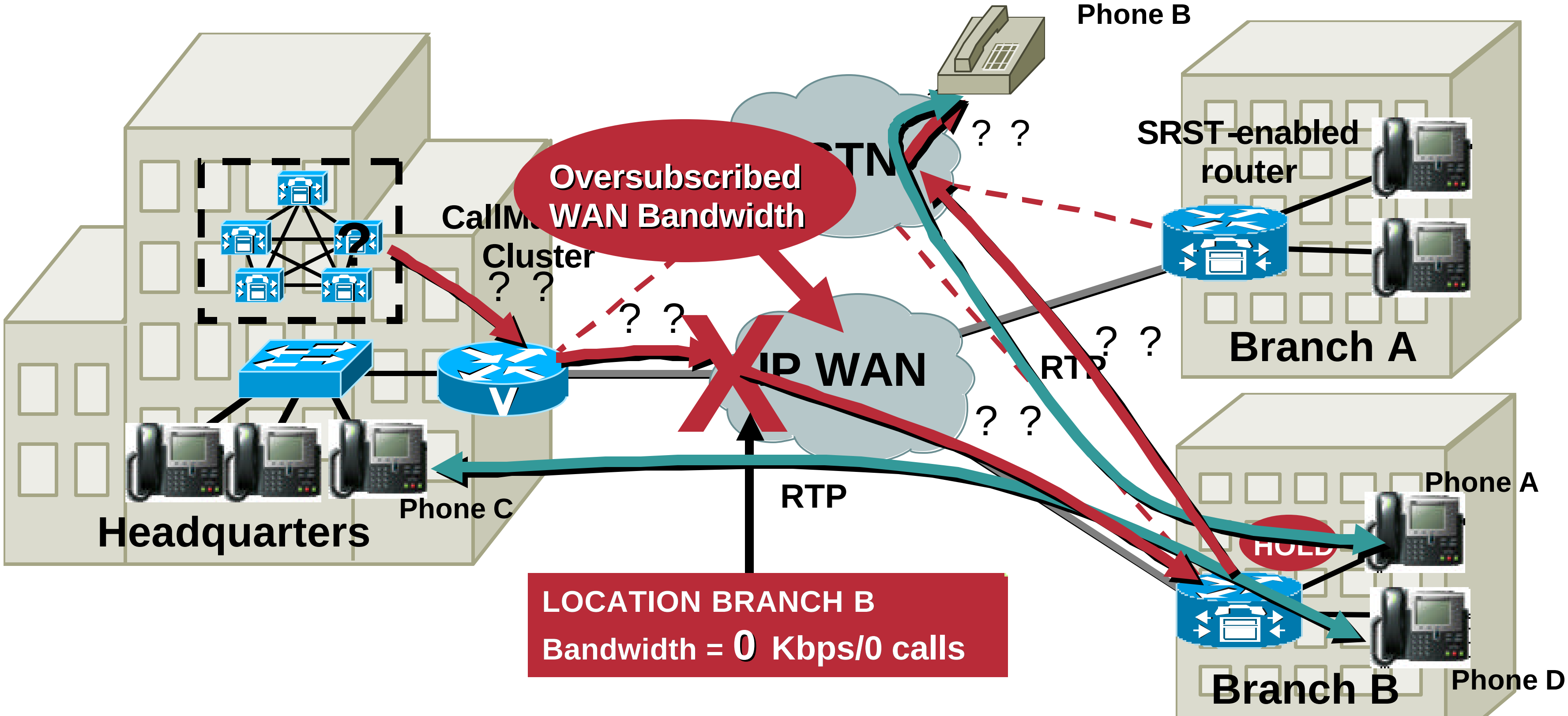
- Configure multicast MoH sources to increment on IP address NOT port number

Increment on IP address for two reasons:

1. Cisco IP Phones have no concept of multicast port numbers
2. IP routers route multicast traffic based on multicast address not port numbers

Deployment Models and MoH
Centralized Multisite: MoH from Central Server

Cisco.com



Only unicast MoH streams are tracked by locations-based CAC

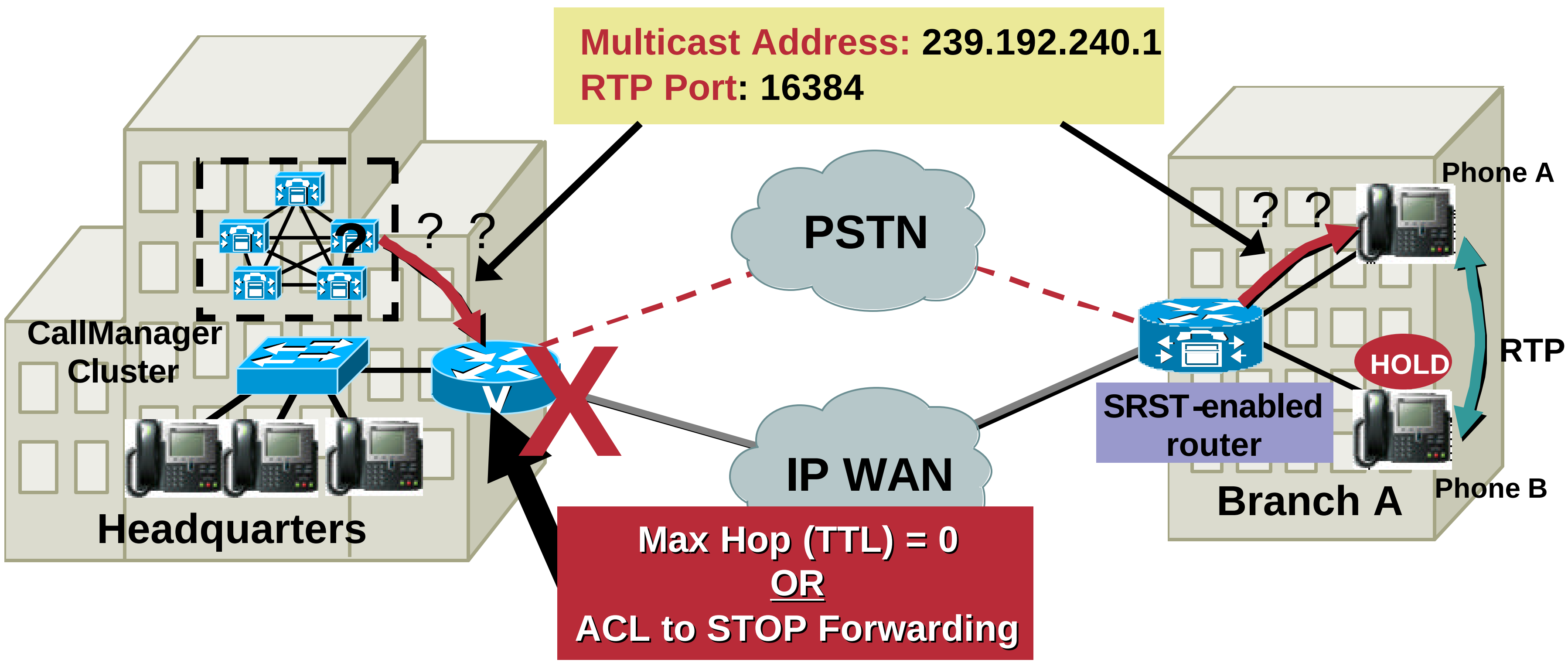
If MoH stream is UNICAST then the stream will be rejected

If MoH stream is MULTICAST then the stream will be allowed

Deployment Models and MoH

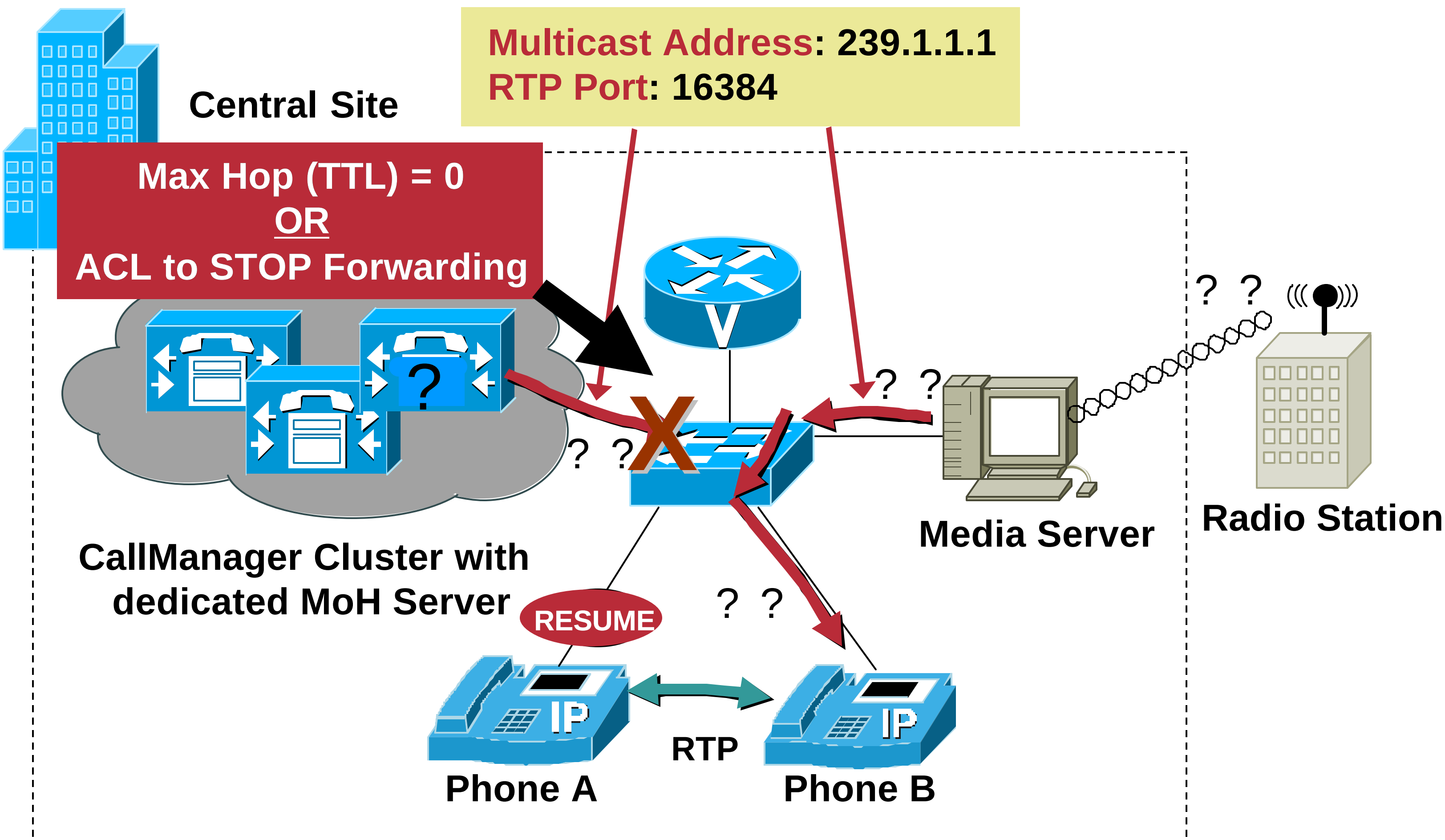
Centralized Multisite: MoH from Branch Router Flash

Cisco.com



- Beginning with 12.2(15)ZJ and SRST Release 3.0
- Stream multicast MoH from Branch router flash
- Works whether branch is operating in SRST mode or not (IP Phones get Tone on Hold in SRST, but GW gets music)

MoH Configuration
Multiple Fixed/Live Audio Sources: Example



Configuration for Multicast MoH from Branch Router Flash:

SRST-router (config)# **call-manager-fallback**

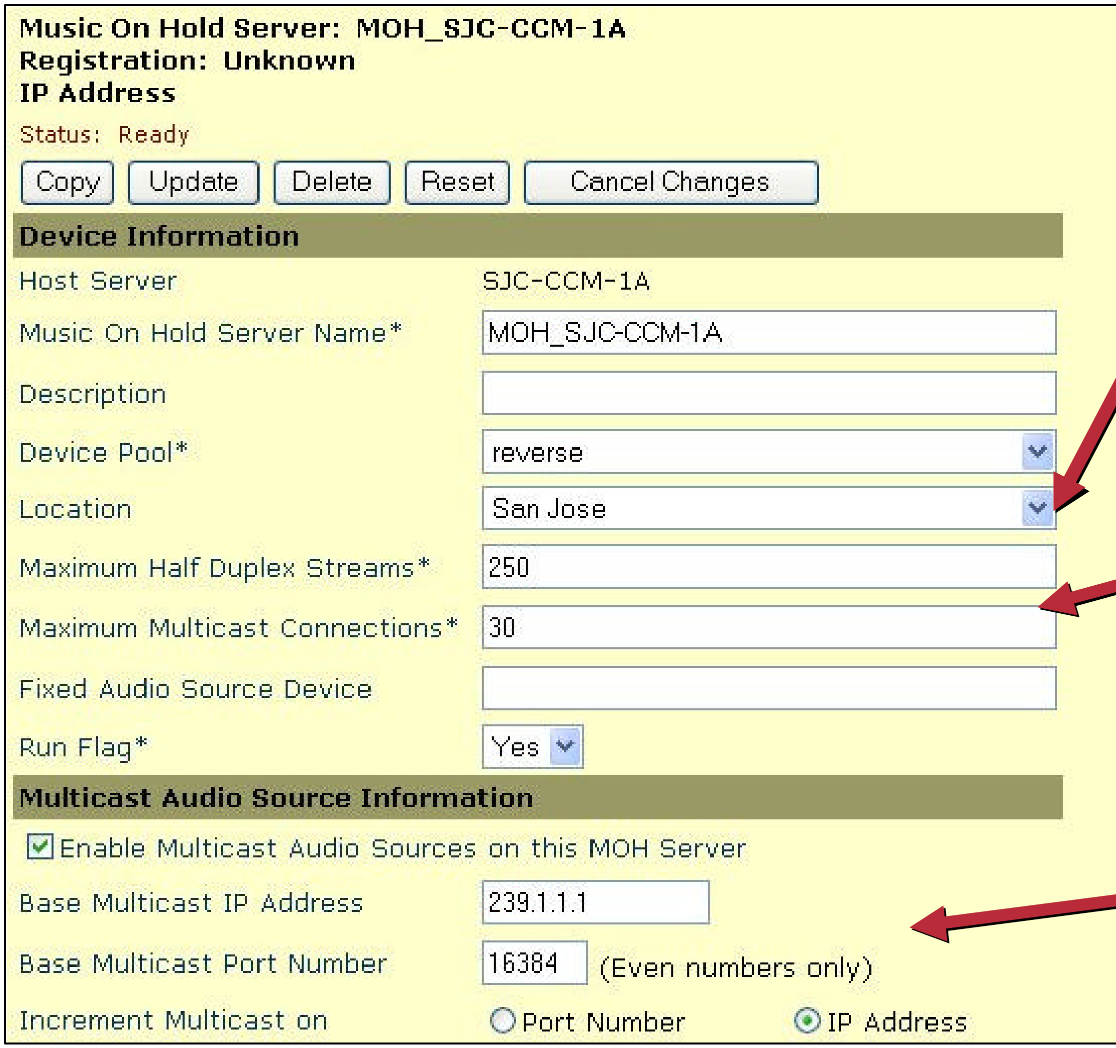
SRST-router (config-cm-fallback)# **moh flash-audio-file.au**

SRST-router (config-cm-fallback)# **multicast moh 239.192.240.1 port 16384 route 10.1.1.254**

- **Stream multicast MoH from flash whether in SRST mode or not**
- **Configuration is the same in either case**

Media Resources
Music on Hold: Server Configuration

Cisco.com



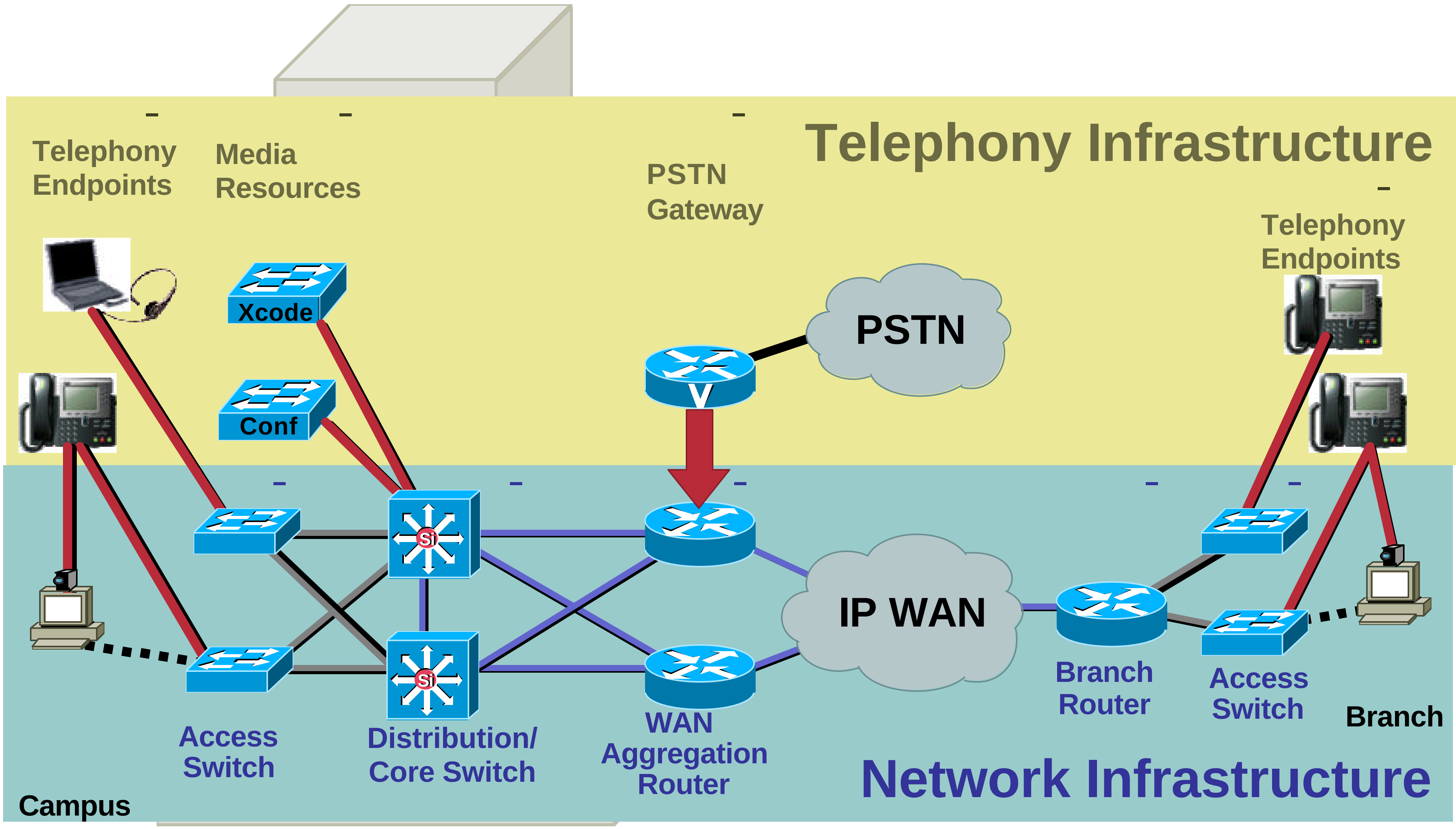
Location of MoH Server; Required for CAC

Maximum Number of Streams (affects capacity)

Enables Multicast Support

What We Have Built So Far

Cisco.com



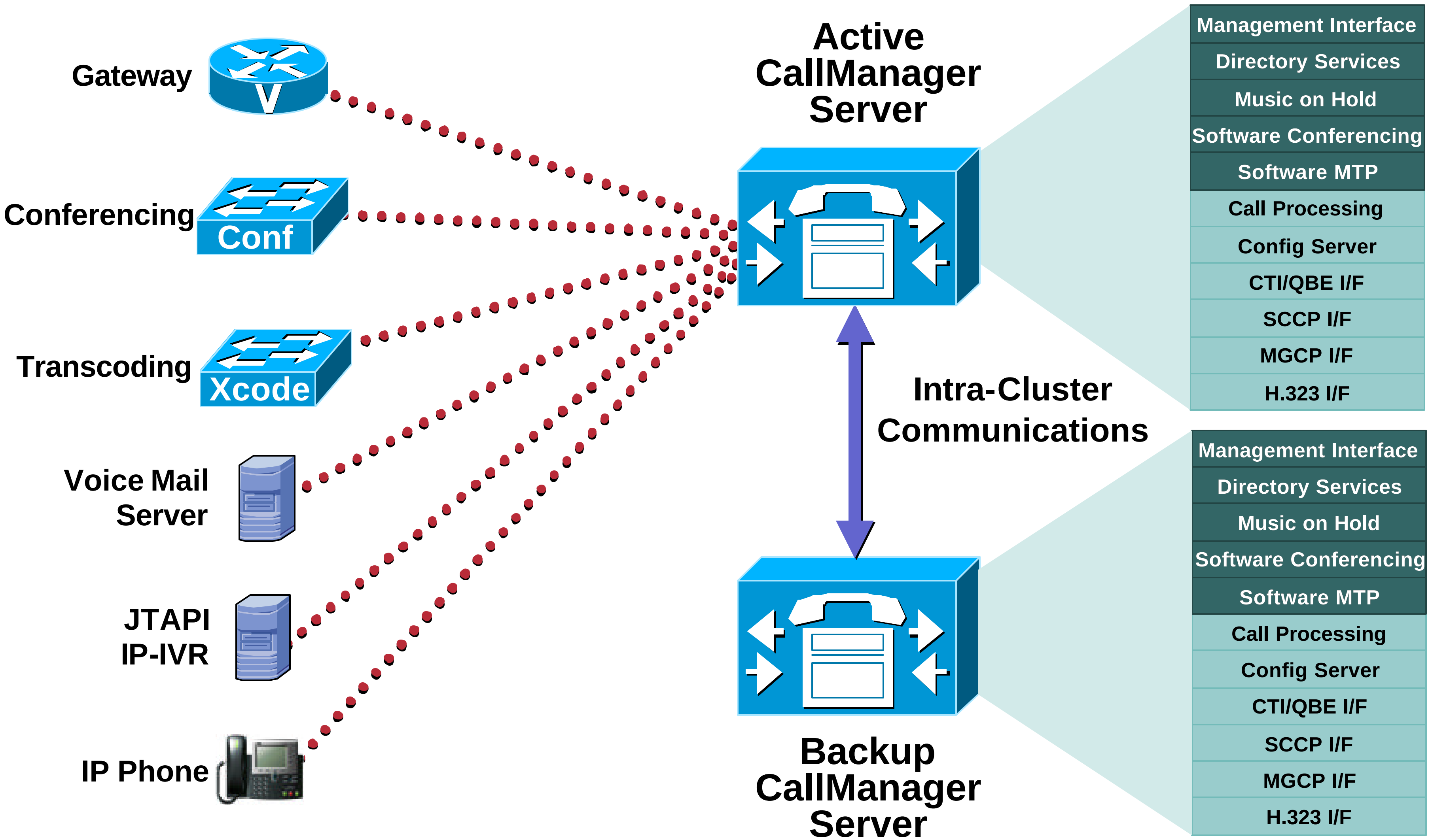
Telephony Infrastructure Agenda (1/2)

- Deployment Models
- Basic Call Processing
- Signaling Protocols
- Gateways
- Media Resources
- Call Processing

Call Processing Agenda

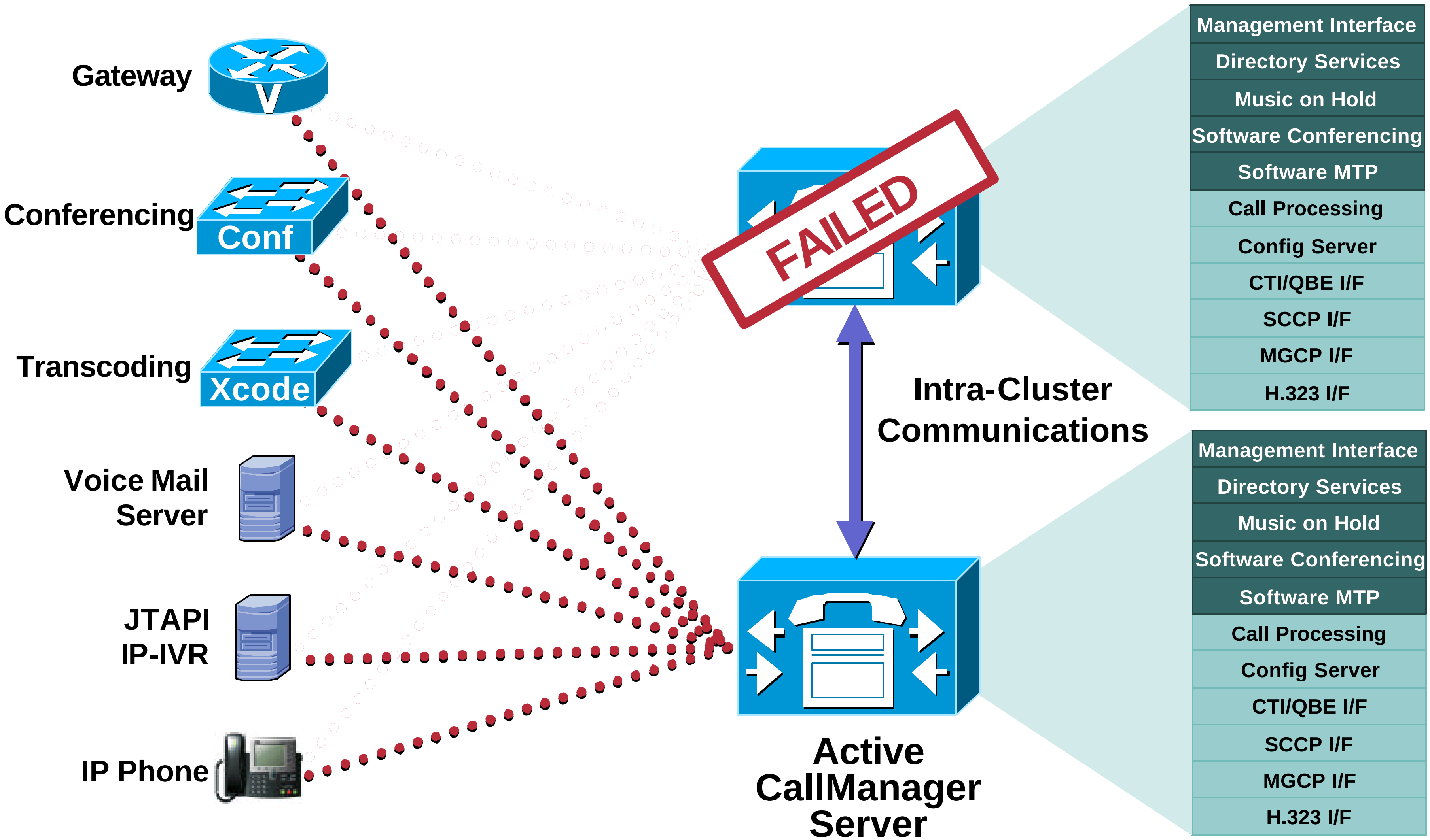
- CallManager Redundancy and Scalability
- CallManager Provisioning
- (J)TAPI and CTI Concepts
- CTI Provisioning
- Inter-Cluster Trunks and H.323

CallManager Redundancy and Scalability
Server Redundancy



CallManager Redundancy and Scalability
Server Redundancy

Cisco.com

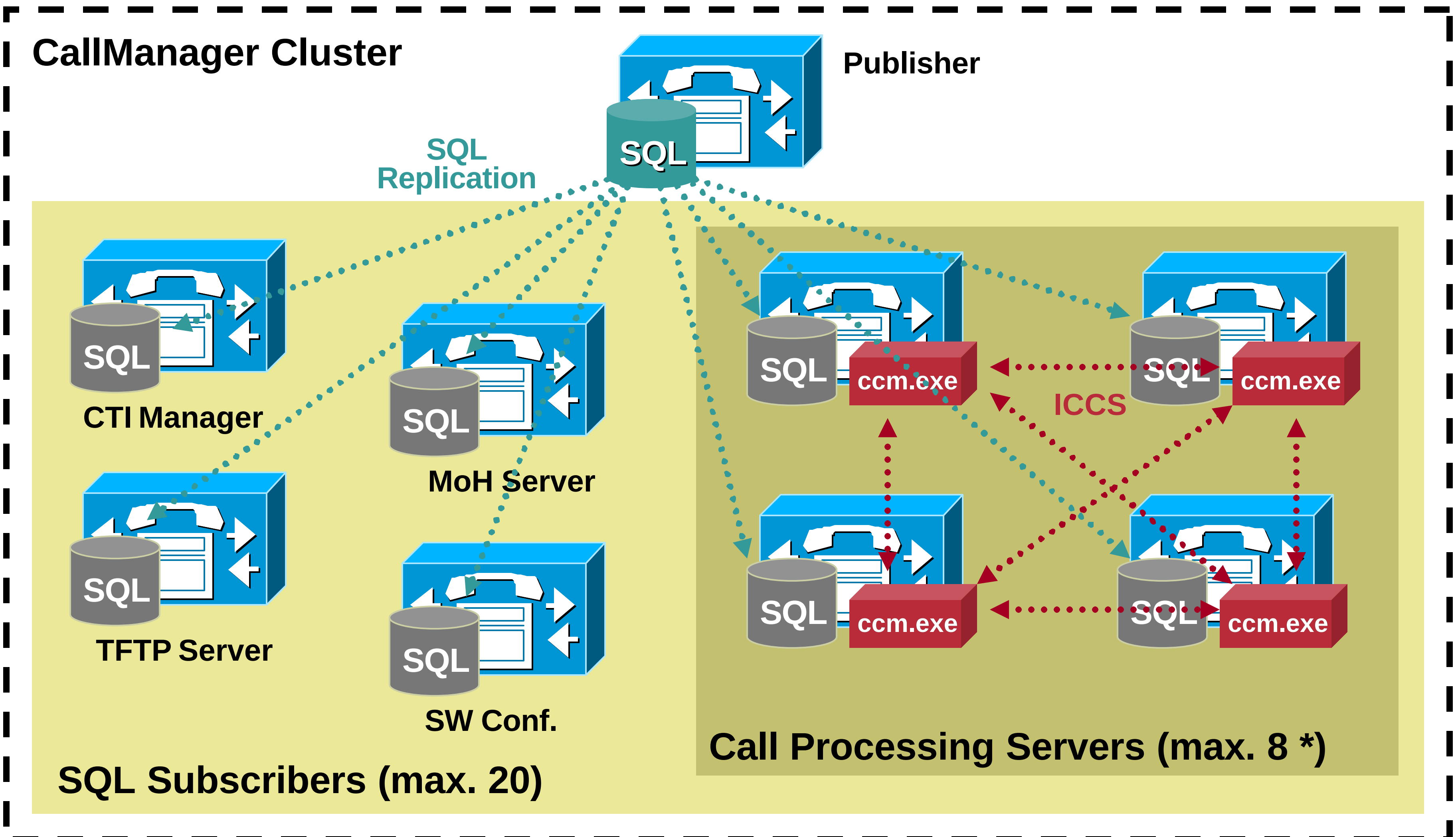


Call Agent Scalability
Clustering Properties and Rules

- The cluster appears as one entity, with a single point of administration (the publisher)
- Several functions can be co-located on the same server, depending on cluster size
- Maximum of 20 SQL subscribers per cluster
- Maximum of 8 call processing servers per cluster (6 prior to CallManager 3.3(2))
- Maximum of 7,500 IP Phones per CallManager server (depending on server platform)
- Maximum of 30,000 IP Phones per CallManager cluster (depending on server platforms and configuration)

Call Agent Scalability
What Is a CallManager Cluster?

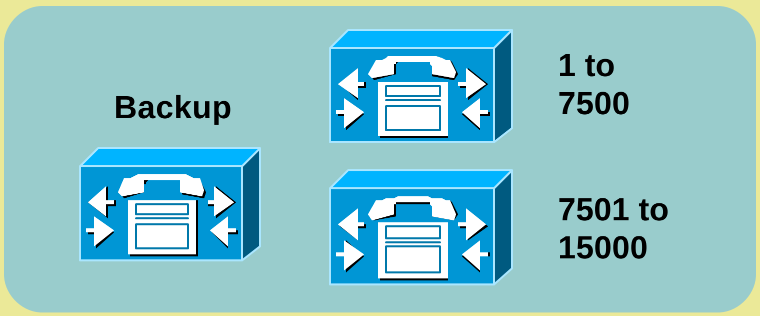
Cisco.com



*** Max. 6 prior to CallManager 3.3(2).**

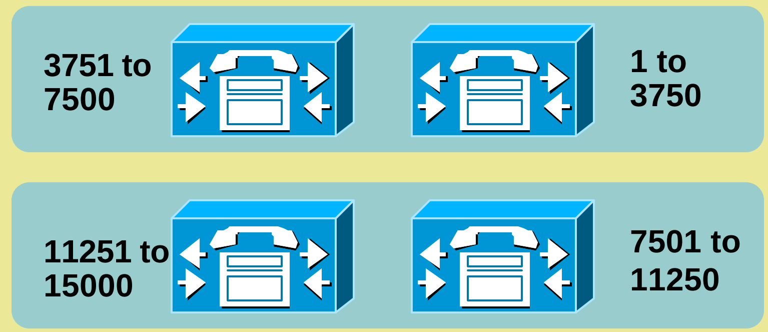
Call Agent Scalability
1:1 vs. 2:1 Redundancy Scheme

2:1 Redundancy Scheme



- Cost-efficient redundancy
- Degraded service during upgrades

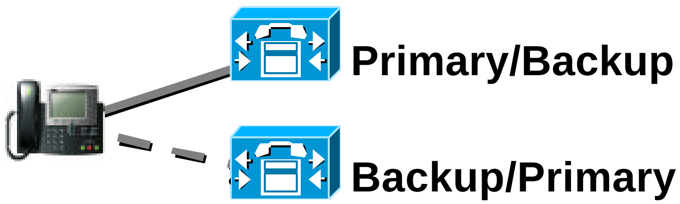
1:1 Redundancy Scheme



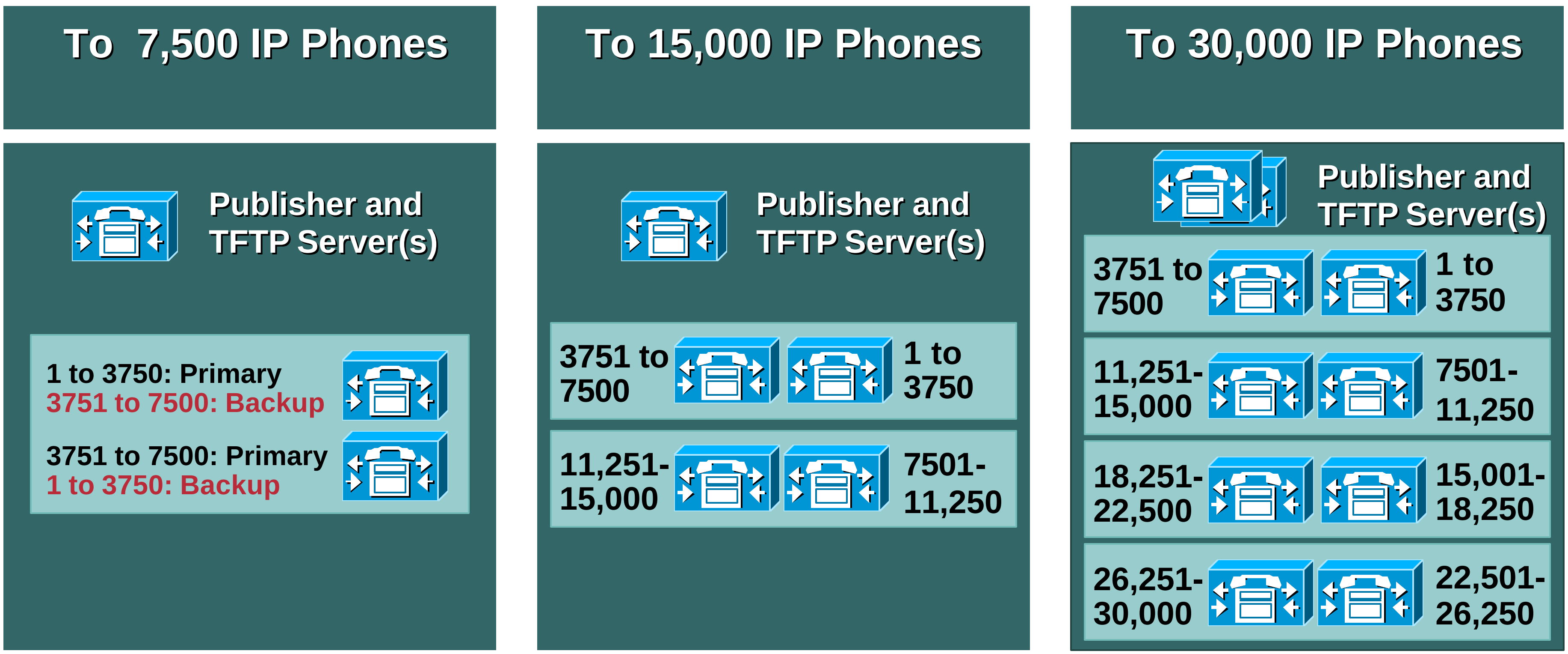
- High availability during upgrades
- Simplified configuration
- Load sharing
- Faster failover

CallManager Redundancy and Scalability
Clustering: 1:1 Redundancy (CM 3.3↑ and MCS 7845)

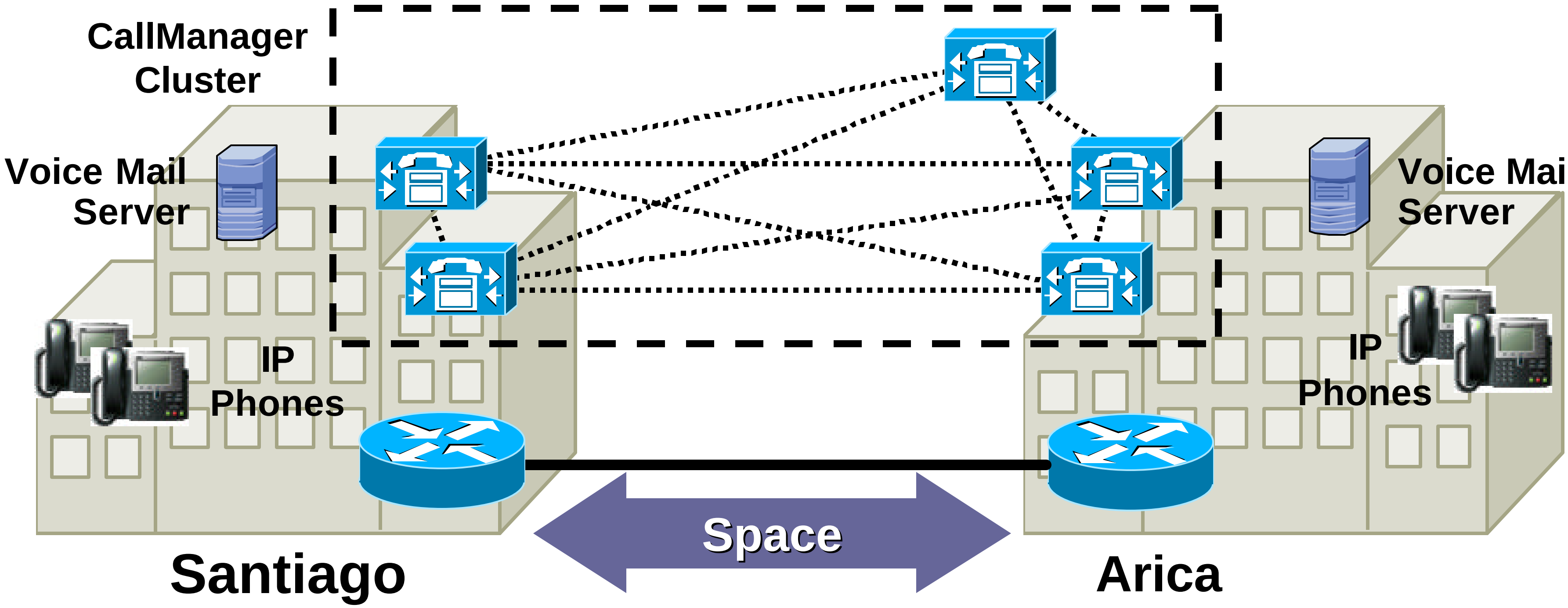
Cisco.com



- Distribute IP phones based on DN
- Load-share between primary and backup servers



CallManager Redundancy and Scalability
Geographic Redundancy

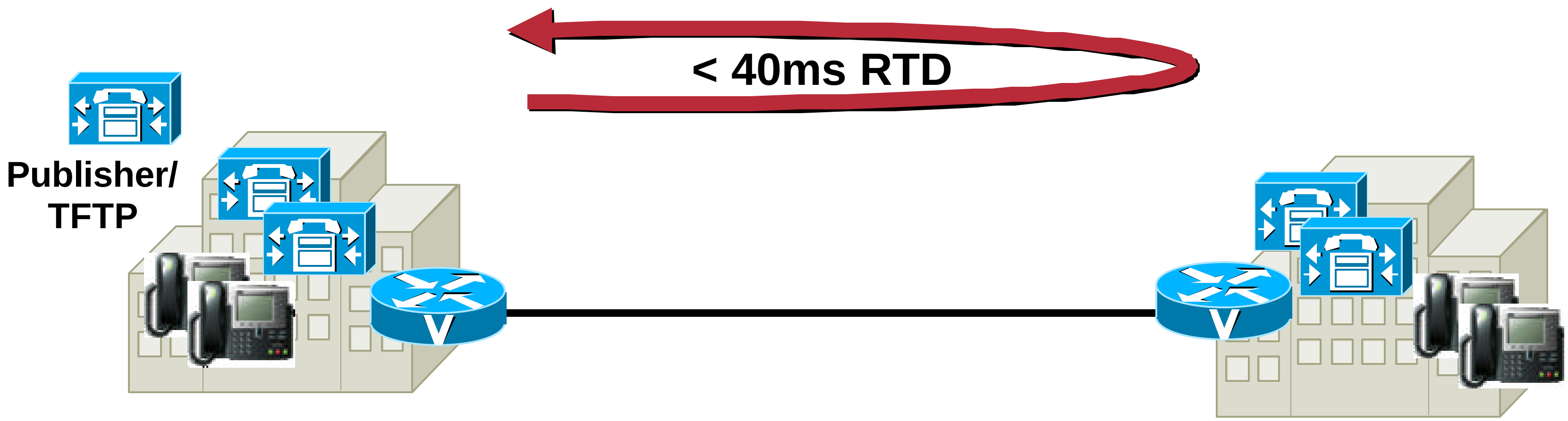


Spatial Redundancy = Resilience

Single Point of Administration, Extension Mobility, Feature Transparency and Unified Dial Plan

CallManager Redundancy and Scalability
Clustering over the WAN: Guidelines

Cisco.com



- Max 40ms round-trip delay between ANY two CallManagers
- 900 kbps for each 10,000 BHCA between sites
- Eight active locations maximum
- Failover across the WAN supported (Additional BW)
- While Publisher is not accessible
  - No Extension Mobility
  - No user access to CallForwardAll
  - No admin changes
- While cluster is split
  - Each part thinks the phones in the other parts are un-registered

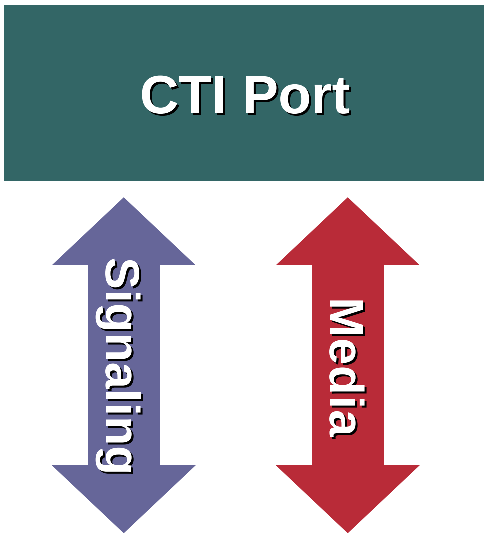
Check Out the IP Telephony Design Guide for CallManager 4.0 for Full Details

Call Processing Agenda

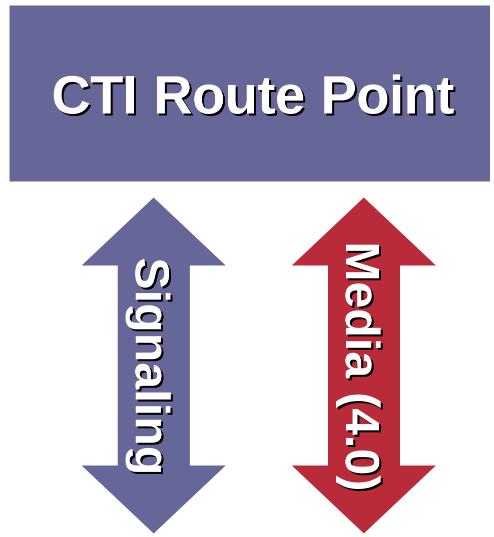
- Redundancy and Scalability
- (J)TAPI and CTI Concepts
- CTI Provisioning
- Inter-cluster Trunks and H.323

(J)TAPI and CTI Concepts
Route Point, Port and Third-Party Control

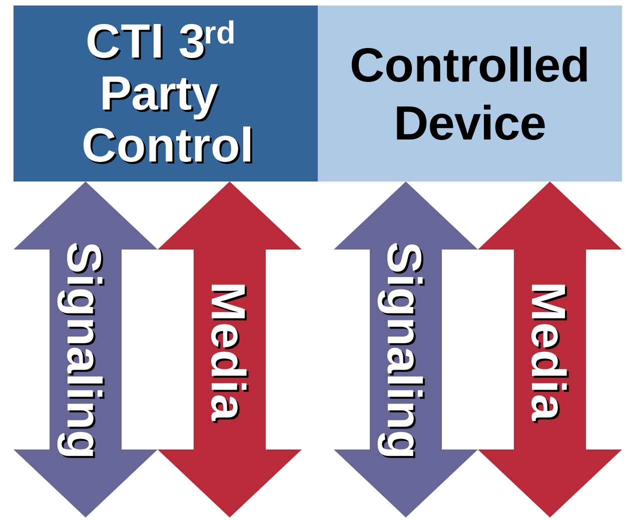
Cisco.com



- Makes and receives calls
- Media capable

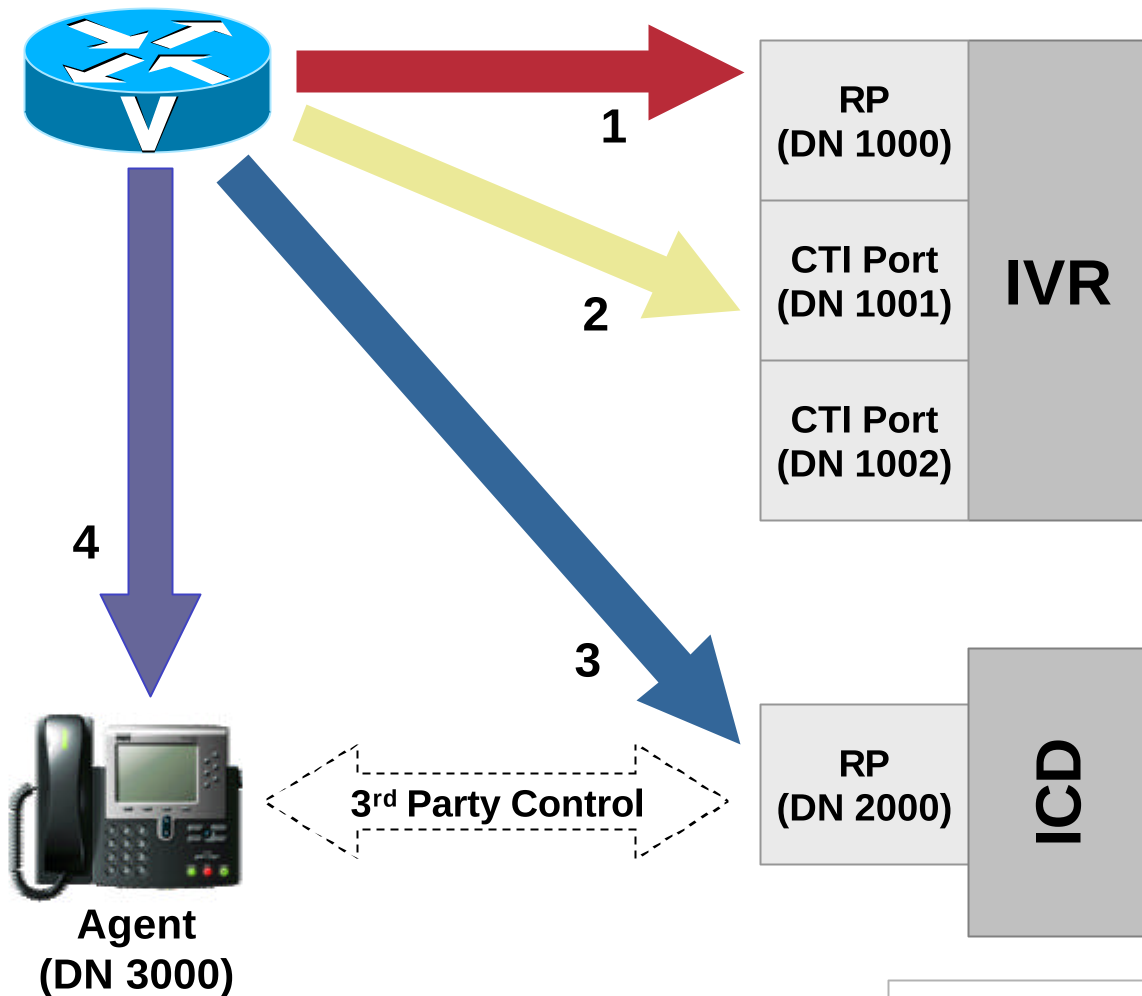


- Routes calls
- Acts as queue point
- No media until 4.0



- “Dual” control
- Status monitoring
- Automatically created when device is associated with user

(J)TAPI and CTI Concepts
Joining All the Elements



1. Incoming Call from GW to IVR's Route Point (Pilot Number 1000) IVR Application Redirect to a Free IVR CTI Port (1001)

2. IVR Answers Call on CTI Port; Plays Messages and Collects Information, Blind Transfers Caller to ICD Route Point (2000)

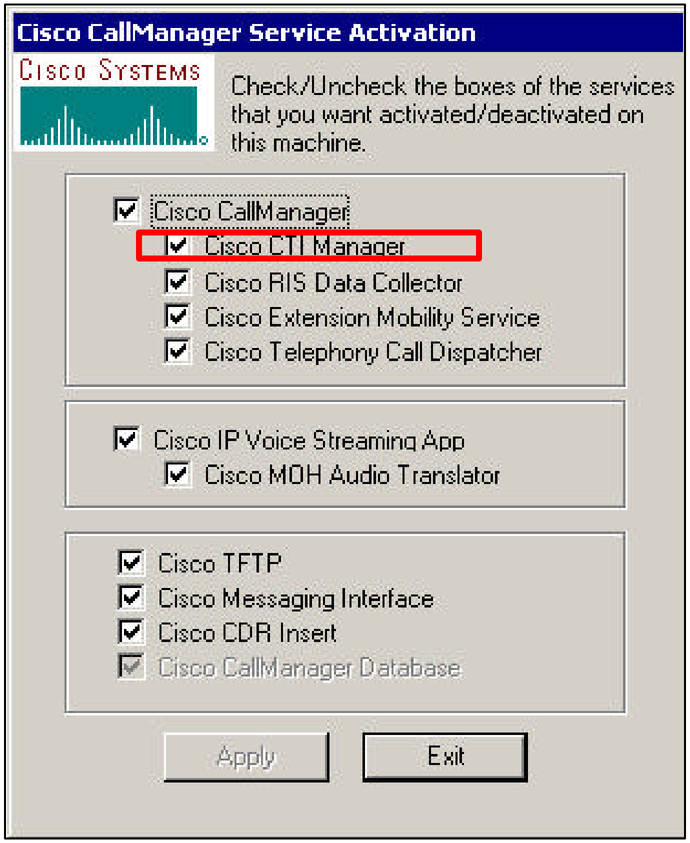
3. ICD Receives Incoming Call from IVR, Checks to Agent Is On-Hook via 3rd Party Control; Redirects Calls to Agent (3000)

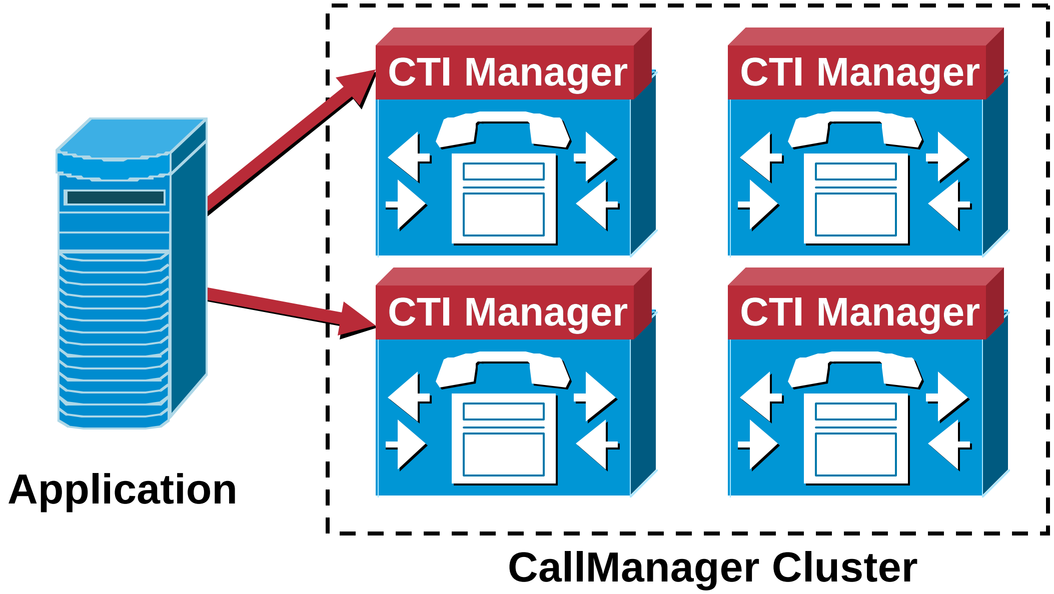
IVR = Interactive Voice Response
ICD = Intelligent Call Distribution

Call Processing Agenda

- Redundancy and Scalability
- CallManager Provisioning
- (J)TAPI and CTI Concepts
- CTI Provisioning
- Inter-Cluster Trunks and H.323

CTI Provisioning
CTI Manager Configuration





800 CTI Connections/Associations per CallManager

3200 CTI Connections/Associations per Cluster

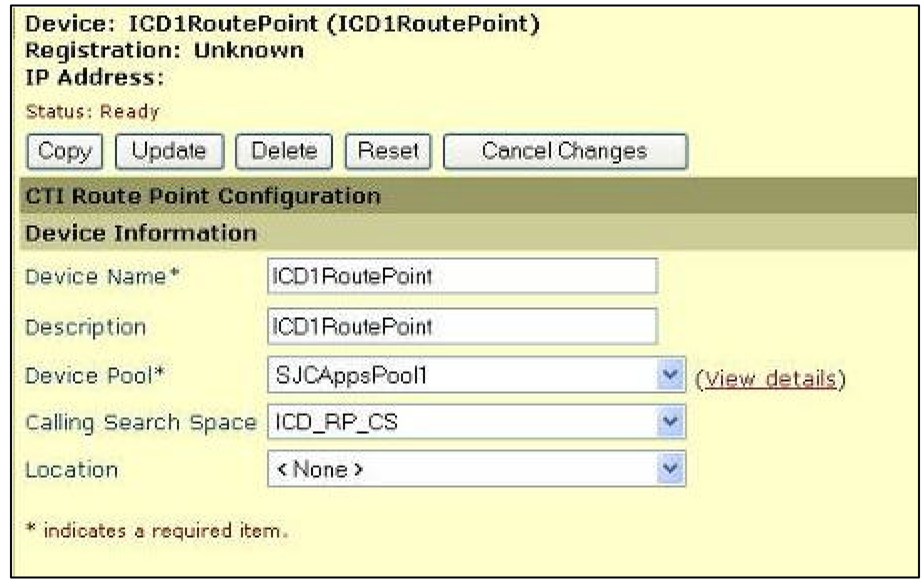
(2500/10,000+ with CM 3.3↑ and MCS 7845's)

- **Primary and backup CTI Managers configured in the application**
- **CTI managers installed co-resident with CallManager**

CTI Provisioning
CTI Device Configuration

Cisco.com

CTI Route Point
- Device pool (redundancy)
- Calling search space
- Multiple lines



Device: ICD1RoutePoint (ICD1RoutePoint)
Registration: Unknown
IP Address:

Status: Ready

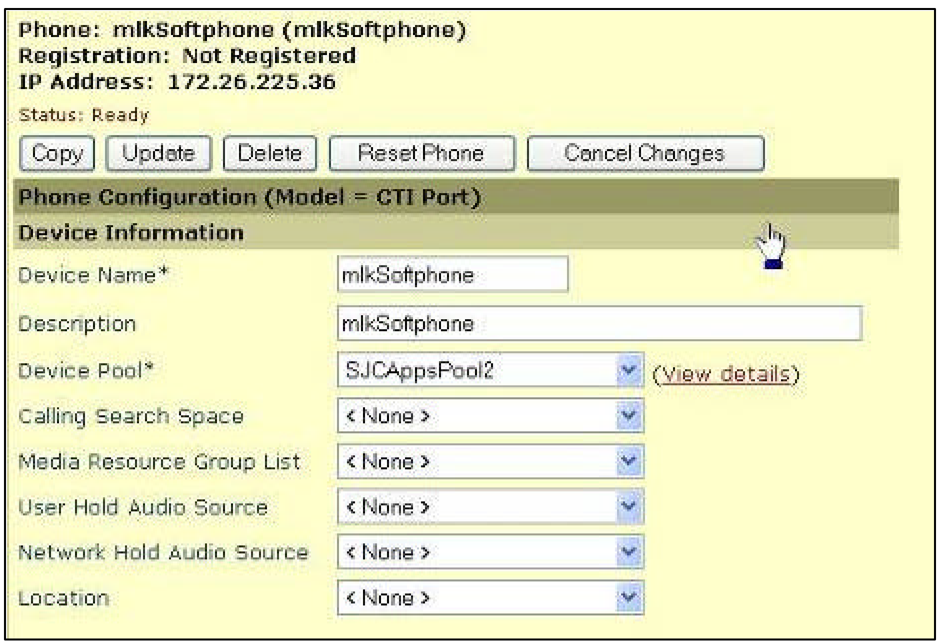
Copy | Update | Delete | Reset | Cancel Changes

CTI Route Point Configuration

Device Information

Device Name*	ICD1RoutePoint
Description	ICD1RoutePoint
Device Pool*	SJCAppsPool1 (View details)
Calling Search Space	ICD_RP_CS
Location	< None >

* indicates a required item.



Phone: mlkSoftphone (mlkSoftphone)
Registration: Not Registered
IP Address: 172.26.225.36

Status: Ready

Copy | Update | Delete | Reset Phone | Cancel Changes

Phone Configuration (Model = CTI Port)

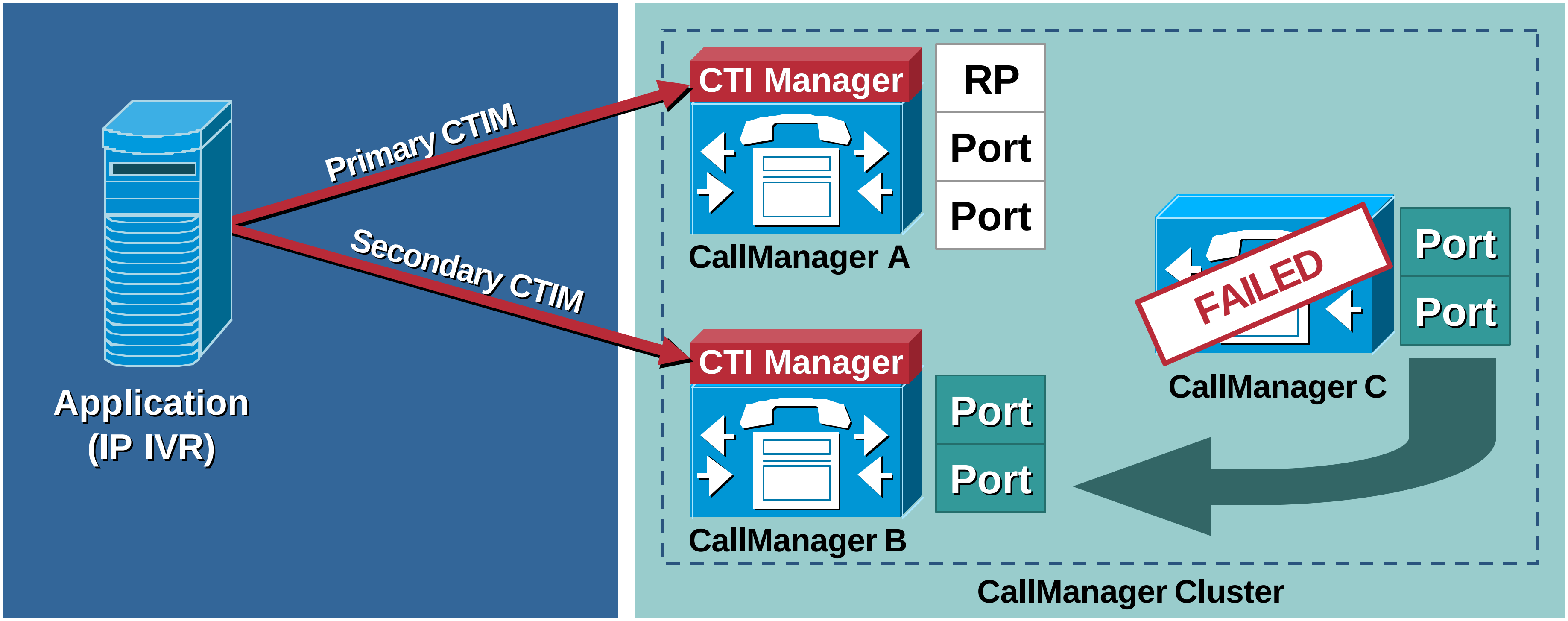
Device Information

Device Name*	mlkSoftphone
Description	mlkSoftphone
Device Pool*	SJCAppsPool2 (View details)
Calling Search Space	< None >
Media Resource Group List	< None >
User Hold Audio Source	< None >
Network Hold Audio Source	< None >
Location	< None >

CTI Port
- Device pool (redundancy)
- Device CSS
- Media resource settings
- Multiple lines

CTI Provisioning
CTI Manager Redundancy

Cisco.com



Application Redundancy

Primary CTIM Is CallManager A

Secondary CTIM Is CallManager B

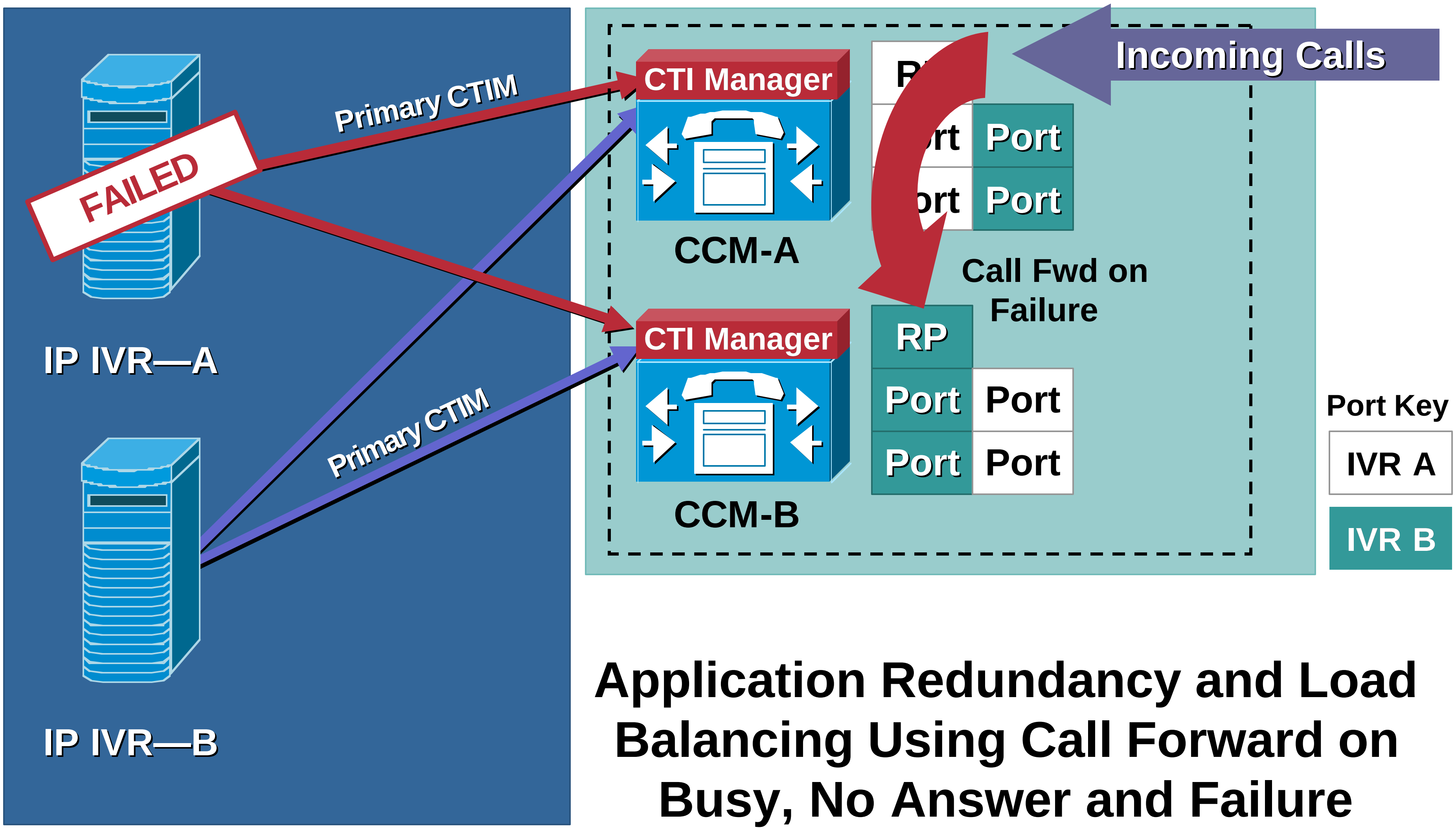
Device Redundancy for Port

CTI Port's Primary CallManager Is C

CTI Port's Secondary CallManager Is B

CTI Provisioning
Application Redundancy and Load Balancing

Cisco.com



Application Redundancy and Load Balancing Using Call Forward on Busy, No Answer and Failure

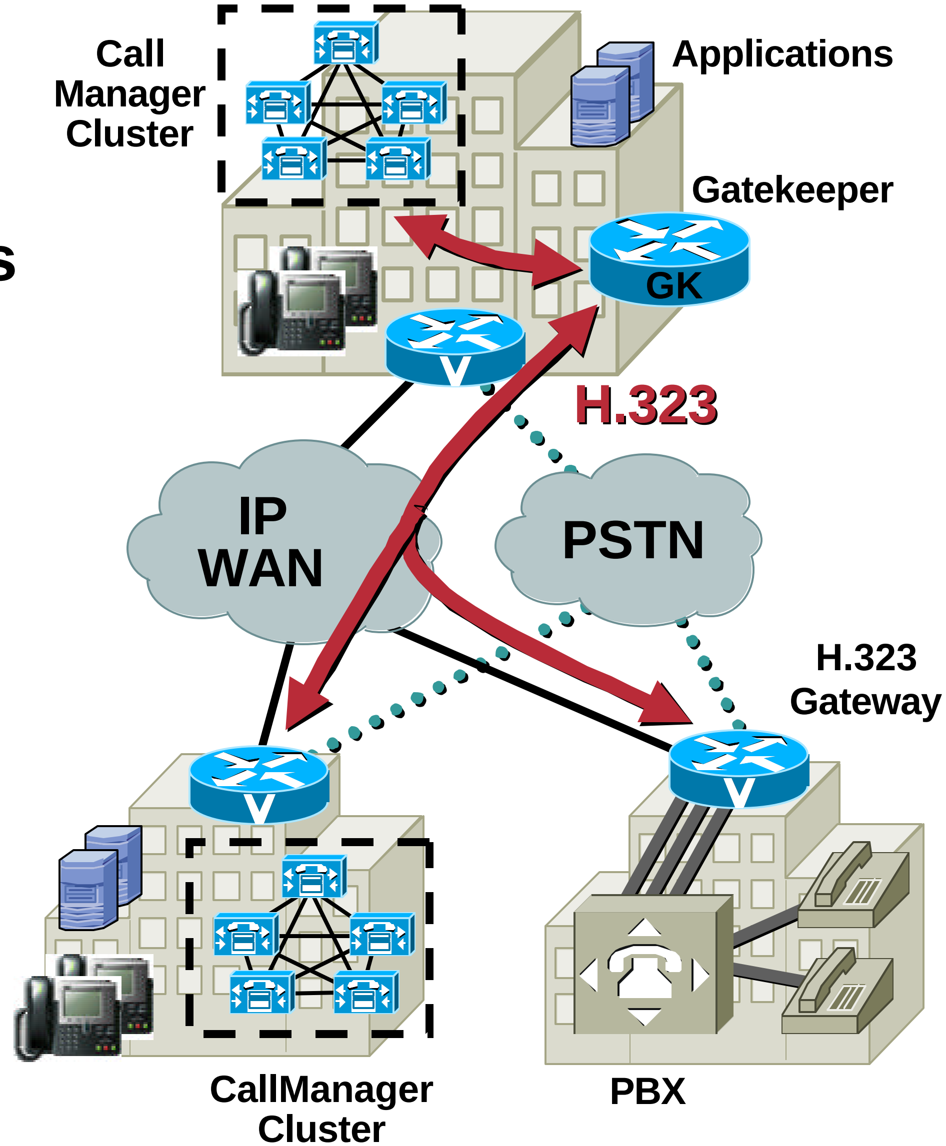
Call Processing Agenda

- Redundancy and Scalability
- CallManager Provisioning
- (J)TAPI and CTI Concepts
- CTI Provisioning
- Inter-Cluster Trunks and H.323

Inter-Cluster Trunks and H.323

Auto-Discovery for Inter-Cluster Trunks

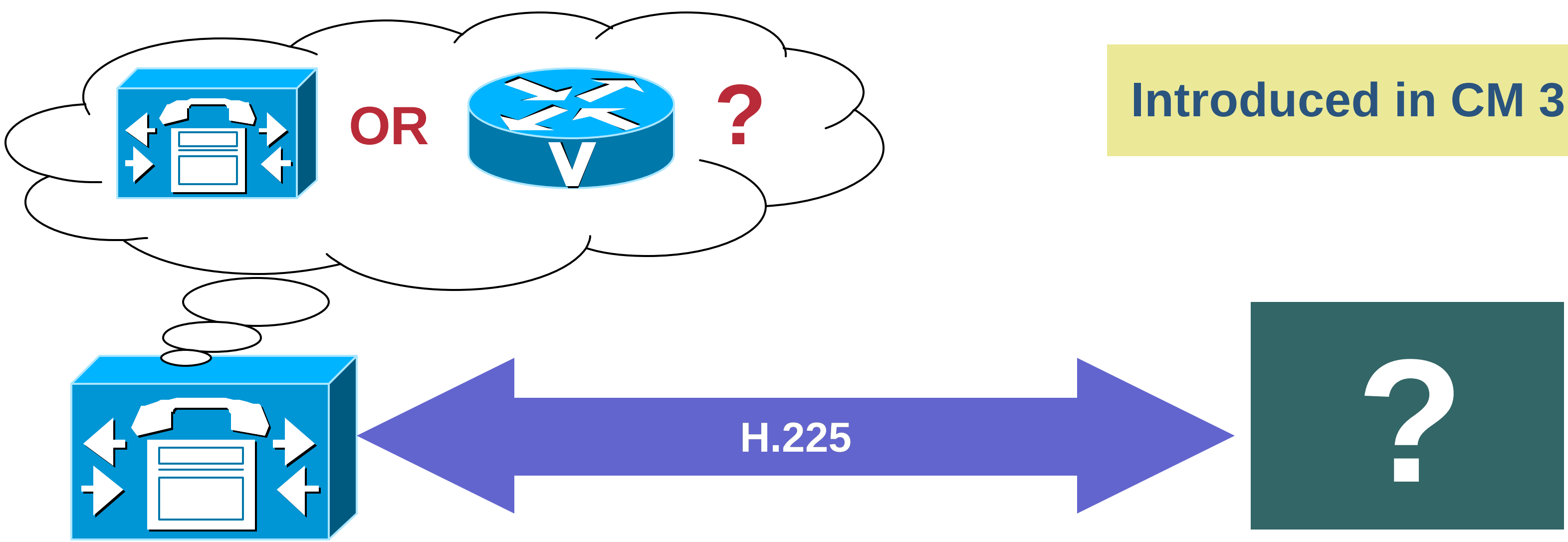
- **Allows a mix-and-match of CallManager clusters and H.323 gateways**
- **All calls across the WAN are controlled by the same gatekeeper**
- **Facilitates migration from toll bypass networks**



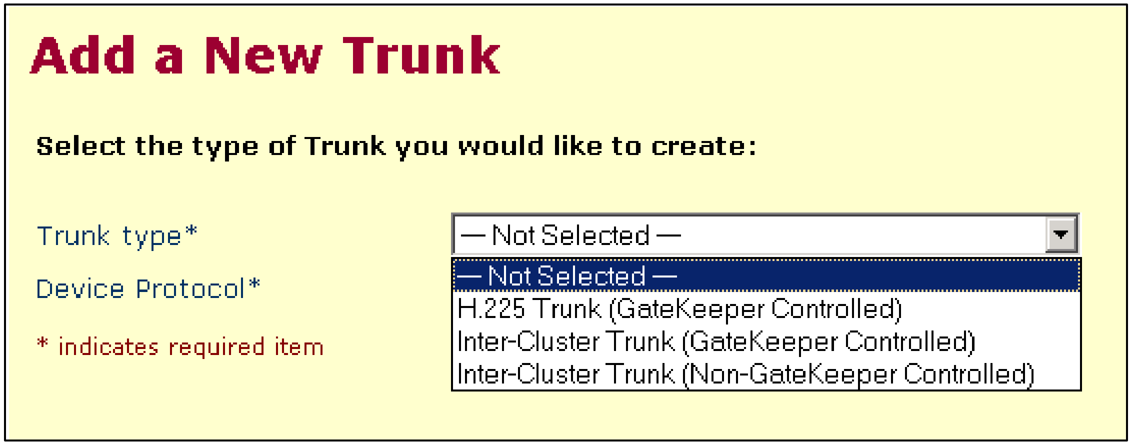
Inter-Cluster Trunks and H.323
Auto-Discovery Mechanism

- During H.225 setup, CallManager identifies itself to the remote device
- If the remote device identifies itself as another CallManager, supplementary services can be used
- Otherwise, the default protocol is used

Introduced in CM 3.2



Inter-Cluster Trunks and H.323
Inter-Cluster Trunk Gateways (CM 3.3↑)

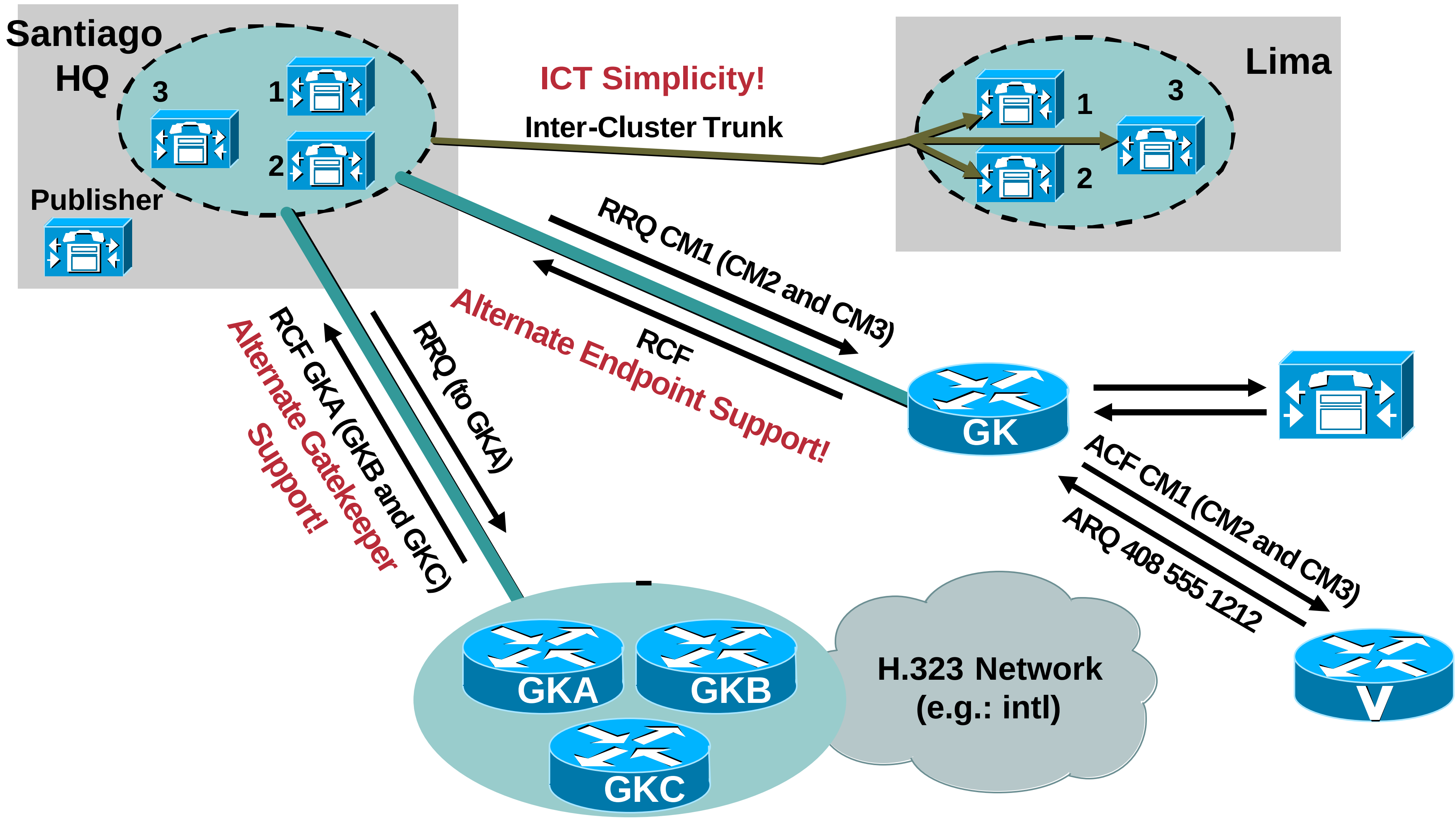


- **The H.225 trunk (Enhanced anonymous device)**
  - **Auto selects between H.225 and standard ICT protocols**
  - **Requires release 3.2 or later at all CallManager sites**
- **Inter-cluster trunk (Enhanced inter-cluster trunk protocol)**
  - **Auto selects between H.225 and ICT protocols (version aware)**
  - **Requires release 3.2 or later at all CallManager sites**

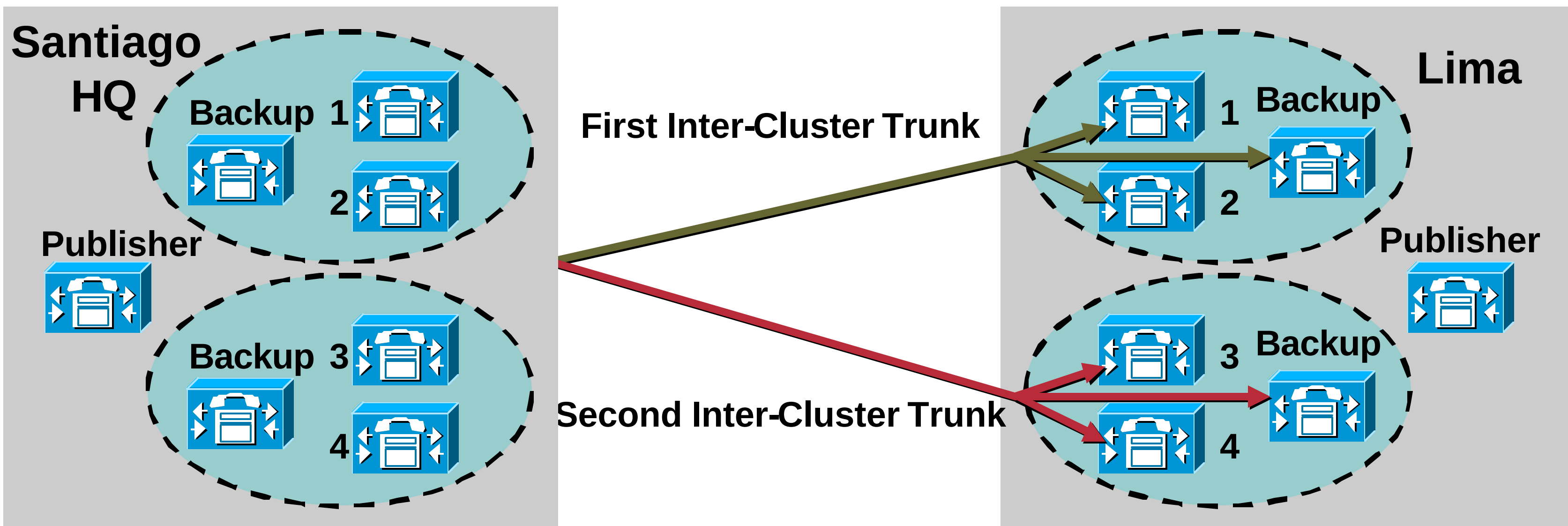
Route Group Devices

H.323 Trunks (3.3↑): New Simplicity and Possibilities

Cisco.com



Inter-Cluster Trunks: Redundancy



Remote Cisco CallManager Information

Server 1 IP Address/Host Name*	172.16.1.100
Server 2 IP Address/Host Name	172.16.2.100
Server 3 IP Address/Host Name	172.16.3.100

* indicates required item

Back to Find/List Trunk

As of CallManager 3.3, Redundancy Is Built into the Inter-Cluster Trunk

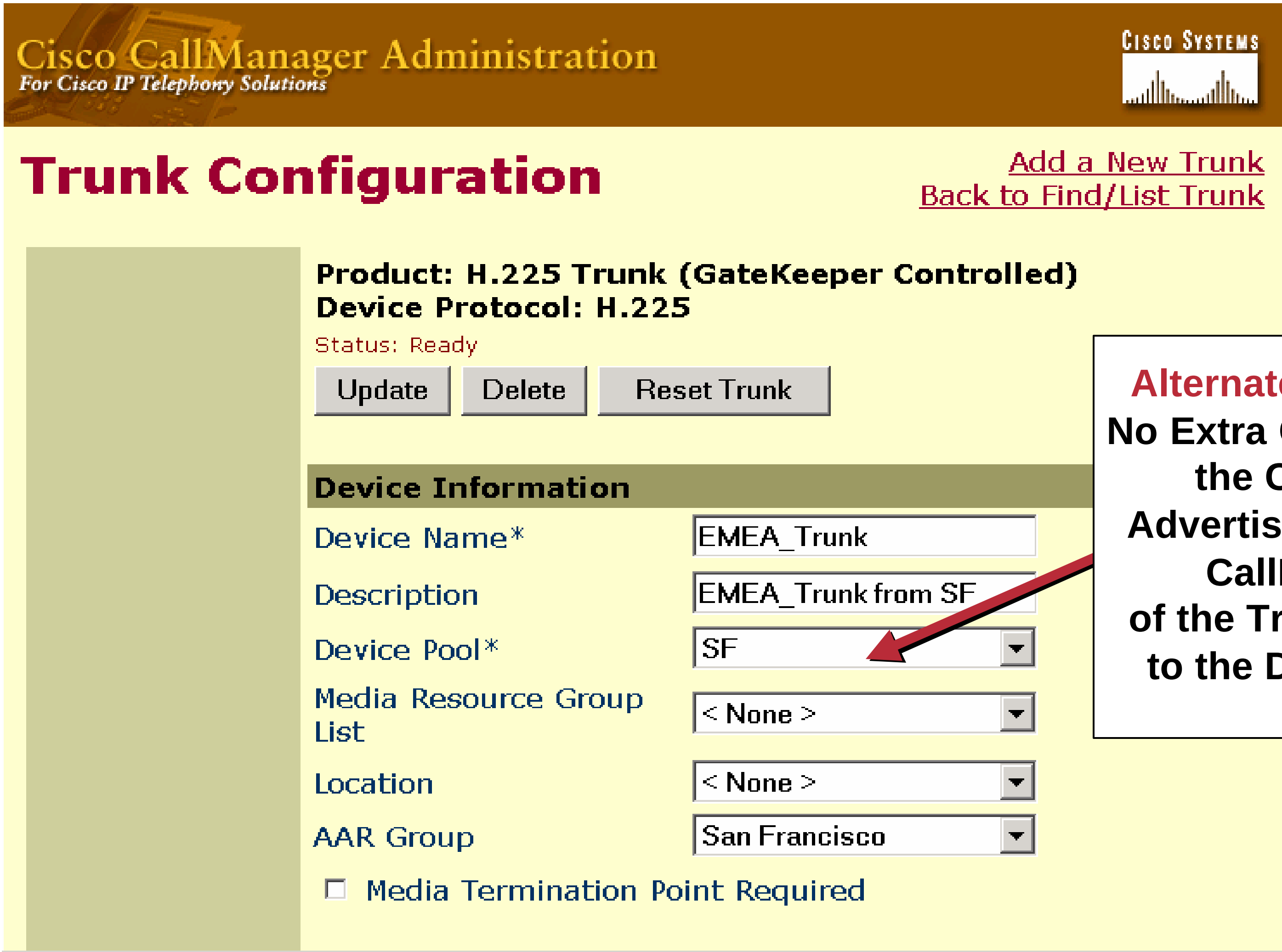
(2 ICTs instead of 6)

Configuration: Inter-Cluster Trunk

Cisco.com

- Calls to an inter-cluster trunk without GK-control are load shared in a round robin fashion among the configured peer signaling addresses
- For example, the first call is routed to peer transport address 1, next call to peer transport address 2, third call to transport address 3, fourth call to transport address 1, and so forth
- Use route-lists/route-groups to provide more specifc control

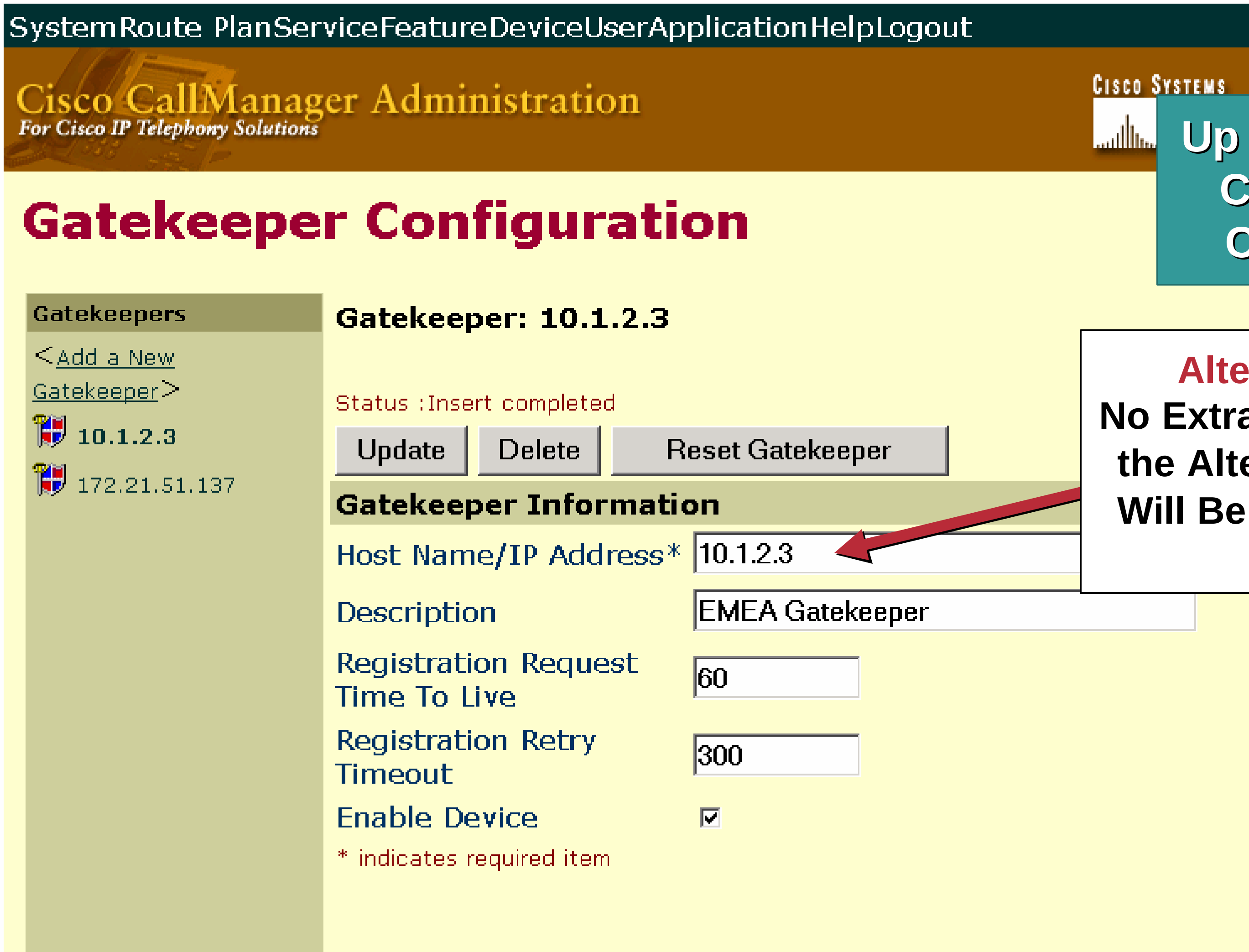
Alternate Endpoint Support



Alternate Endpoint Support

No Extra Config Needed Here; the CallManager Will Advertise All Servers in the CallManager Group of the Trunk (as Associated to the Device Pool) in the RRQ

Alternate GK Support



Up to 10 Gatekeepers Can Be Defined in CallManager 3.3↑

Alternate GK Support

No Extra Config Needed Here; the Alternate GK Addresses Will Be Returned in the RCF from this GK

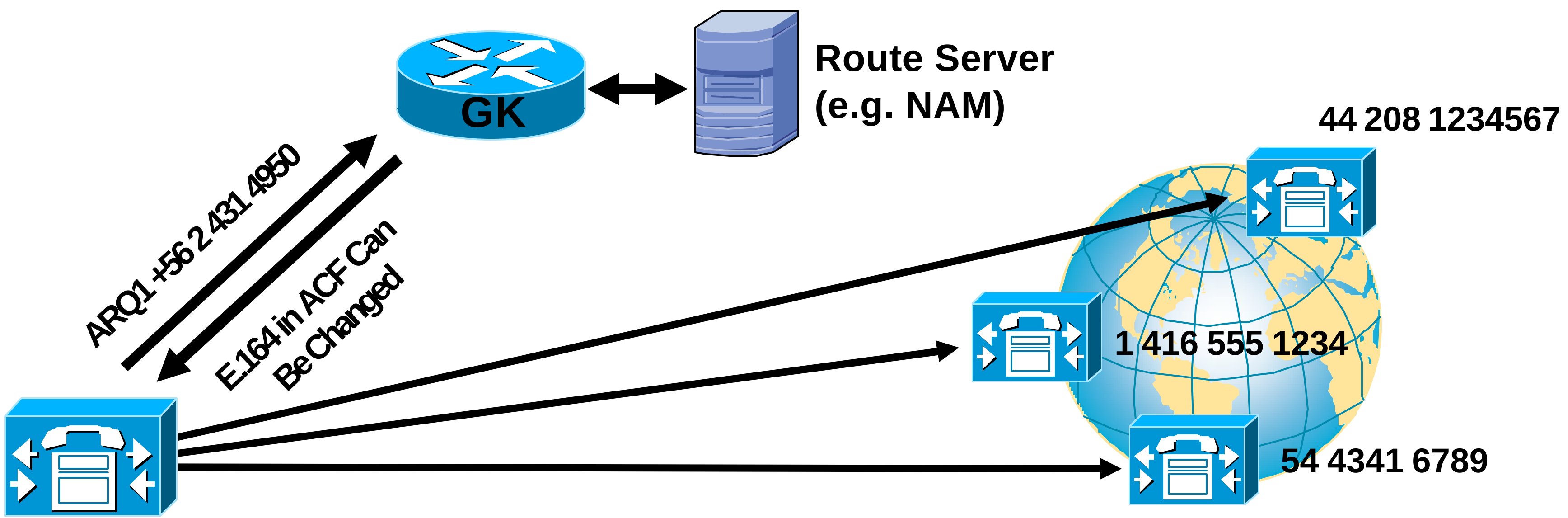
H.323 Trunk Possibilities

Cisco.com

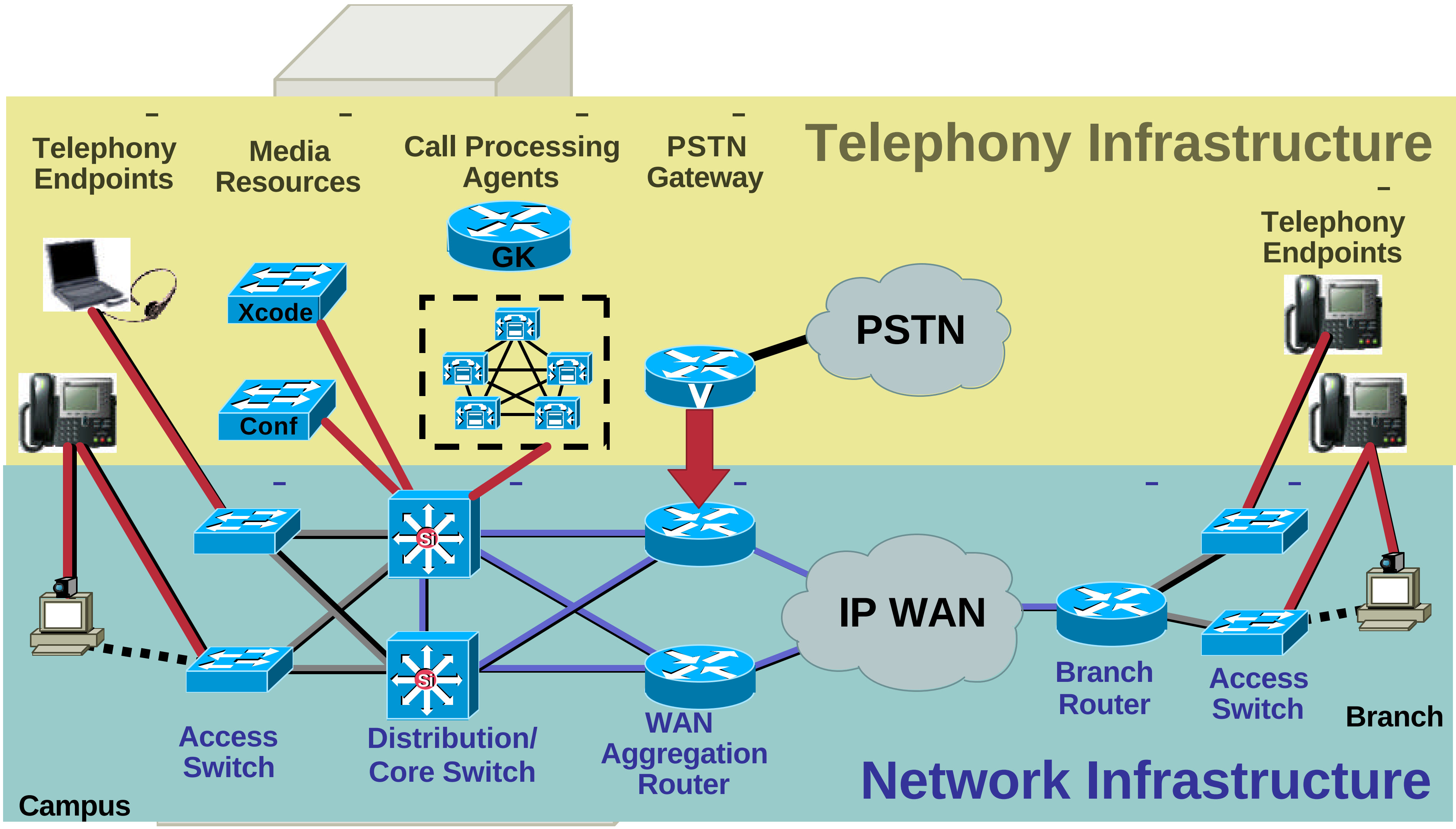
- Up to 10 Gatekeepers can be defined
- Trunks allow multiple path into IP telephony networks: IP PTT, international IP IXCs, etc…
- When a GK-controlled trunk is configured with more than one CCM in the device pool, CCM will automatically send RRQ with alternate endpoints when backup CCM(s) come up in service
- If the given destination call signaling address is unreachable, all of the alternate CCMs in the device pool will be attempted before giving up
- No CLI configuration in Cisco IOS GK is needed (to enable alternate endpoint support)
- Alternate endpoint is supported in Cisco IOS GK load 12.2T

H.323 Enhancements
CanMapAlias

- Time of day routing (follow the sun)
- Follow me service (virtual phone number)
- “Number mobility” single point of administration
- Bank “gold customer”



What We Have Built So Far

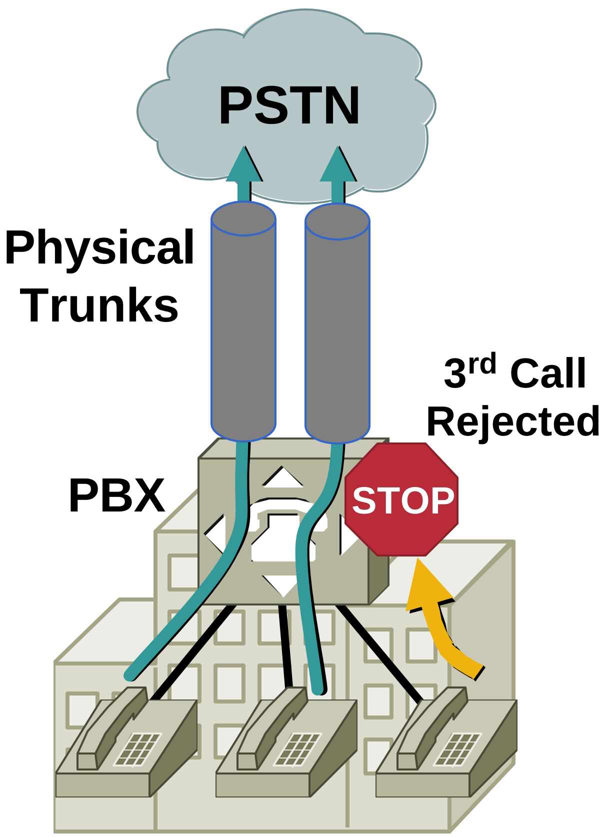


Telephony Infrastructure Agenda (2/2)

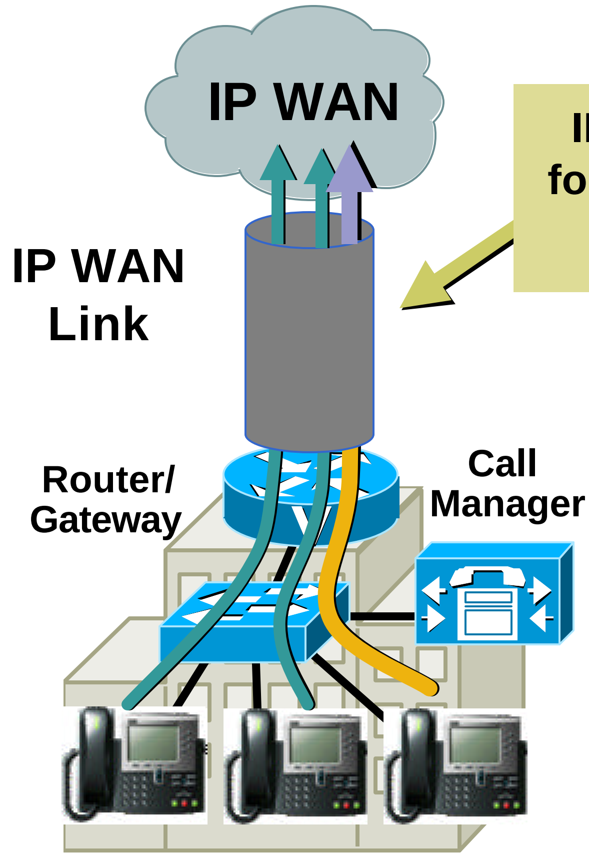
- Call Admission Control
- Survivable Remote Site Telephony
- Call Manager Express
- Dial Plan
- Voice Mail
- Security
- Video Telephony
- Management
- LDAP Directories

Call Admission Control
Why Is It Needed?

Circuit-Switched Networks



Packet-Switched Networks



IP WAN Link Provisioned for 2 VoIP Calls (Equivalent to 2 "Virtual" Trunks)

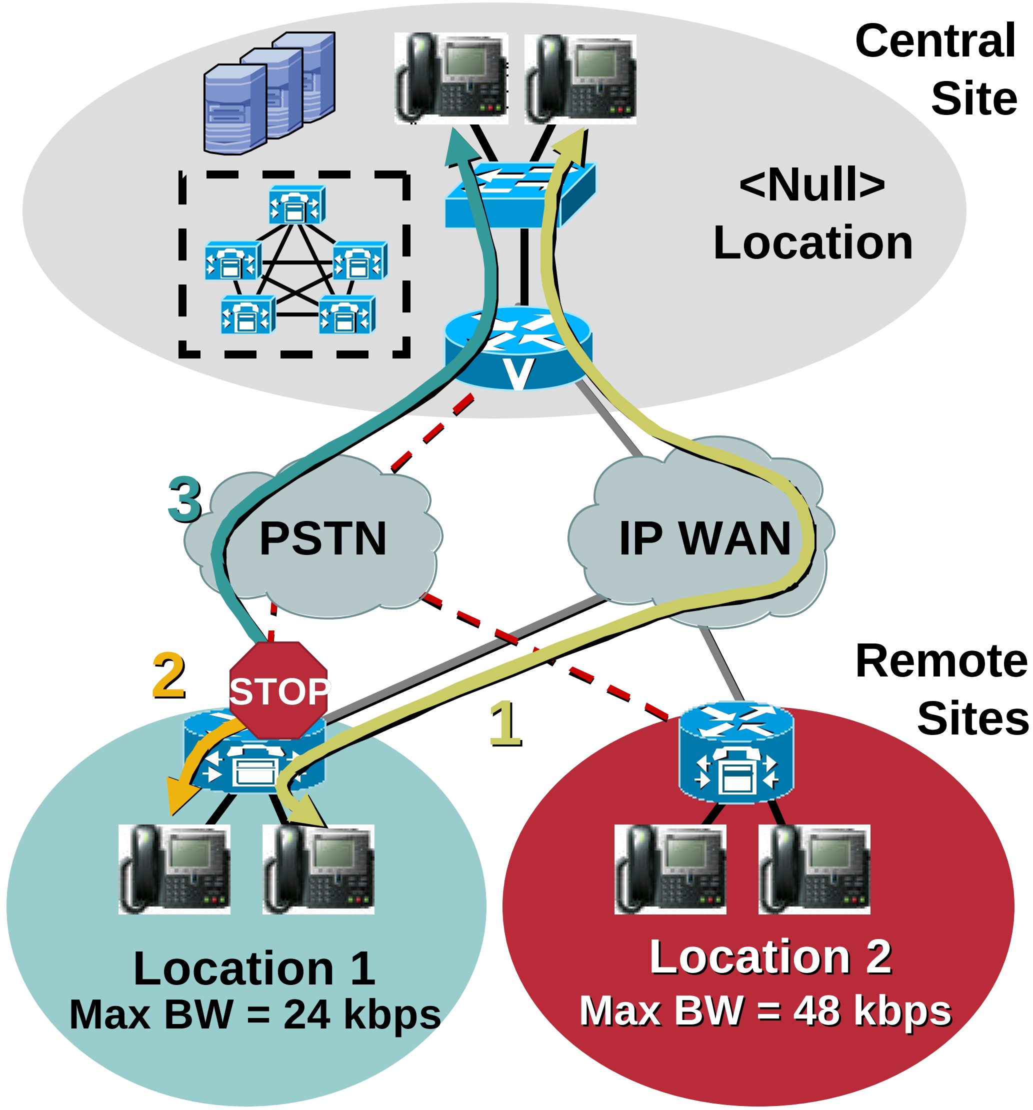
No Physical Limitation on IP Links

If 3rd Call Accepted, Voice Quality of All Calls Degrades

Call Adm. Control Limits # of VoIP Calls on Each WAN Link

Call Admission Control
CallManager “Locations”

- **Prevent WAN link over-subscription by limiting voice bandwidth**
- **Assign bandwidth limit for voice per location**
- **When resources are insufficient, phone gets fast-busy tone and a message is displayed**
- **If automatic alternate routing (AAR) is enabled, the call is automatically rerouted across the PSTN (requires CM 3.3↑)**

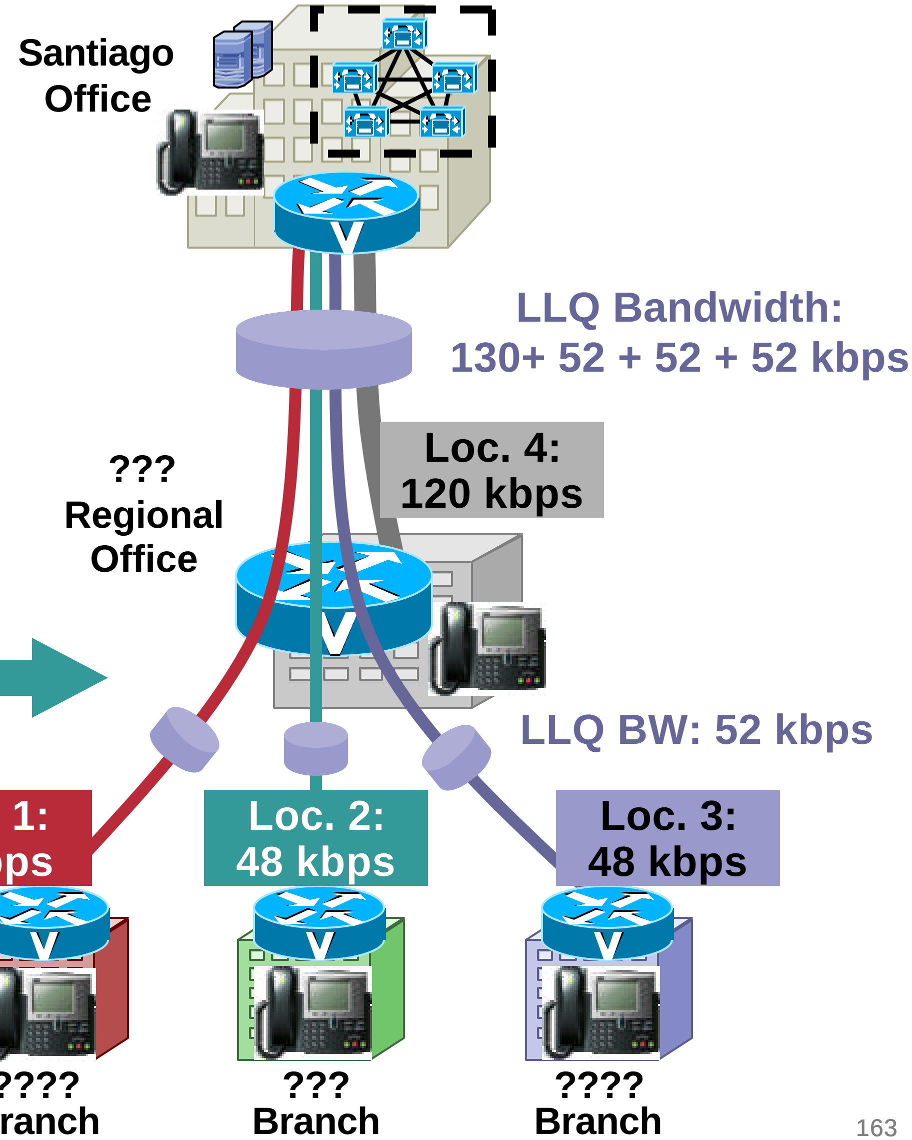


Call Admission Control
Two-Tiered Hub-and-Spoke Topologies

LLQ Bandwidth between Central and Regional sites must be over-provisioned by adding LLQ values for <u>all</u> Branches connected to the Regional site

Regional Site:
- 20 IP phones
- 5 calls across WAN (<u>all links!</u>)

Branches:
- 5 IP phones
- 2 calls across WAN

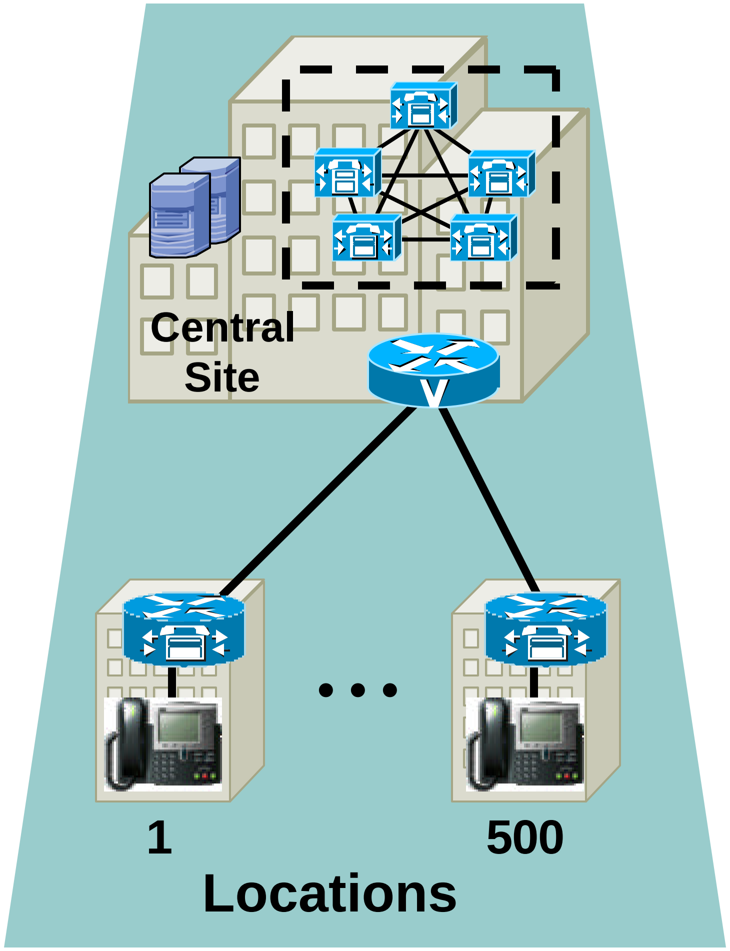


Call Admission Control
CallManager "Locations"

Cisco.com

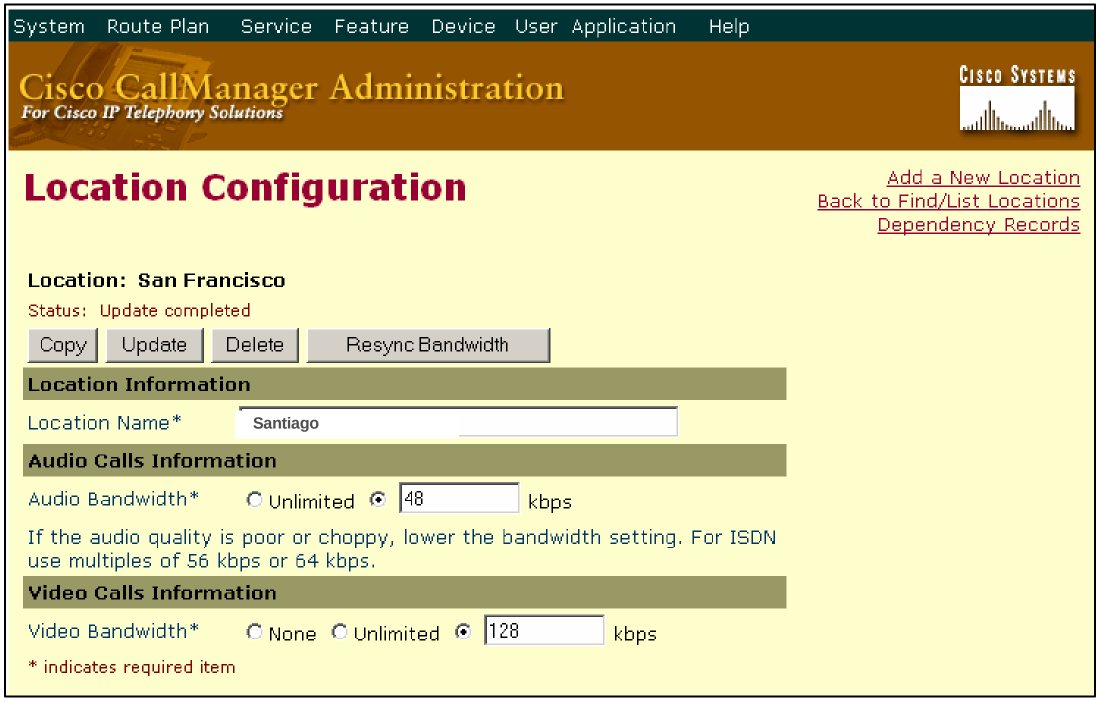
Locations—Deployment Guidelines

- **Hub-and-spoke IP WAN topology**
- **Up to 30,000 lines controlled by a single CallManager cluster (centralized call processing deployments)**
- **Up to 500 locations per CallManager cluster (configuration dependent)**
- **Centralized administration**



Call Admission Control
Video Considerations: Locations

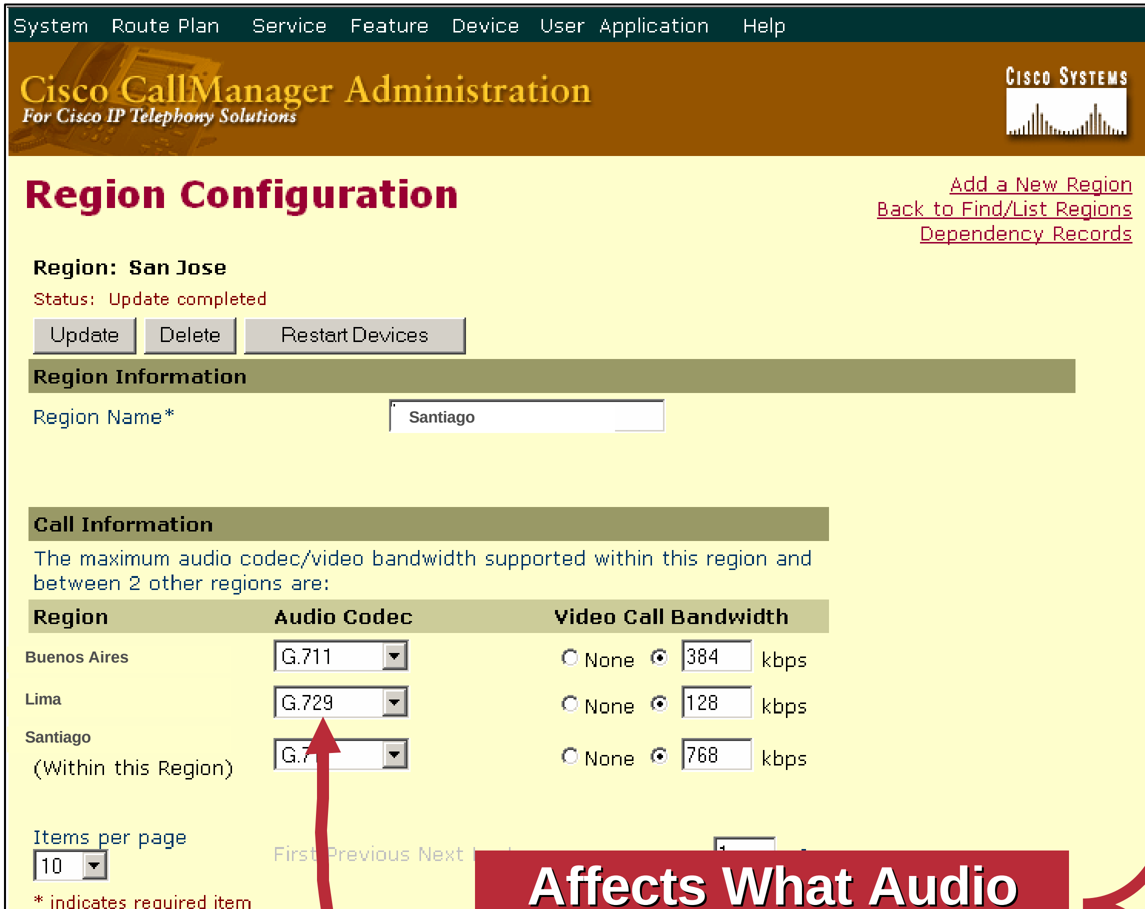
Cisco.com



- **Audio is represented as bit-rate + overhead (i.e. 24k for G.729, 80k for G.711)**
- **Video is represented as bit-rate only (i.e. 384k for a 384k call) and includes the audio portion**
  - **!!!VERY IMPORTANT!!!**
  - **The audio bandwidth setting does not pertain to the audio channel of a video call**
- **Kept separate for a very good reason: voice should have its own dedicated bucket, separate from video, rather than having them fight over one big bucket**
  - **Matches the way it works at Layer-2 in Low-Latency Queuing configurations where video is placed in a separate PQ, or in a CBWFQ, and the audio channel of a video call is placed in the same class as the video channel**

Call Admission Control
Video Considerations: Regions

Cisco.com



Affects What Audio Codec Is Used for Video Calls as Well!

- **Audio is represented by codec while video is represented by speed. Both really mean the same thing: the maximum bit-rate allowed**
- **Video bandwidth includes audio (i.e. 320kbps + 64kbps)**
- **Audio codec also applies to video calls**

!!VERY IMPORTANT!!!

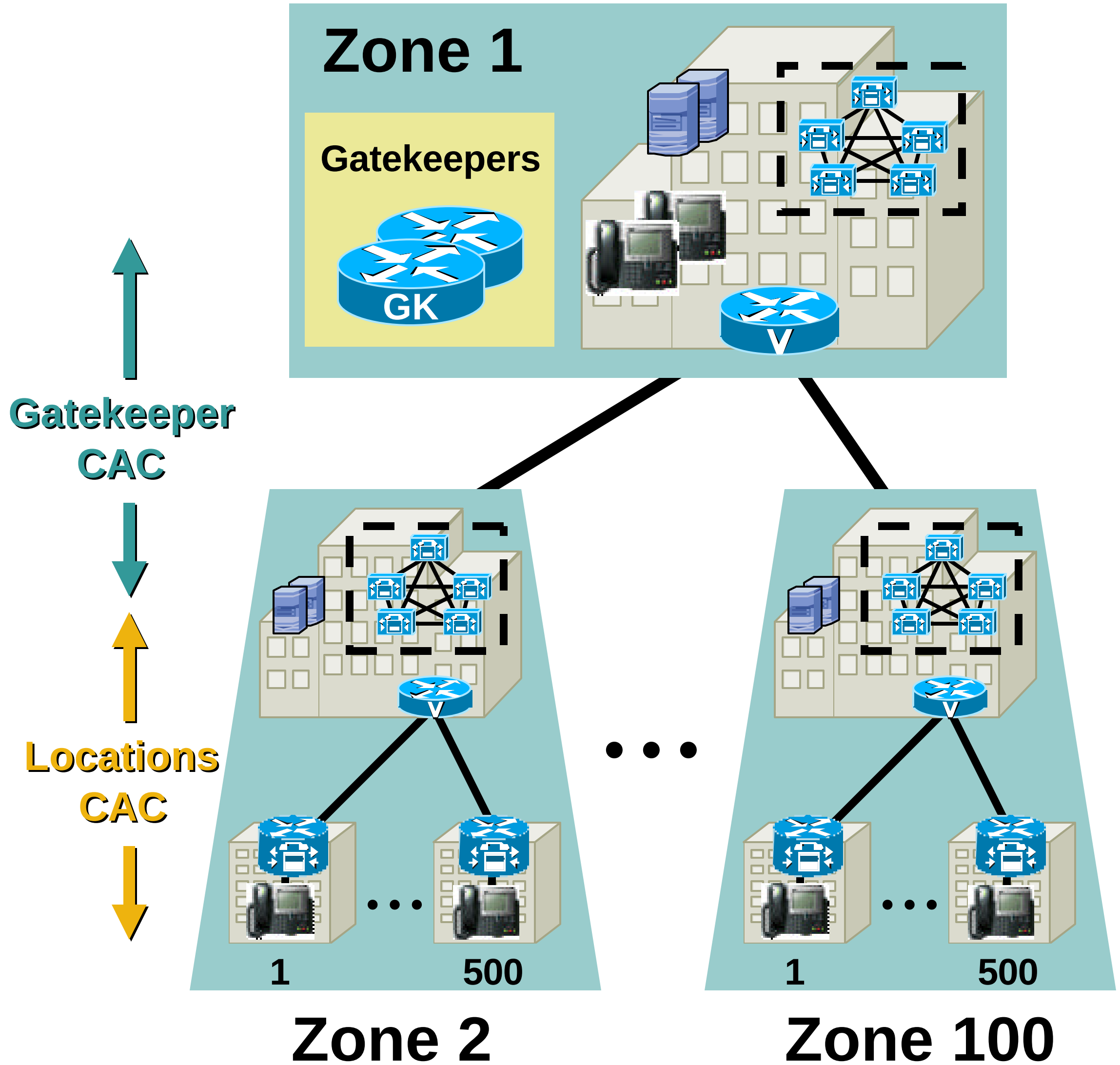
Video endpoints typically only support G.728, G.711 and G.722

Audio endpoints typically only support G.729 and G.711

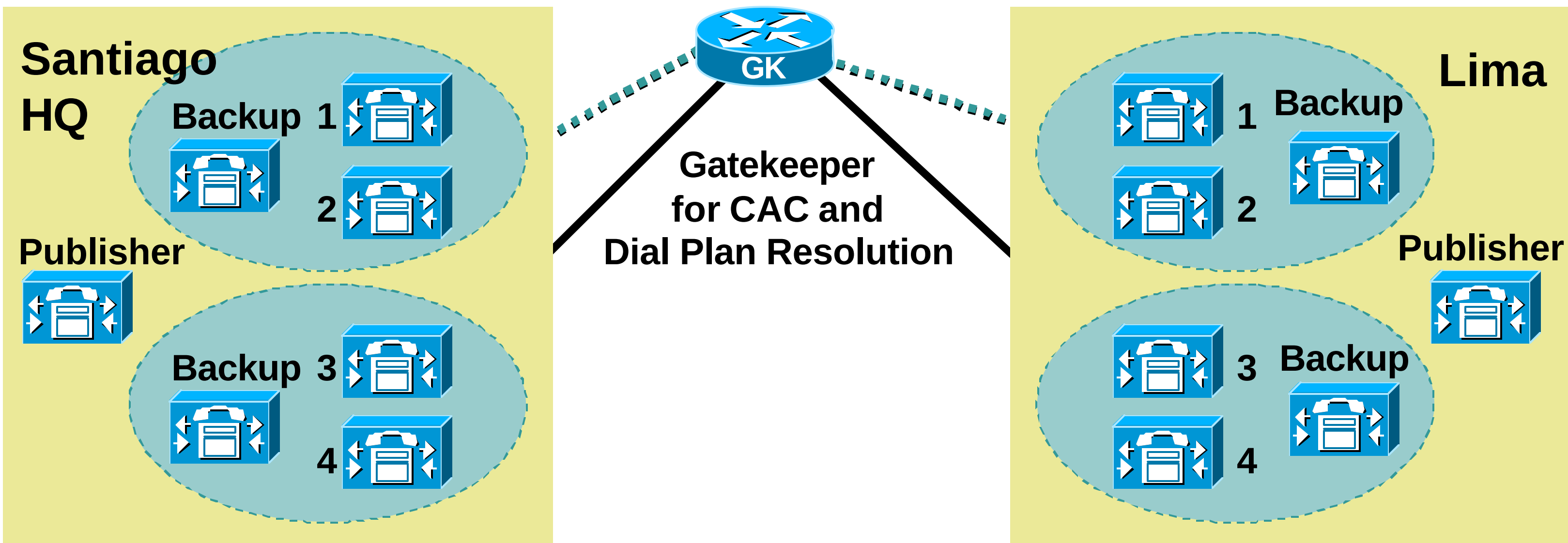
Call Admission Control
Up to 100 CallManager Clusters

Cisco.com

- Hub-and-spoke topology
- 1 CallManager cluster per zone
- 100 CallManager clusters per gatekeeper
- Locations CAC used for remote sites with no CallManager (centralized model)



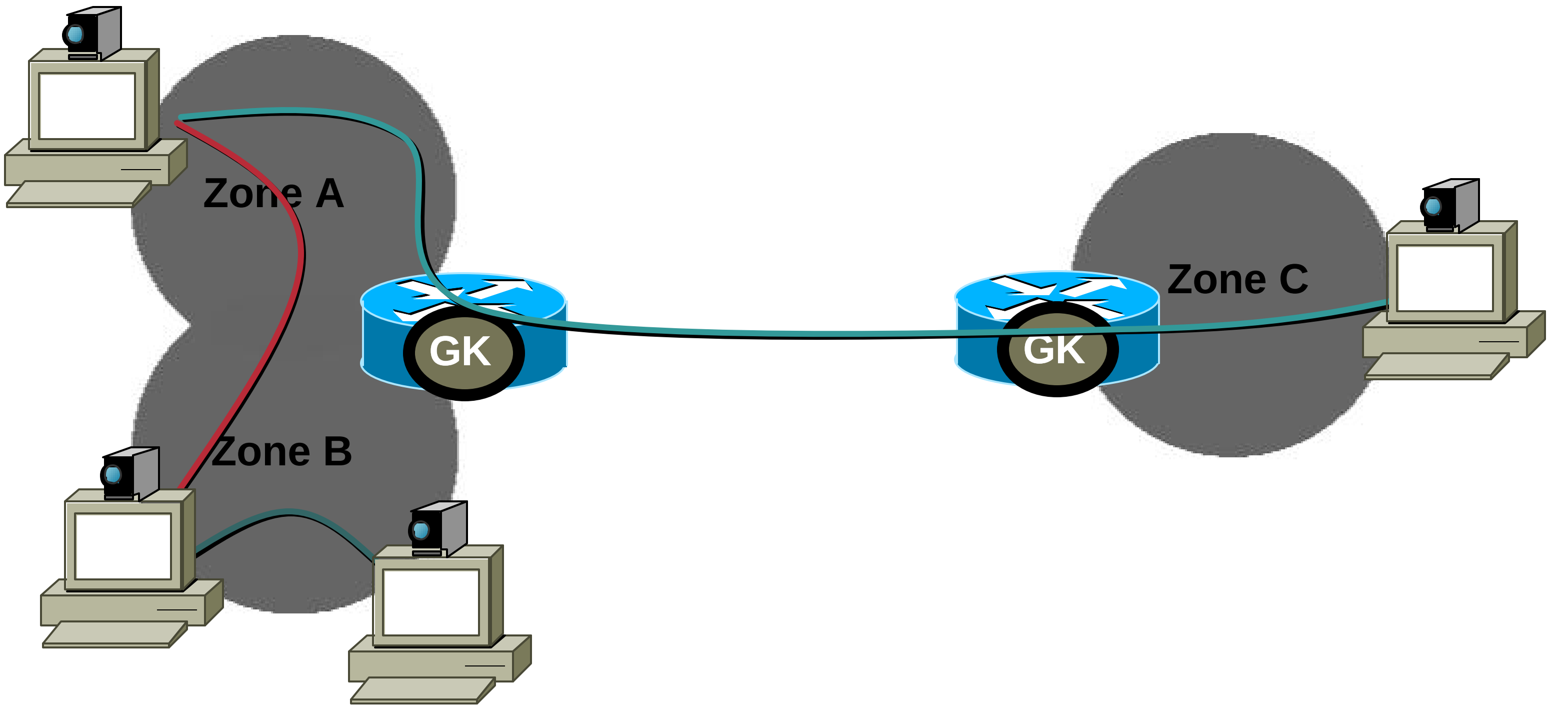
Call Admission Control
Gatekeeper



- Gatekeeper provides call admission control in presence of multiple CallManager clusters (distributed call processing deployments)
- Configure CallManager with “anonymous device” (CM 3.2) or “GK-controlled inter-cluster trunk” (CM 3.3↑) to use gatekeeper also to resolve E.164 addresses

Call Admission Control

Gatekeeper Bandwidth Commands Explained

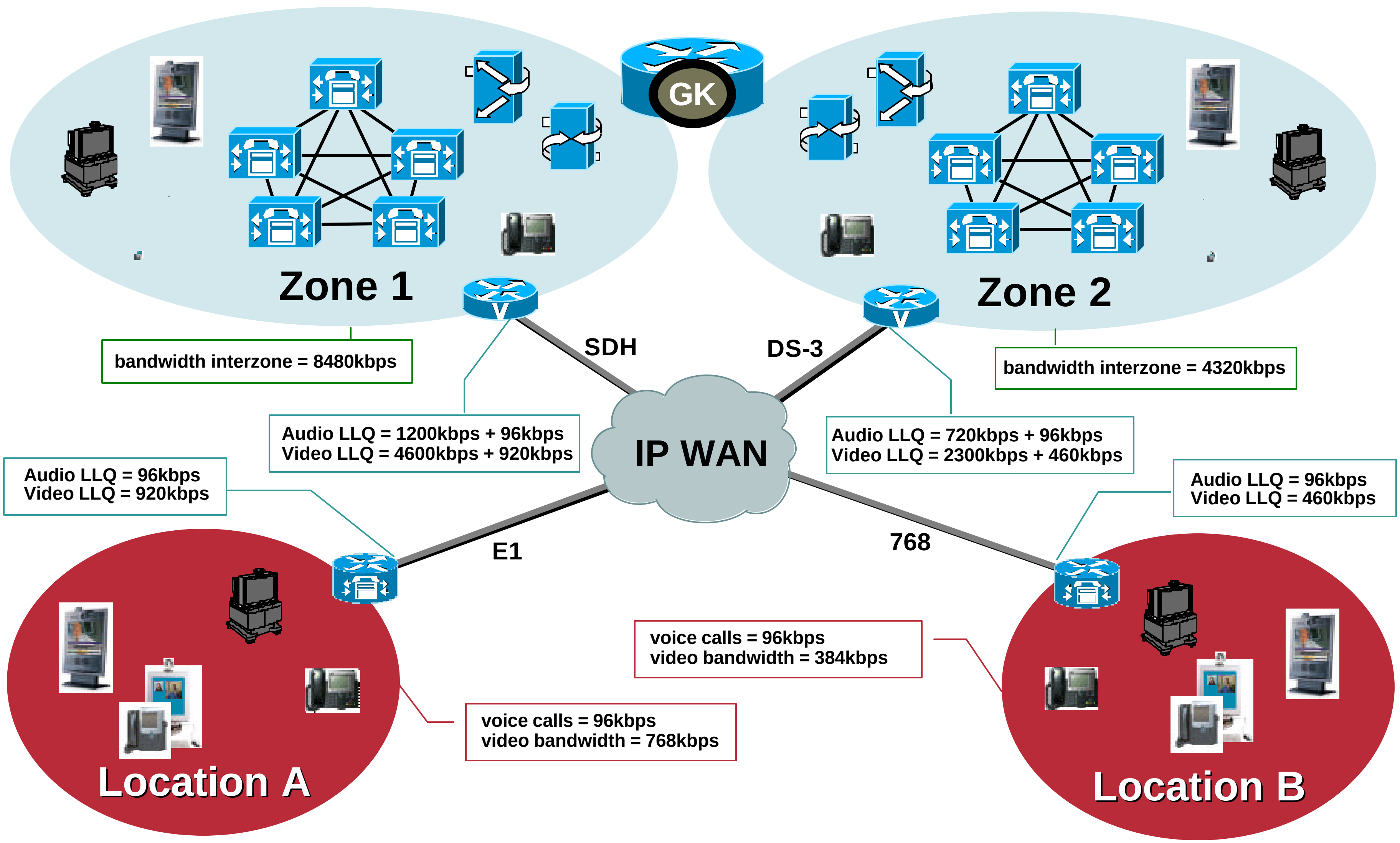


1. Interzone = Bandwidth of all calls for a local zone to/from all other zones
2. Remote = Aggregate bandwidth of all local zone(s) to/from any remote zones
3. Total = Bandwidth of all calls within an individual zone
4. Session = Bandwidth allowed on a per call basis

Call Admission Control

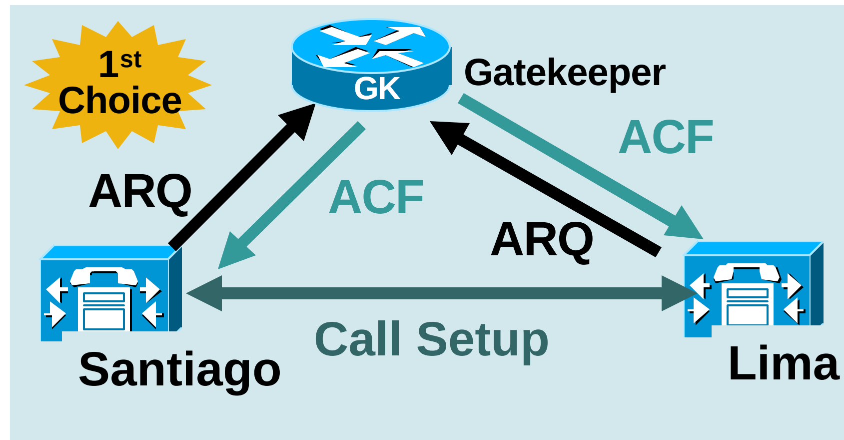
What Values to Use: Example

Zone 1	(50) G.729 calls and (10) 384kbps video calls
Zone 2	(30) G.729 calls and (5) 384kbps video calls
Location A	(4) G.729 calls and (2) 384kbps video calls
Location B	(4) G.729 calls and (1) 384kbps video call

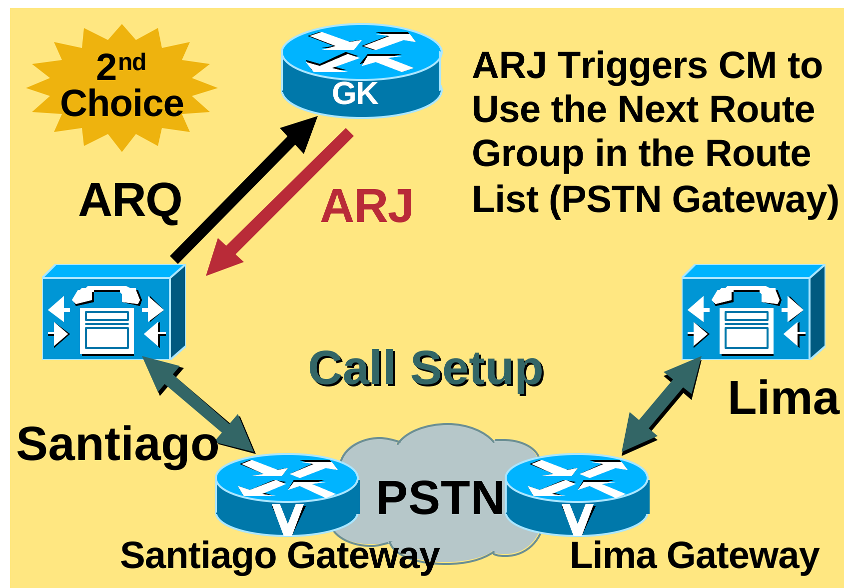


Call Admission Control
Automatic Reroute with Gatekeeper

1. CallManager sends a request to Gatekeeper before making a call between Santiago and Lima
2. Gatekeeper sends a confirmation to admit the call to the network

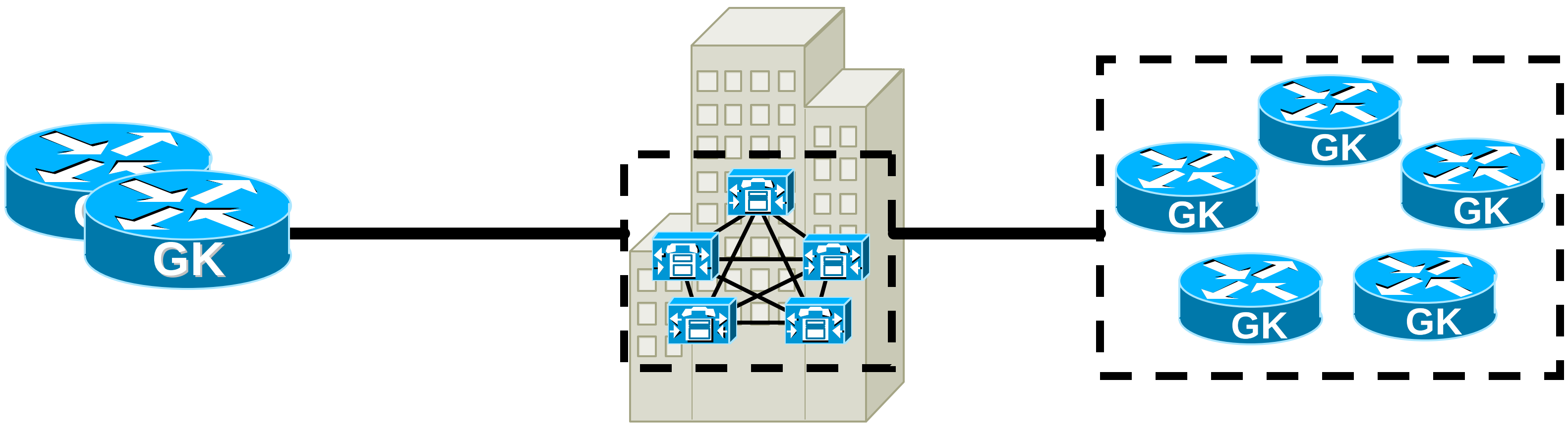


1. CallManager sends a request to Gatekeeper
2. Gatekeeper rejects the call
3. CallManager uses next route group in route list to place the call; In this example, the call to Lima is placed via the PSTN; The end user is unaware of the route taken by the call



Call Admission Control

Gatekeeper Redundancy



HSRP

Same VLAN

Single GK Performance

Works with < CM 3.3

AltGatekeeper

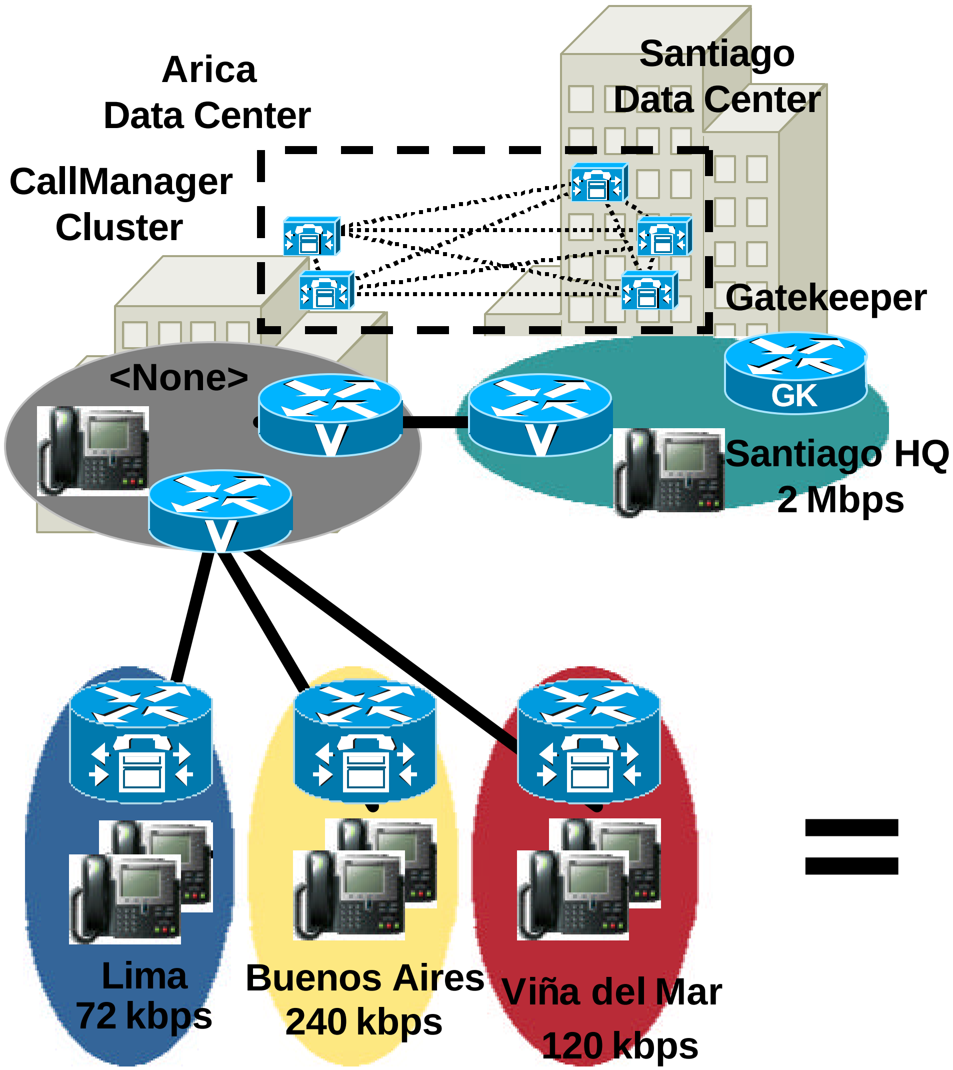
Different Subnets

Load Balancing

Up to 5 GK's in a Cluster

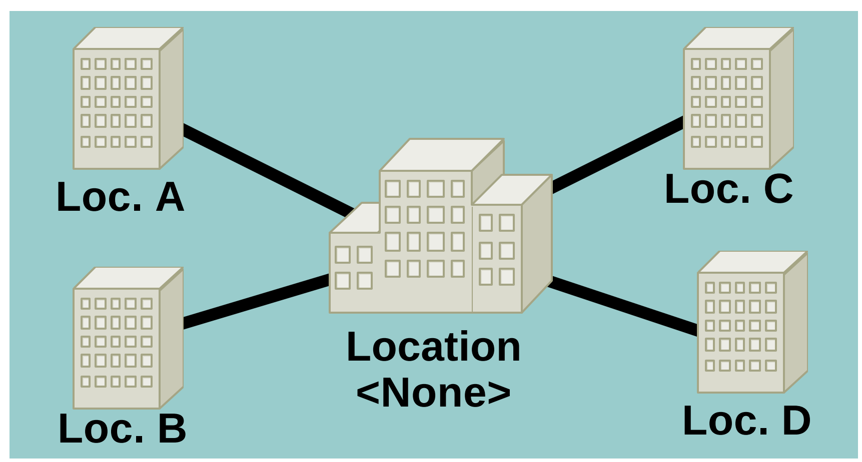
Faster Failover

Call Admission Control
Clustering over the WAN Considerations



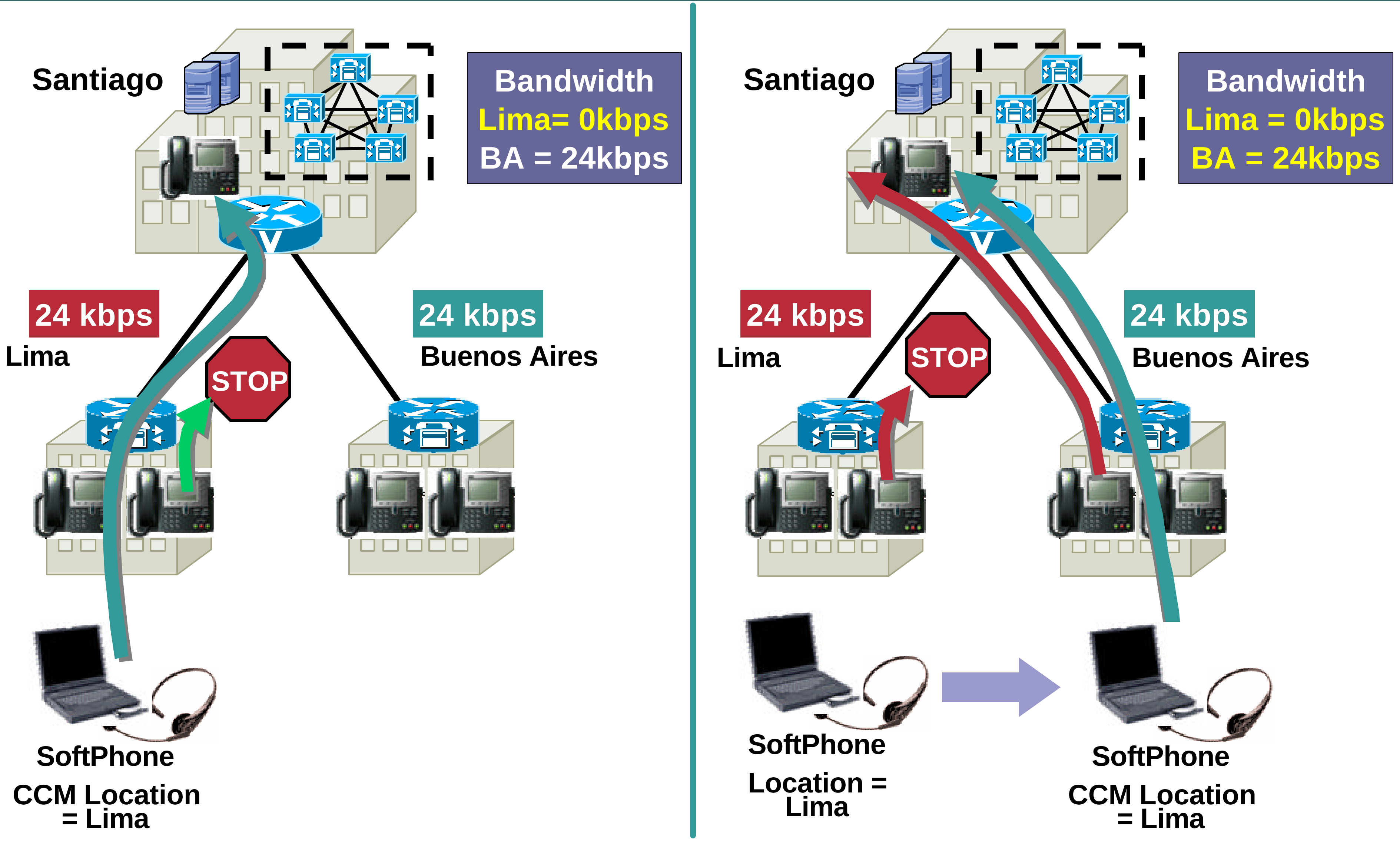
- Need to preserve hub-and-spoke topology
- Leave devices in Arica data center in the <None> location, assign all other sites to locations (up to 500)

=



Call Admission Control
Mobile Users and Locations CAC

Cisco.com



Call Admission Control
Mobile Users and Locations CAC

- Soft clients (such as Communicator) can be used on the road
- Many users combine remote access (e.g.: VPN) and internet-based telephony to access the intranet and the enterprise telephony network
- A possible approach to simplify the configuration of nomadic devices
  - Configure nomadic devices in a "nomad" region to select low BW codec
  - Configure nomadic devices in a "nomad" location with infinite bandwidth
  - Configure classification, trust boundary, and queuing to put media stream in non-priority queue
  - All "soft client" calls thus placed in a best effort queue, not competing for PQ access
- Results are generally very good on the internet and in the CB/WFQ of branches
- Advertise service to users as a best effort system

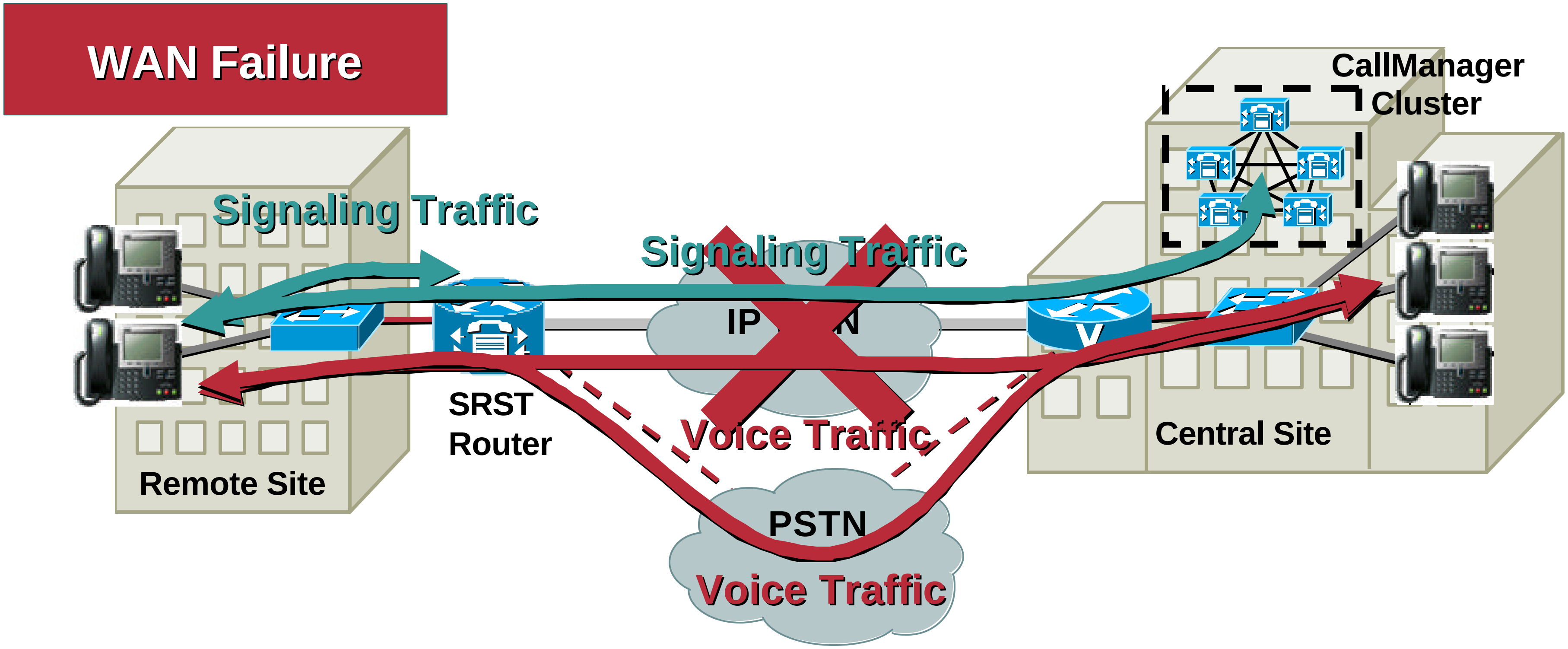
Telephony Infrastructure Agenda (2/2)

Cisco.com

- Call Admission Control
- Survivable Remote Site Telephony
- Call Manager Express
- Dial Plan
- Voice Mail
- Security
- Video Telephony
- Management
- LDAP Directories

Survivable Remote Site Telephony (SRST)
Mode of Operation

Cisco.com



- **SRST router needs minimal configuration**
- **Subset of features available to the phones (DID, DOD, Call Hold, Transfer, Speed Dial, Caller ID)**

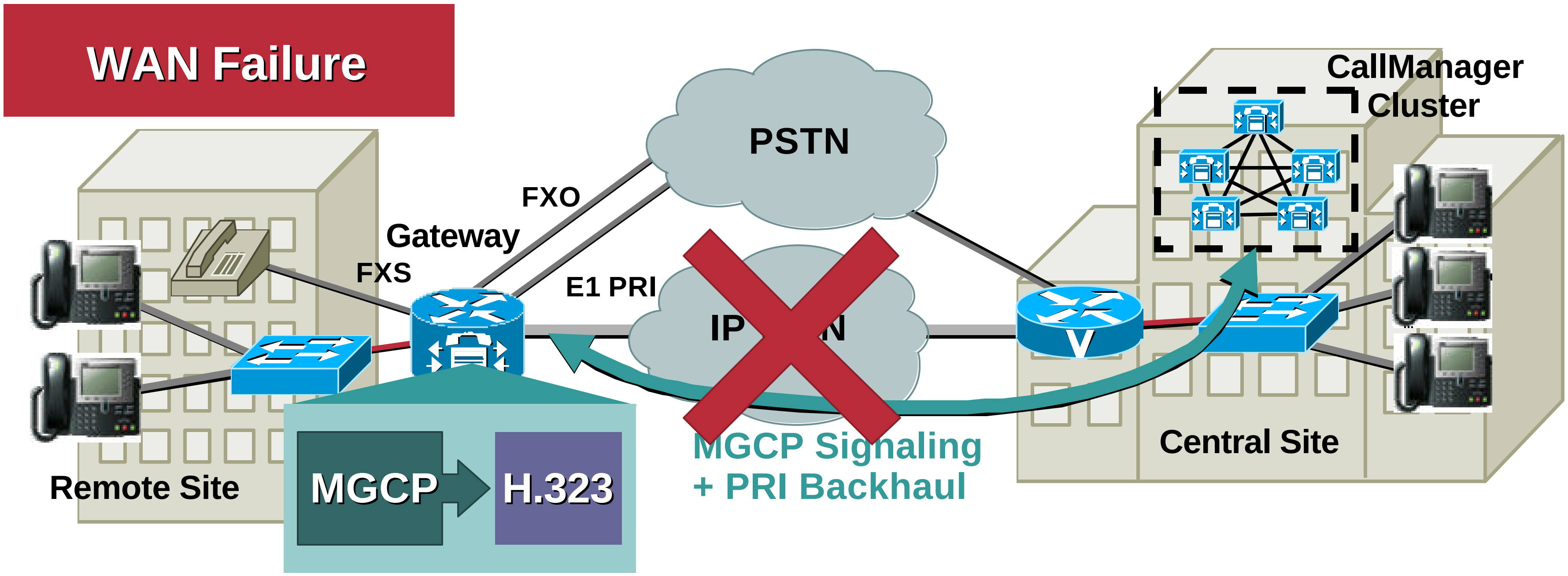
SRST
Configuration Example

Cisco.com

```
dial-peer voice 10 pots
 destination-pattern 0
 port 1/0/0

dial-peer voice 201 voip
 destination-pattern 562365....
 session target ipv4:10.2.10.100

call-manager-fallback
   access-code fxo 0
   default-destination pattern 4000
   dialplan-pattern 1 562365.... extension-length 4
   ip source-address 10.10.10.10 port 2000
   keepalive 30
   max-ephones 24
   max-dn 48
   voicemail 05623651000
   call-forward busy 05623651000
   call-forward noanswer 05623651000
```

SRST
MGCP Fallback to H.323

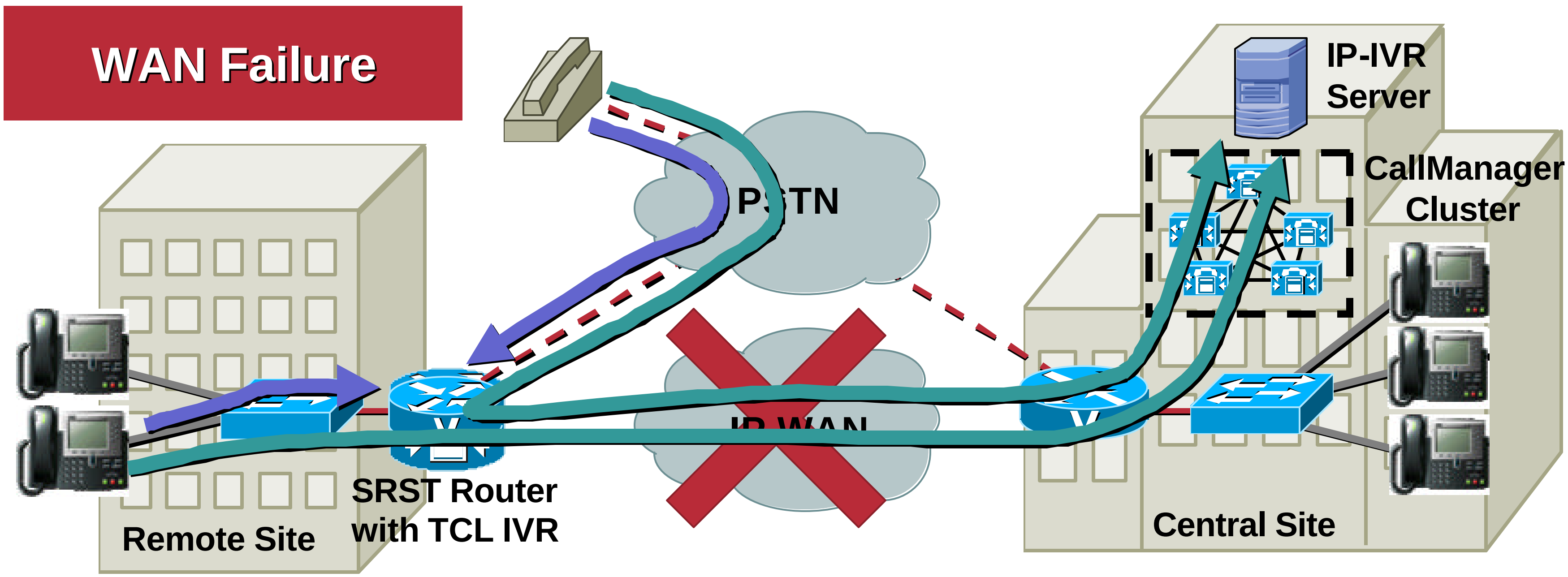
IOS 12.2(11)T



- Under normal operation, the gateway translates FXS/FXO signaling into MGCP and backhauls L3 PRI signaling to CallManager
- When the WAN fails, the gateway reverts to H.323 operation—SRST provides backup for the IP phones

SRST and Applications:
Centralized IP-IVR + Remote TCL IVR

Cisco.com



- **When WAN is up, use centralized IP-IVR**
- **When WAN is down, use Cisco IOS IVR within SRST router (subset of features)**

SRST Feature Set Available Today

Cisco.com

Phone Features:

- Support for all Cisco IP Phones; 7971-GIG, 7970, 7960, 7940, 7912, 7905, 7935, 7914
- Up to eight lines per phone
- Primary line on phone
- Speed and Last Number Dial
- Transfer (without consult)
- Call Hold

Trunk Features:

- PSTN—E1 PRI and E1 R2 trunks support
- Analog FXS and FXO support
- ISDN BRI and PRI support
- WAN link Support: FR, ATM, MLPPP, Serial, DSL
- Distinctive ringing – Internal vs External
- H323 based transfer across Cisco IOS endpoints
- Translation Rules – allows user speed dials to be expanded to use PSTN during WAN outage

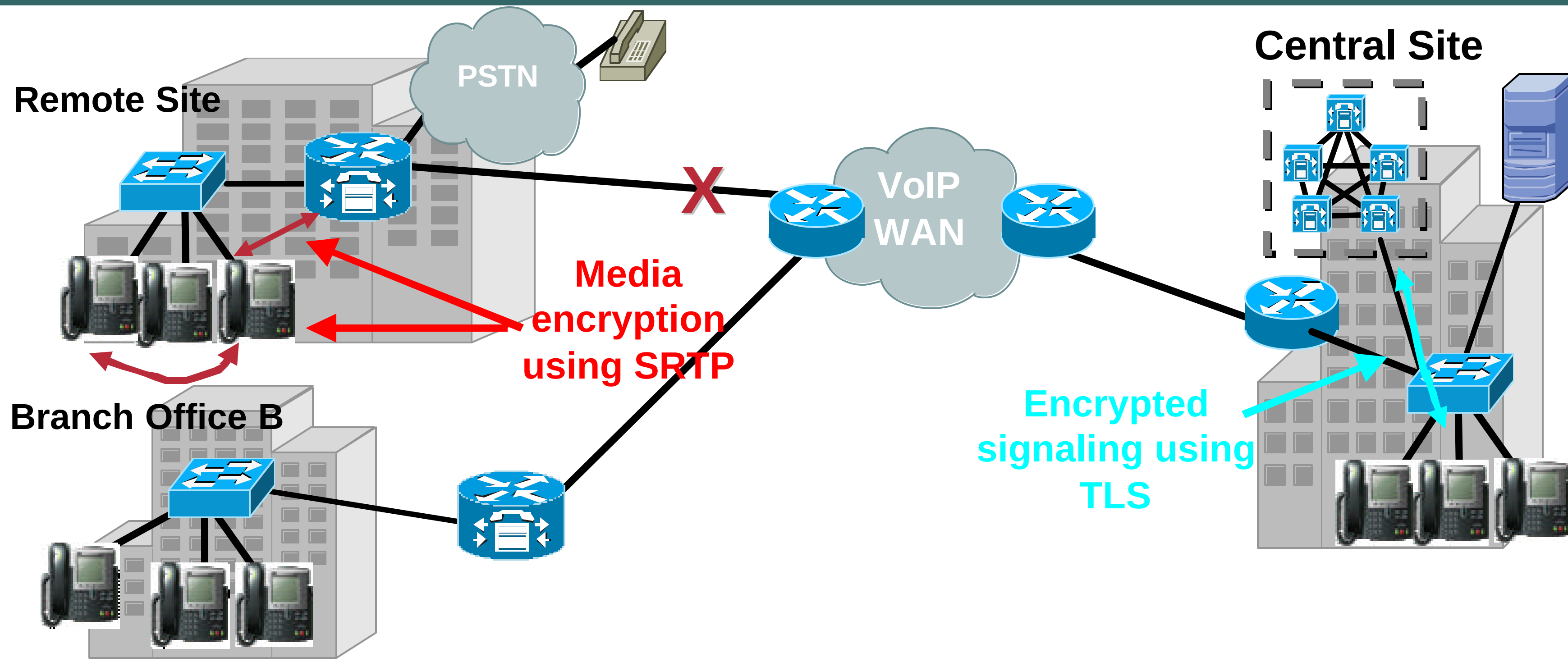
System Features:

- Re-homing of IP phones upon failure to branch router for call processing
- International language support:
- Local ext.- to-ext. calls maintained
- Maintain Ext. to PSTN calls upon failure
- Maintain existing calls upon recovery
- Support for IP and POTs phones
- DID and DOD calling
- Caller ID and ANI support
- Calling Party Name
- Call Detail Recording via Billing Server
- Inter-working with Cisco Gatekeeper
- Tone / Music on hold and on Transfer
- Alias Lists - route calls meant for central site target to a selected local destination
- Transfer to central voicemail system - Call Fwd NA to Unity with Personal Greeting
- Class of Restriction

Voicemail Features:

- Support with Cisco Unity Express on site
- Integration with Centralized Unity VM/UM

Secure SRST Support



- IP phone calls in SRST mode remain secure
- Calls are authenticated and encrypted
- Secure lock icon on IP phone gives visual confirmation to user
- Supported on IOS MGCP Gateways with PVDM2, NM-HDV2 and NM-HD modules. Support for H.323 available planned.
- Available with CCM 4.1(2) and 12.3(14)T March 2005

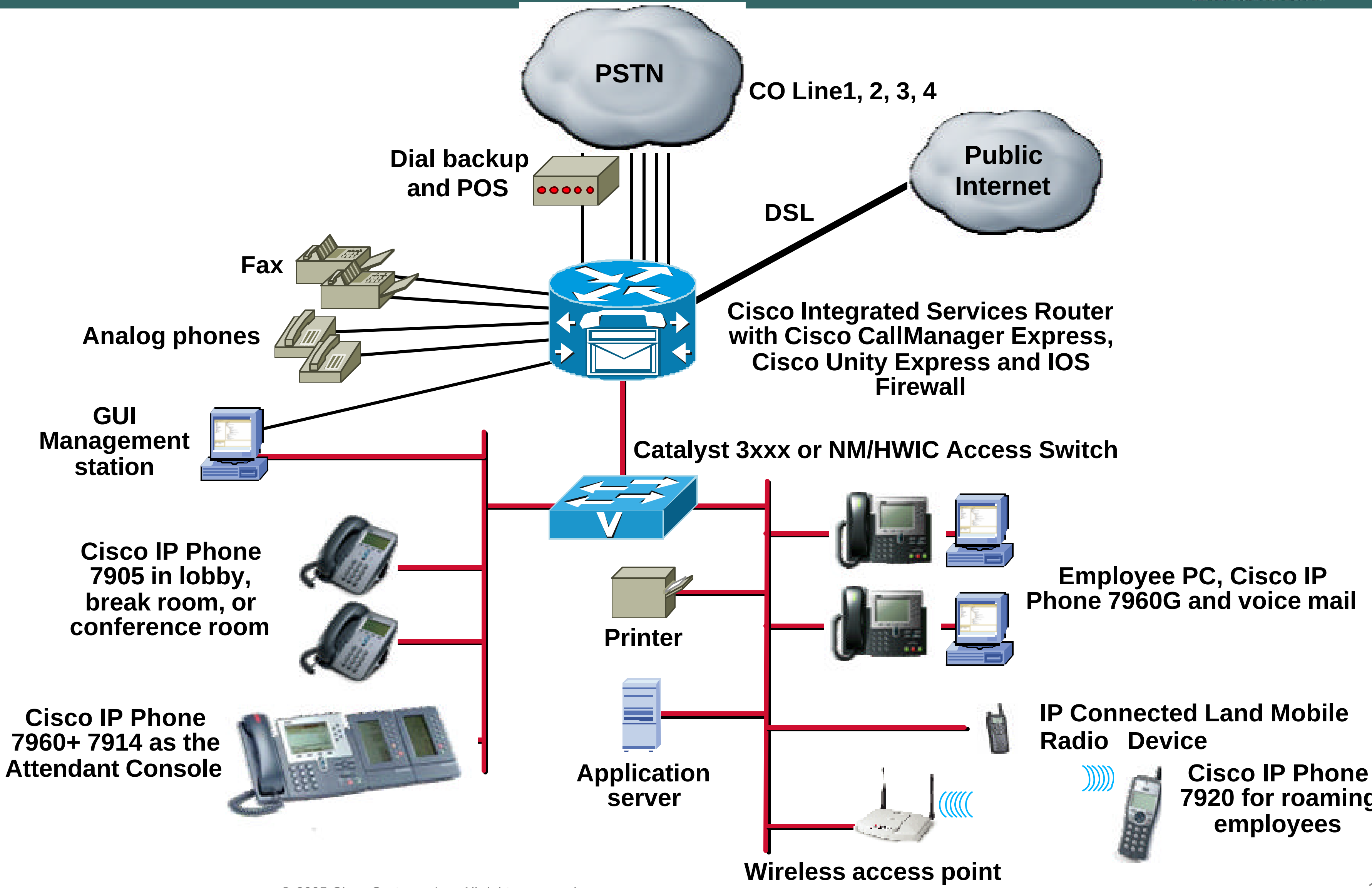
CallManager Express – What is it?

Cisco.com

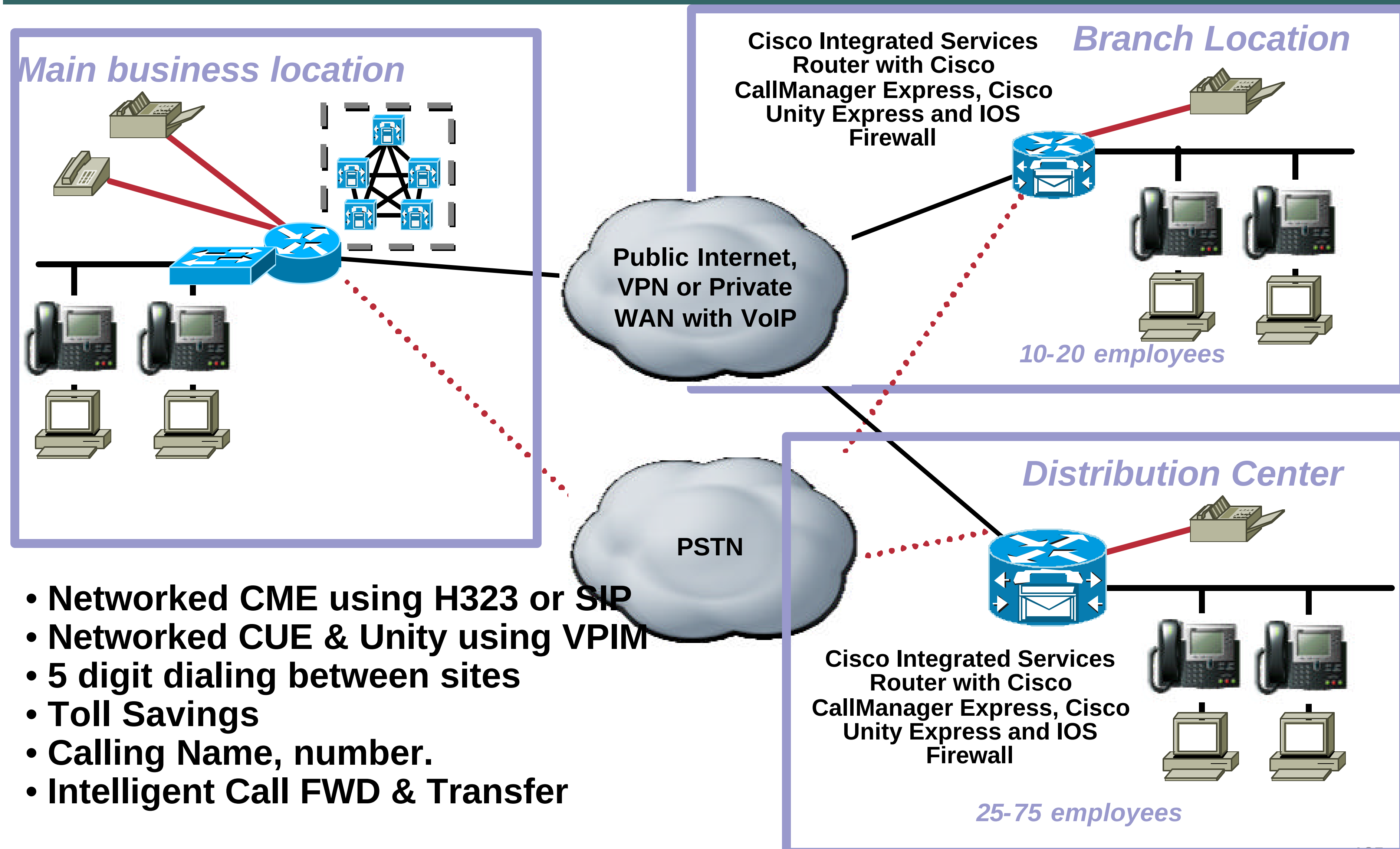
- **Configurable IP PBX or IP Key System functionality for 240 station market**
- **Primary Telephony Solution for small office or branch**
- **Many features (far more than SRST, some features even not supported on Call Manager yet)**
- **Provides Robust Networking Across Sites (H323 or SIP) – 5 digit dial, Toll Savings**
- **Voicemail Support with Cisco Unity Express (Spanish planned**
- **Unified Messaging support with Cisco Unity**
- **Integrated GUI for day two system administration**
- **Number of phones supported determined by platform:**

  24 – 17xx, 2801; 36 – 2811/2621/2611; 48 – 2821/2651; 96 - 2851; 144/192 – 3725/3745; 168/240 - 3825/3845

IP Communications Express Application: Small Standalone Office Deployment

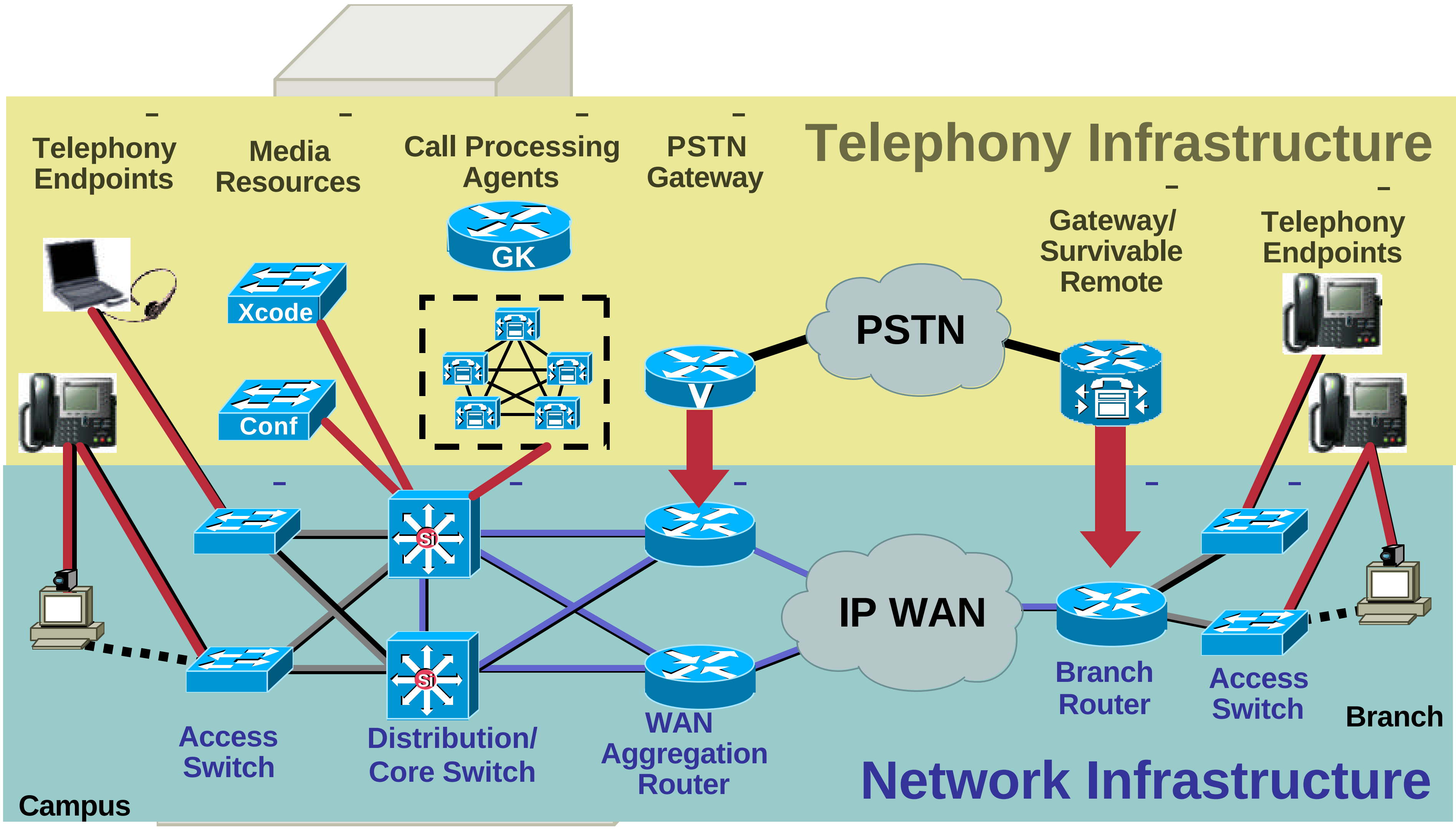


IP Communications Express Application: Distributed Enterprise Branch Office



- Networked CME using H323 or SIP
- Networked CUE & Unity using VPIM
- 5 digit dialing between sites
- Toll Savings
- Calling Name, number.
- Intelligent Call FWD & Transfer

What We Have Built So Far

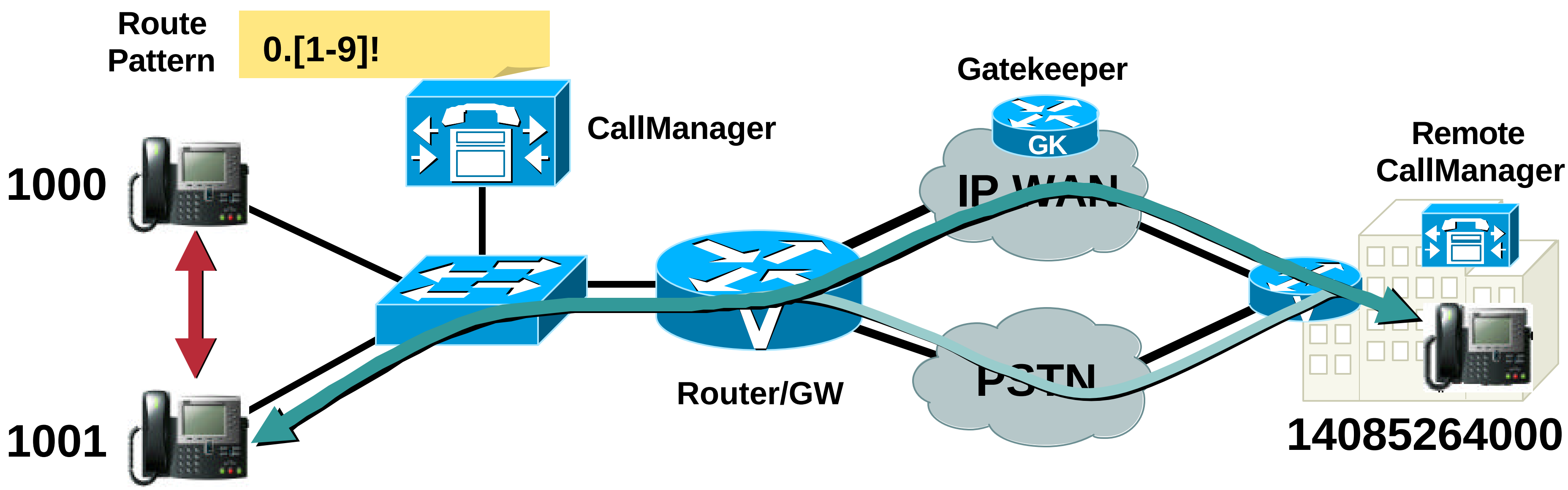


Telephony Infrastructure Agenda (2/2)

- Call Admission Control
- Survivable Remote Site Telephony
- Call Manager Express
- Dial Plan
- Voice Mail
- Security
- Video Telephony
- Management
- LDAP Directories

Dial Plan
The “IP Routing” of IP Telephony

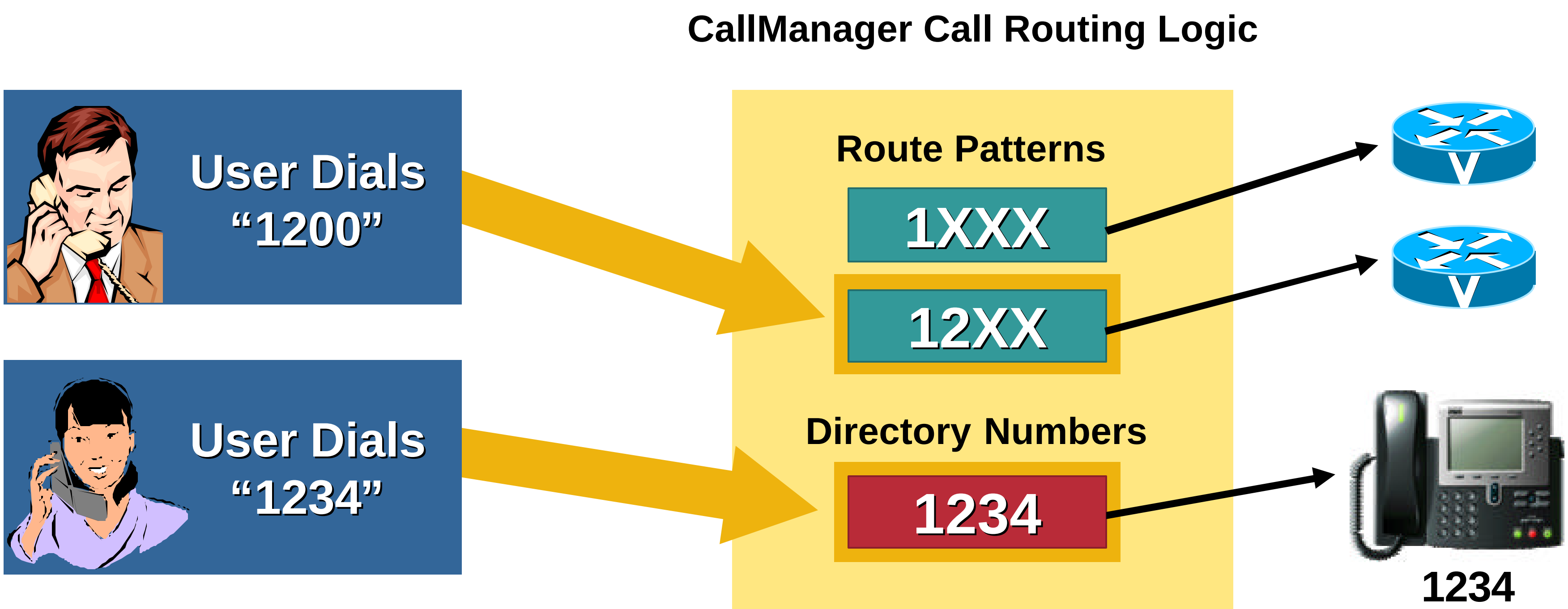
Cisco.com



CallManager Routes Two Basic Call Types:

- On-Cluster Calls—Destination Directory Number (DN) is registered with CallManager
- Off-Cluster Calls —External route patterns must be configured on CallManager

Dial Plan
CallManager Call Routing Logic



- CallManager matches the most specific pattern (longest-match logic)
- An IP phone directory number is a special case of route pattern that matches a single number

Dial Plan Agenda

- Defining External Routes
- Building Classes of Service
- Distributed Call Processing Deployments
- Centralized Call Processing Deployments
- Tail-End Hop-Off (TEHO)

Defining External Routes
External Route Elements in CallManager

Cisco.com

Route Pattern

- Matches dialed number for external calls
- Performs digit manipulation (optional)
- Points to a route list for routing

Route List

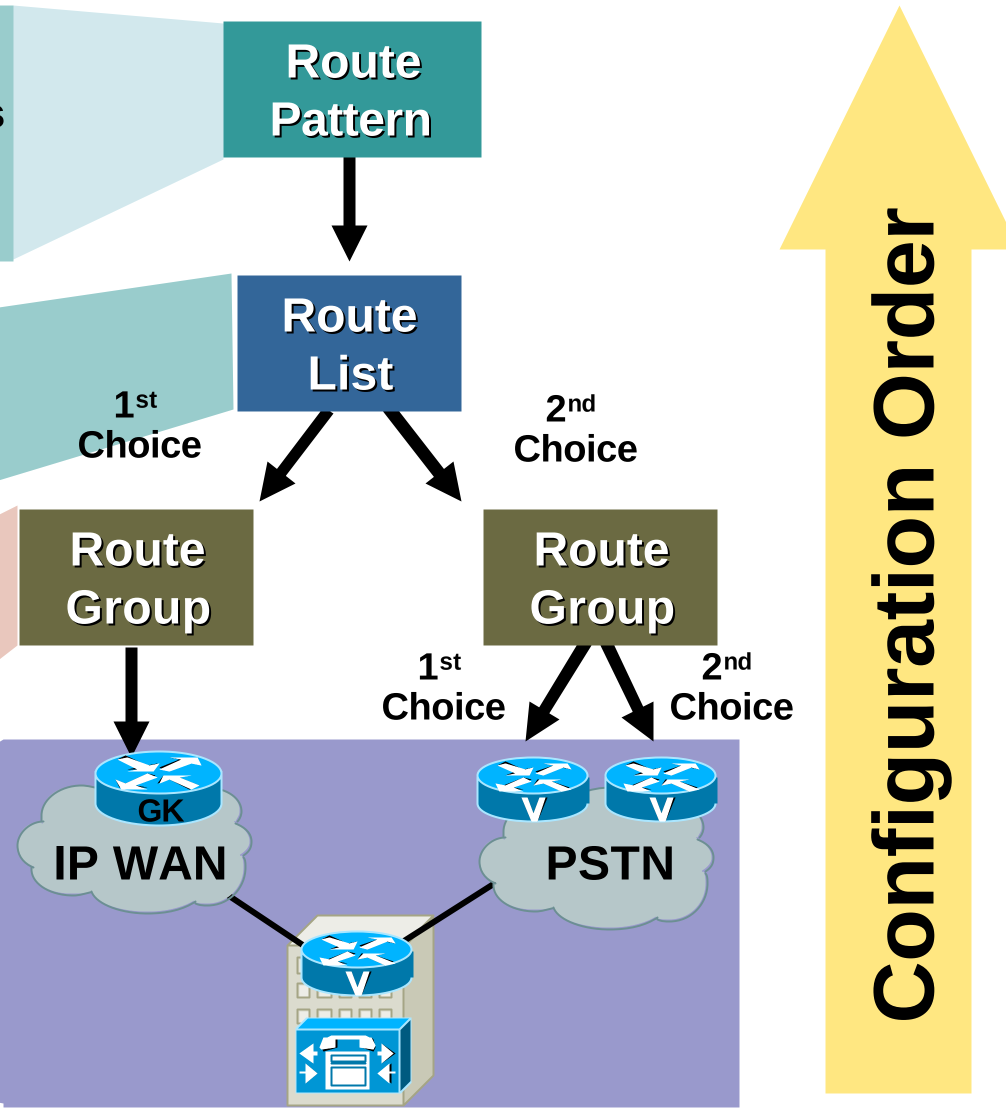
- Chooses path for call routing
- Points to prioritized route groups

Route Group

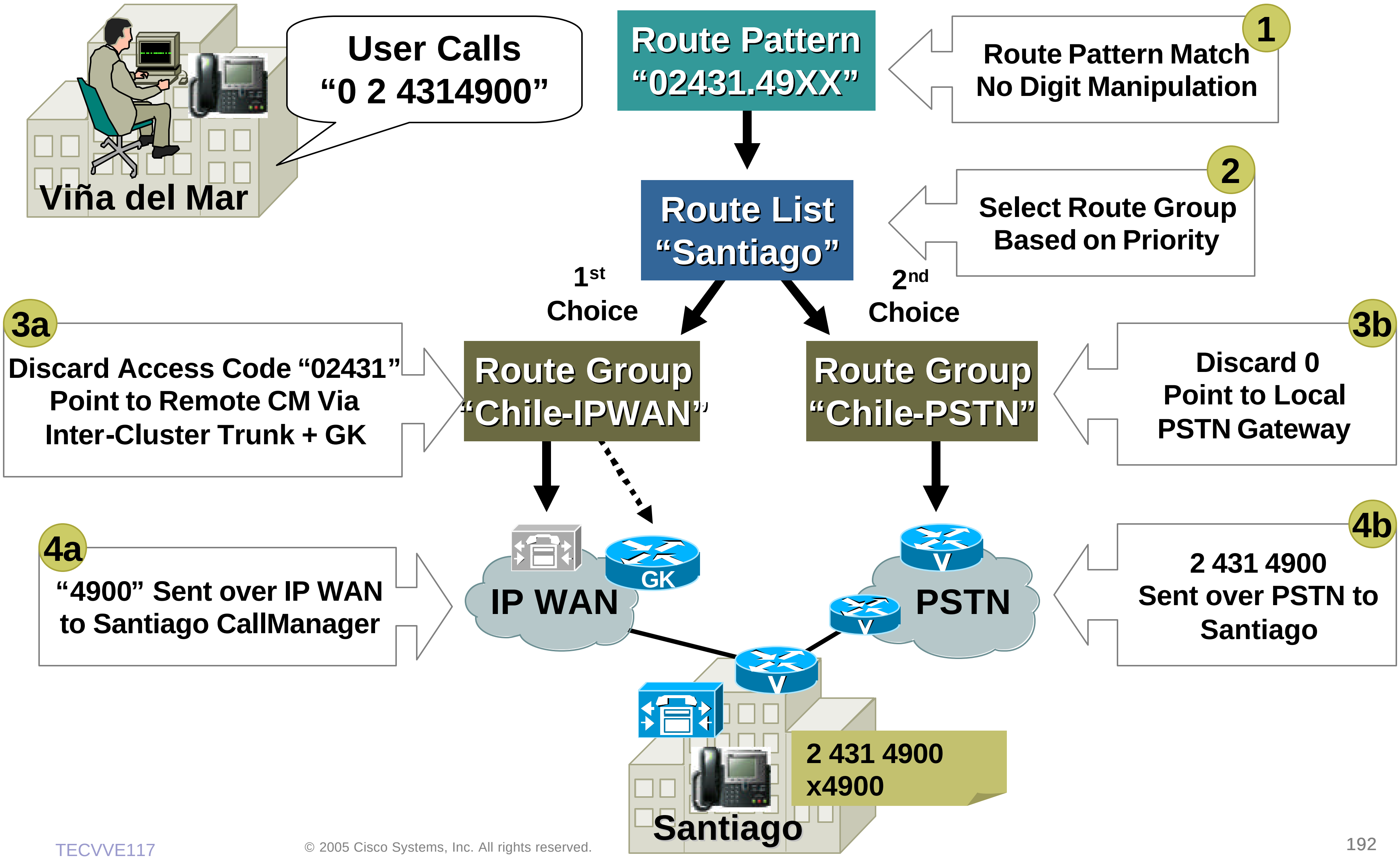
- Performs digit manipulation
- Points to the actual devices

Devices

- Gateways (H.323, MGCP)
- Gatekeeper
- Inter-Cluster Trunk (remote CM)



Defining External Routes
Example: PHL to SJ



Defining External Routes
Commonly Used Route Pattern Wildcards

Cisco.com

Delimiter (Does Not Match Any Digits)—Used for Discarding

Range of Digits (between 1 and 9)

Single Digit between 0 and 9

0 . [1-9] XXXXXX

One or More Occurrences of Digits between 0 and 9

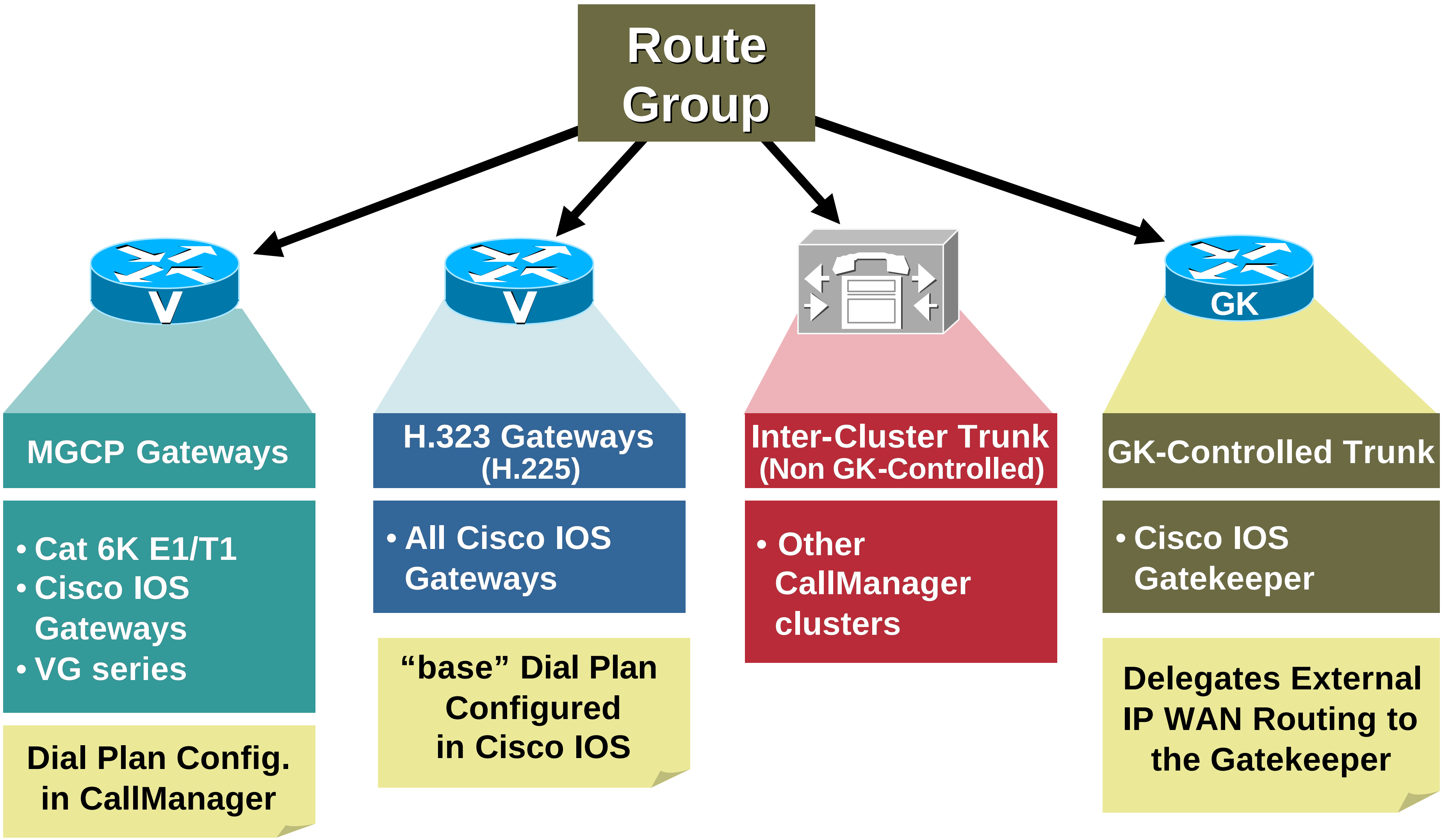
The “#” Digit—Used to Avoid Inter-Digit Timeout

0.[1-9] ! #

0. @

A Macro that Enters the Custom Numbering Plan into CallManager (Hundreds of Individual Route Patterns) – built initially for North America requires customization for Global – not recommended

Defining External Routes
Route Group Device Types

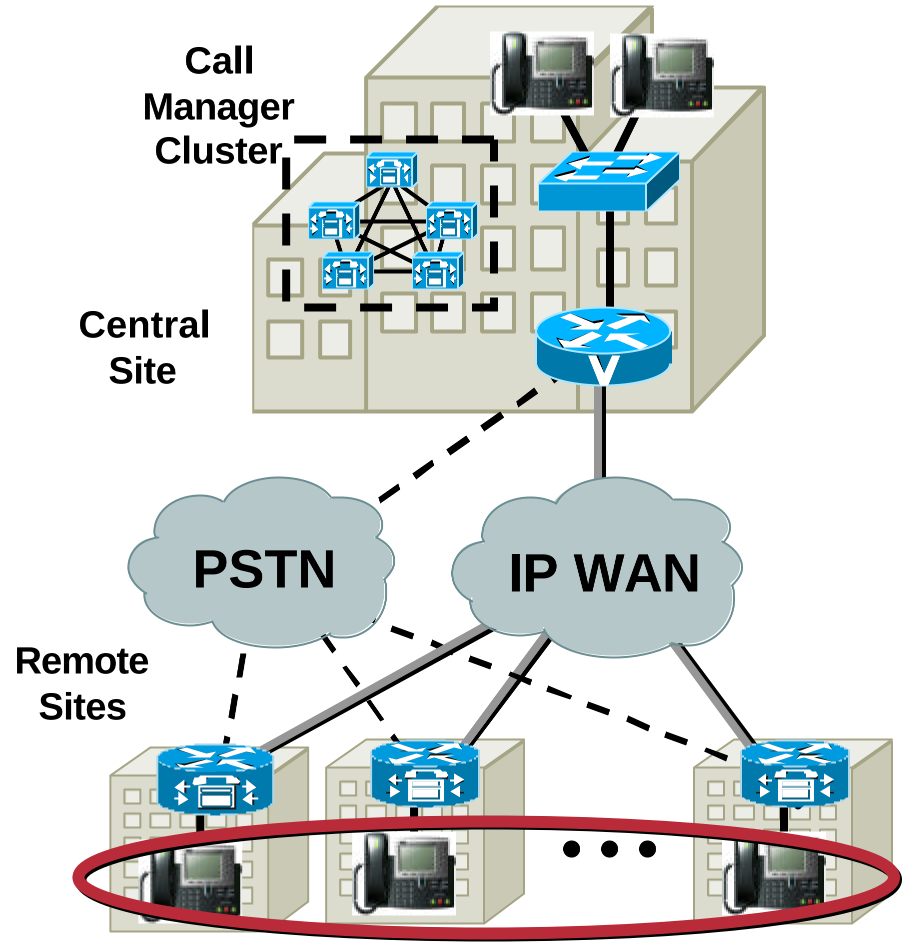


Dial Plan Agenda

- Defining External Routes
- Building Classes of Service
- Distributed Call Processing Deployments
- Centralized Call Processing Deployments
- Tail-End Hop-Off (TEHO)

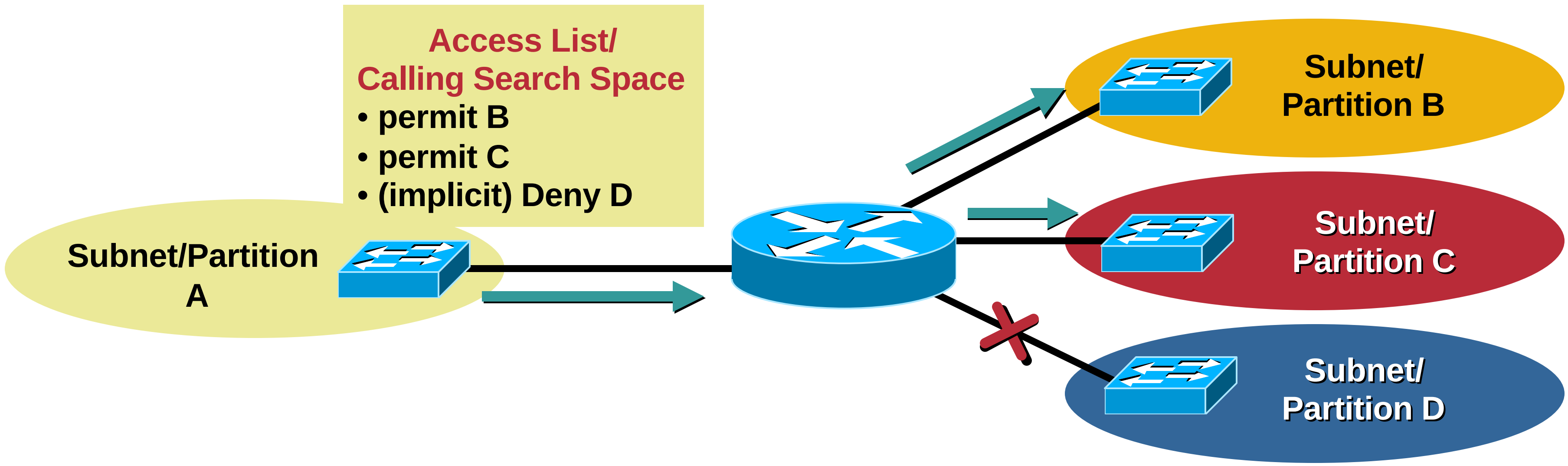
Building Classes of Service
Routing by User Class or Location

Create "Dial Plan Policy Groups" to Define Calling Restrictions



Instruct these Phones to Use Their Local Gateway for PSTN Access

Building Classes of Service
Analogy Partitions/CSS: Subnets/Access Lists



Partition— "Where You Are"

- Collects devices with similar "reachability" characteristics
- Items placed in partitions: Directory Numbers (DN), Route Patterns, Voice Mail Ports...

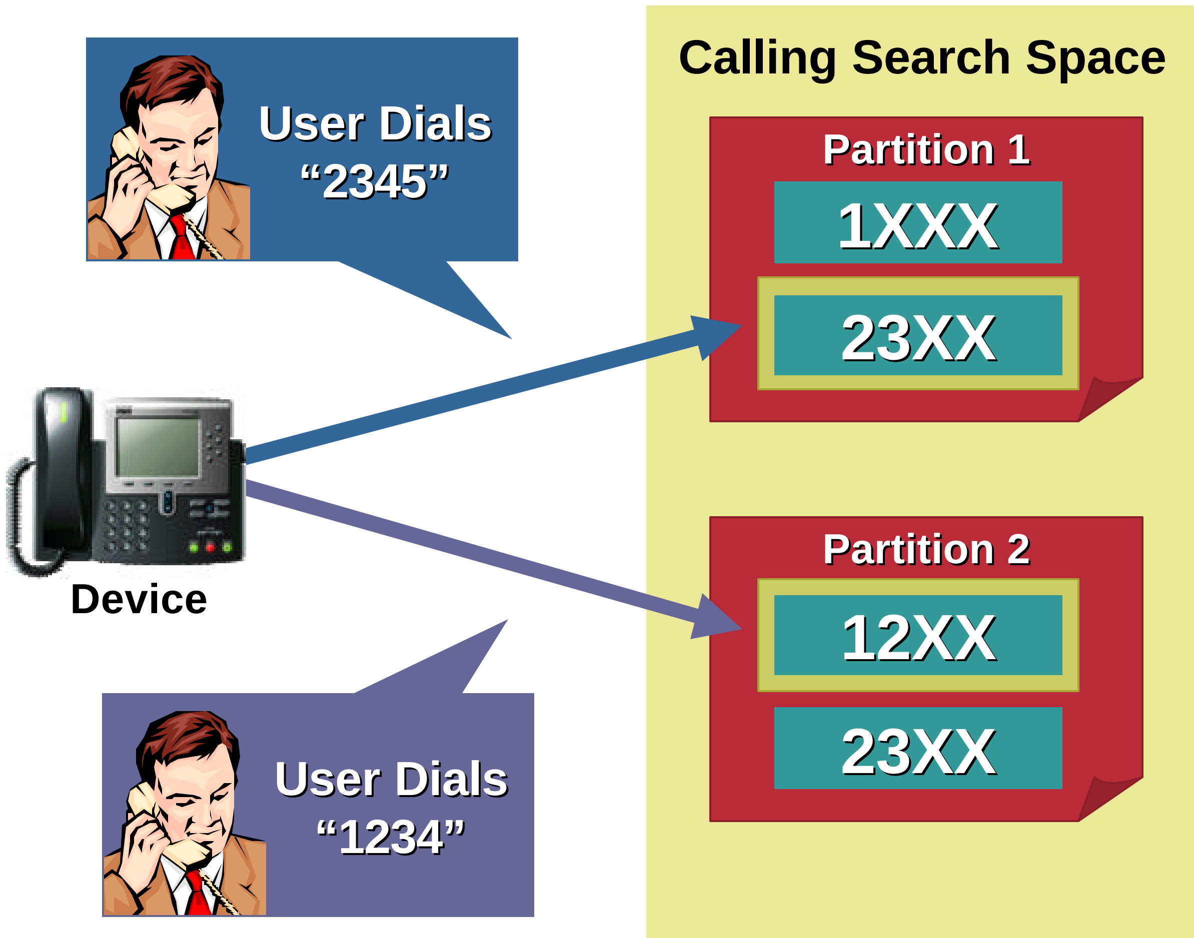
Calling Search Space— "Where You May Call"

- Set of rules to set call restrictions/permissions
- Defines which partitions a device may search to reach a dialed number
- Is assigned to IP phones, GWs

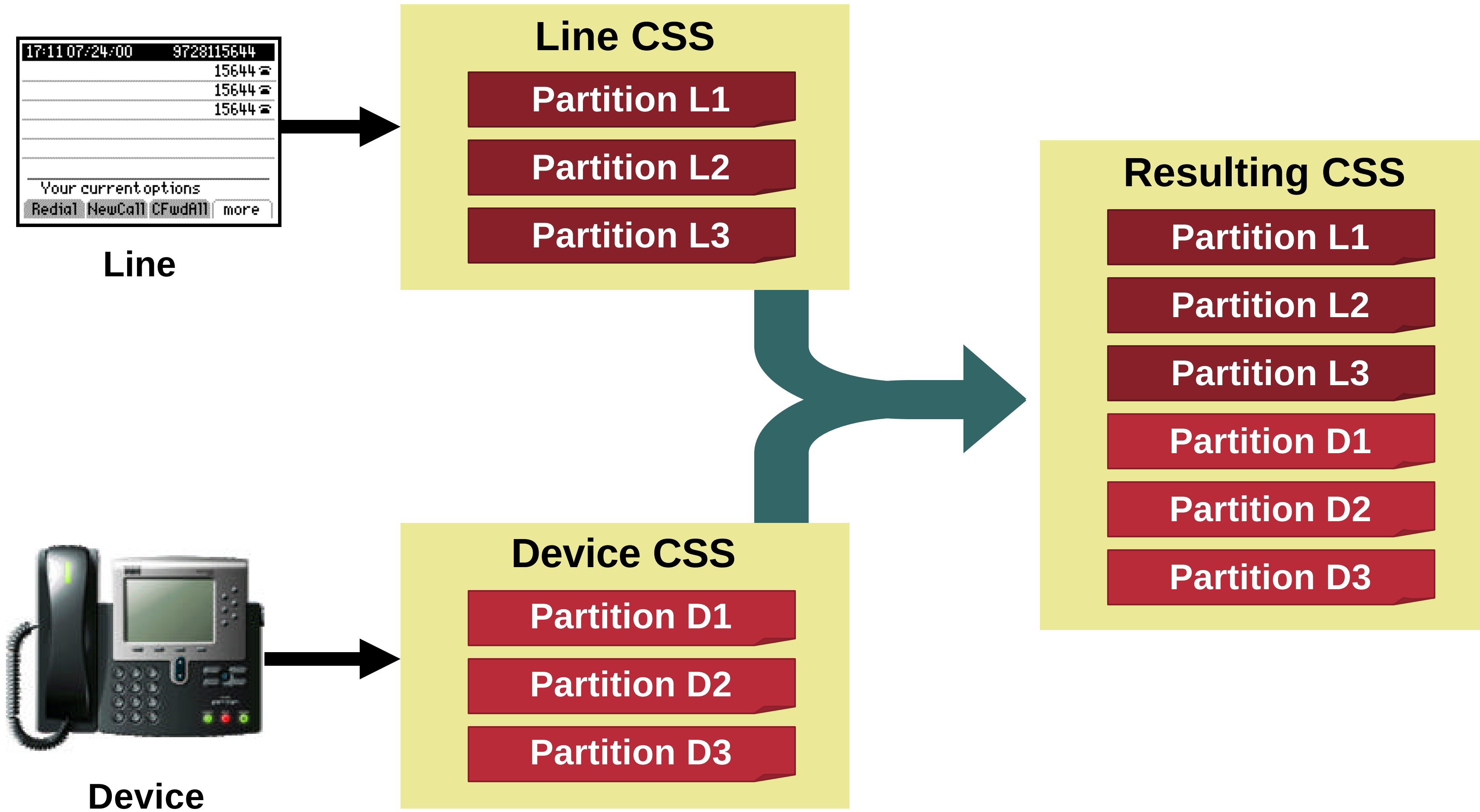
Building Classes of Service
Impact of Partition Order

Cisco.com

- **Most specific patterns are chosen irrespective of partition order**
- **Partition order is only used as a tie-breaker in case of equal matches**

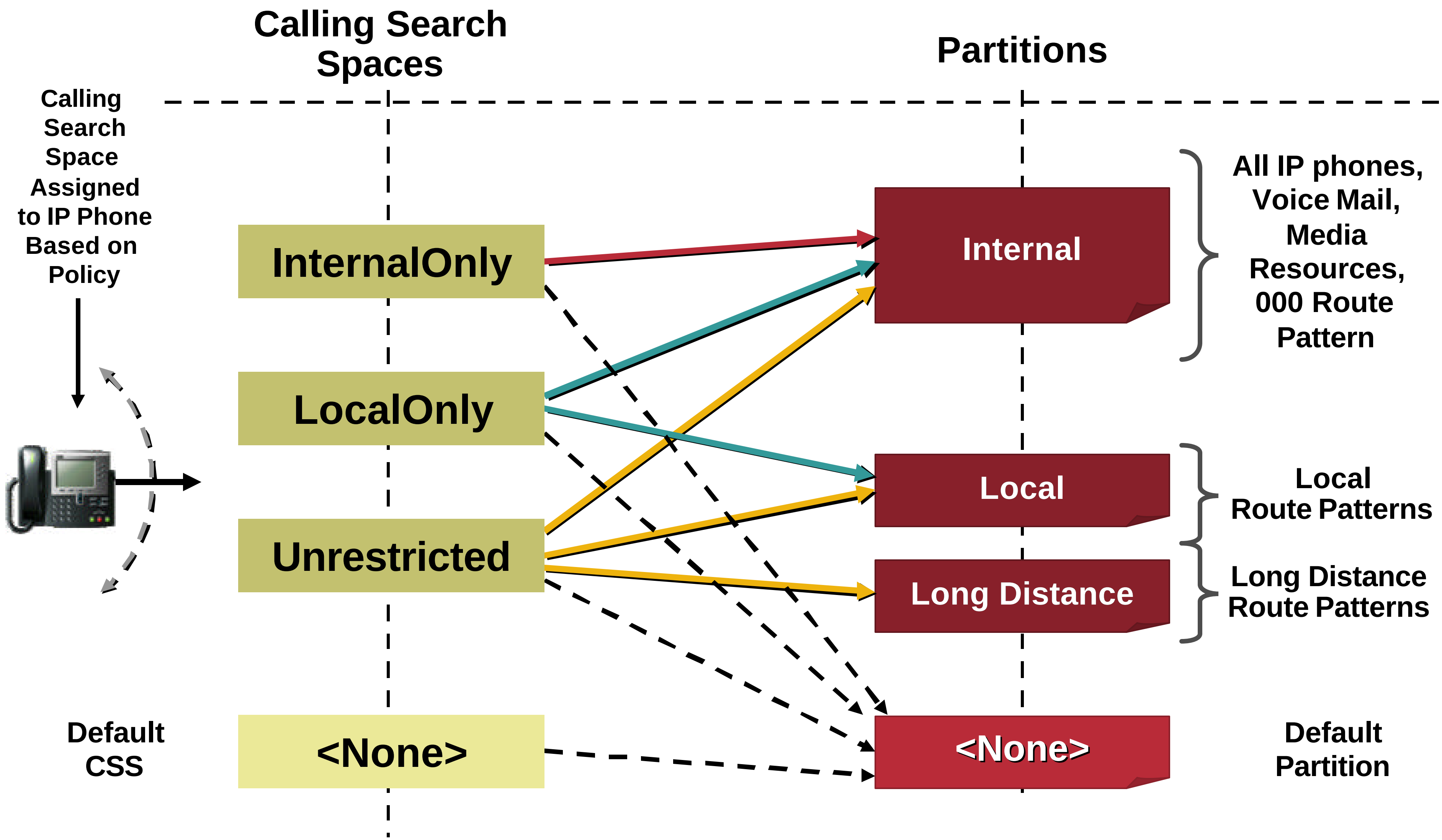


Building Classes of Service
Device-Line CSS Interaction

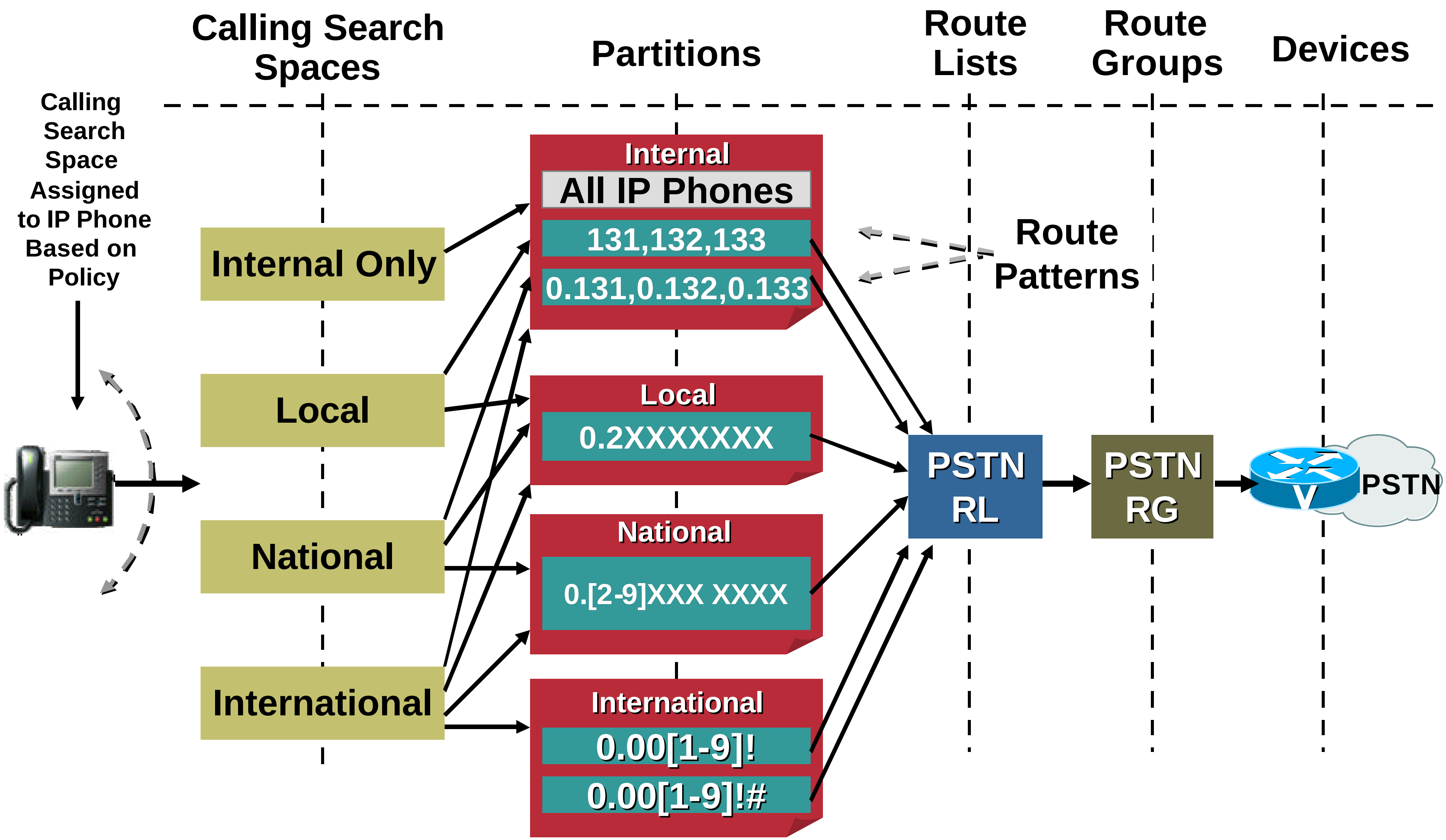


Building Classes of Service
Typical Example of Classes

Cisco.com

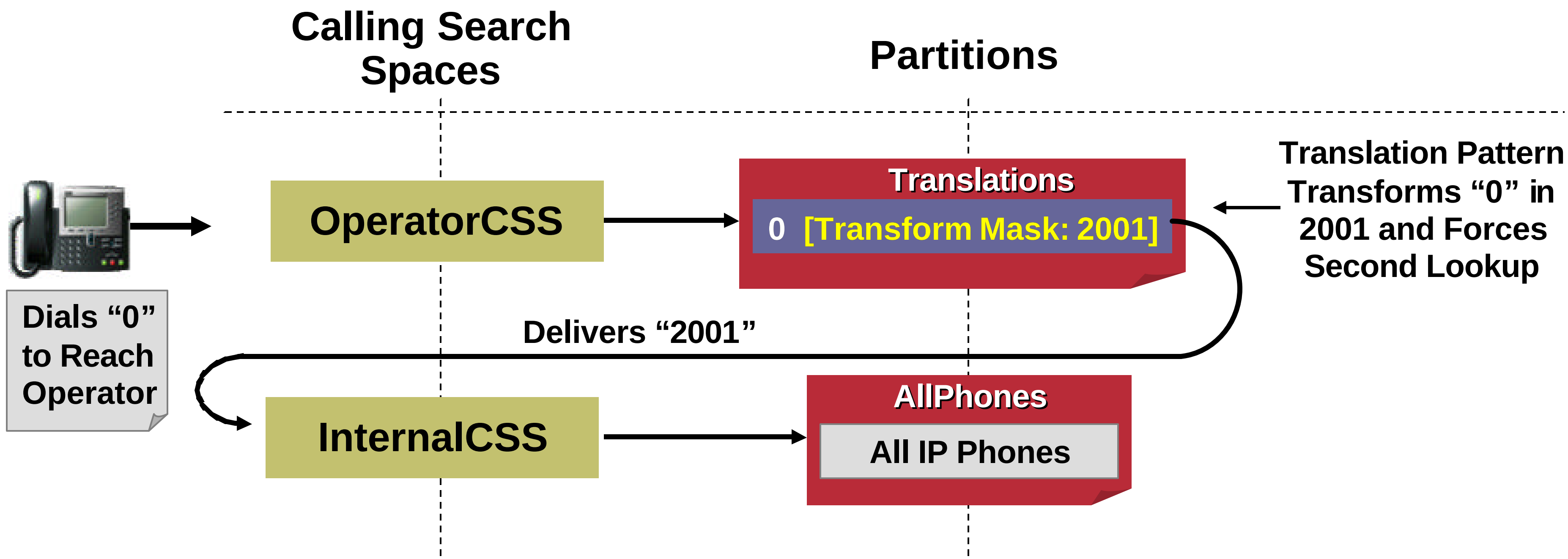


Building Classes of Service
Example of Dial Plan Composite View



Building Classes of Service
Translation Pattern Basics

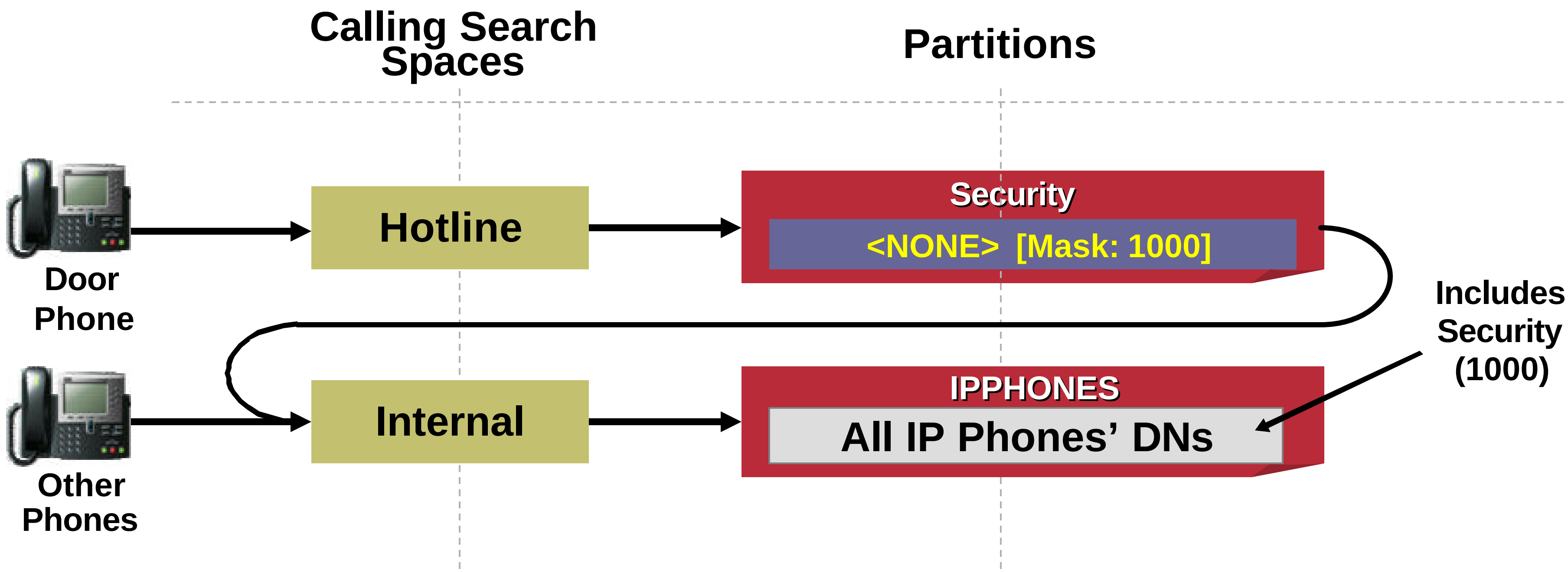
Cisco.com



- Looks like a route pattern, allows digit manipulation
- Instead of sending calls outside via a route list, forces second lookup in CallManager, using a (possibly different) calling search space

Building Classes of Service
Configuring a Security Hotline (PLAR)

Cisco.com



Create Partition SECURITY

Create HOTLINE CSS with SECURITY Partition

Create Translation Pattern Matching <NONE> , Called Party Transformation Mask Equal to 1000, CSS Set for Internal; (Contains Partition with Security Phone

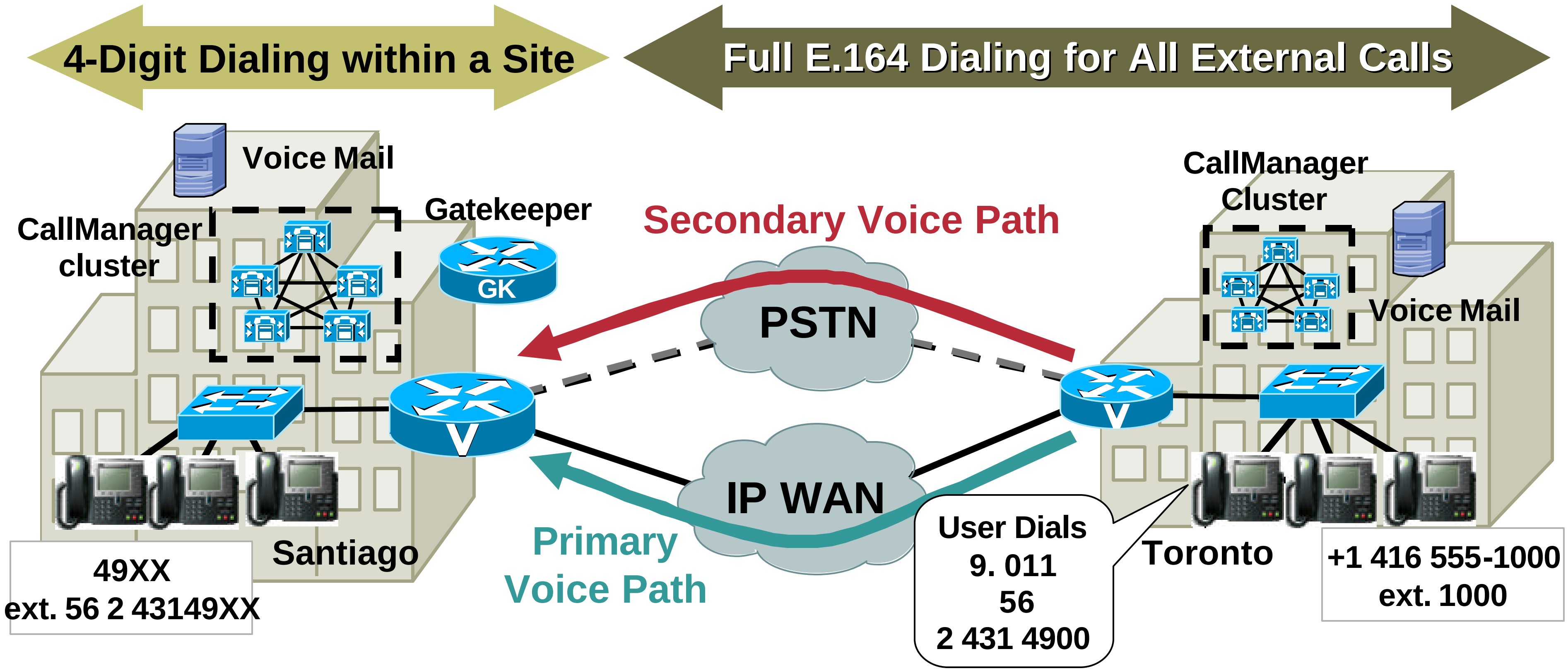
Create Door Phone with CSS set to HOTLINE

Dial Plan Agenda

- Defining External Routes
- Building Classes of Service
- Distributed Call Processing Deployments
- Centralized Call Processing Deployments
- Tail-End Hop-Off (TEHO)

Distributed Call Processing Deployments
Example of Dial Plan Requirements

Cisco.com



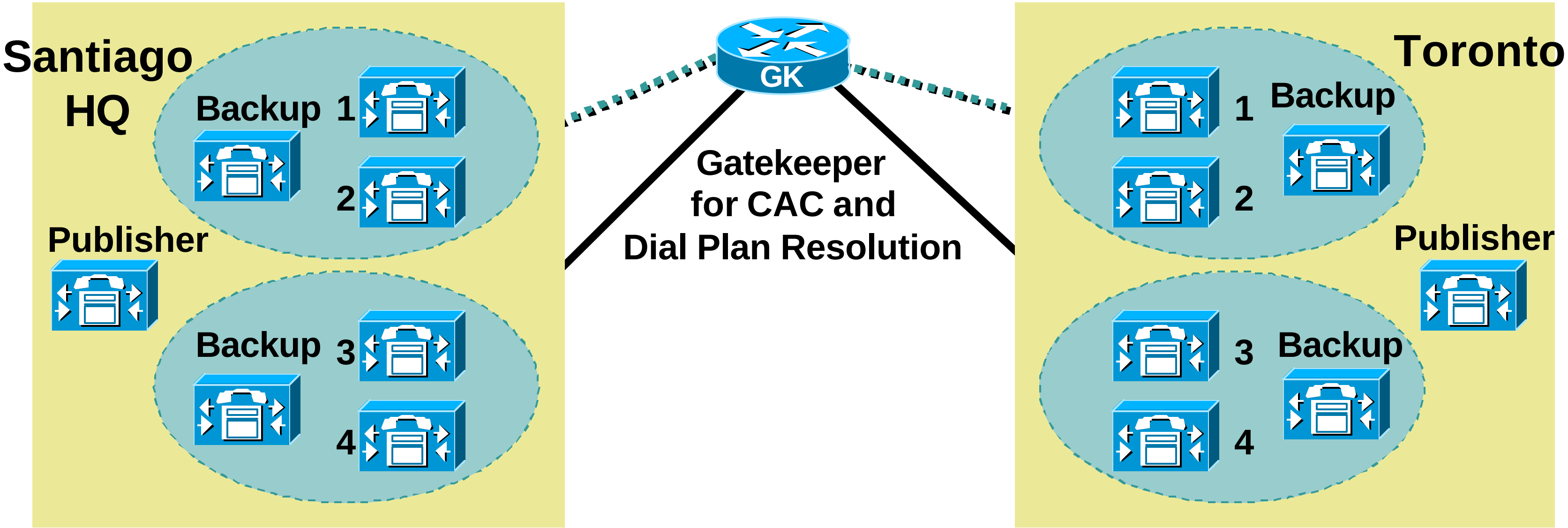
Primary Voice Path: IP WAN

- **Outgoing** (Tor cluster): strip "9.011" and deliver "56 2 4314900" to Gatekeeper
- **Incoming** (Santiago cluster): strip all but significant 4 digits

Secondary Voice Path: PSTN

- **Outgoing** (Santiago cluster): strip "0" and deliver "0014165551000" to the PSTN
- **Incoming** (Toronto cluster): strip all but significant 4 digits

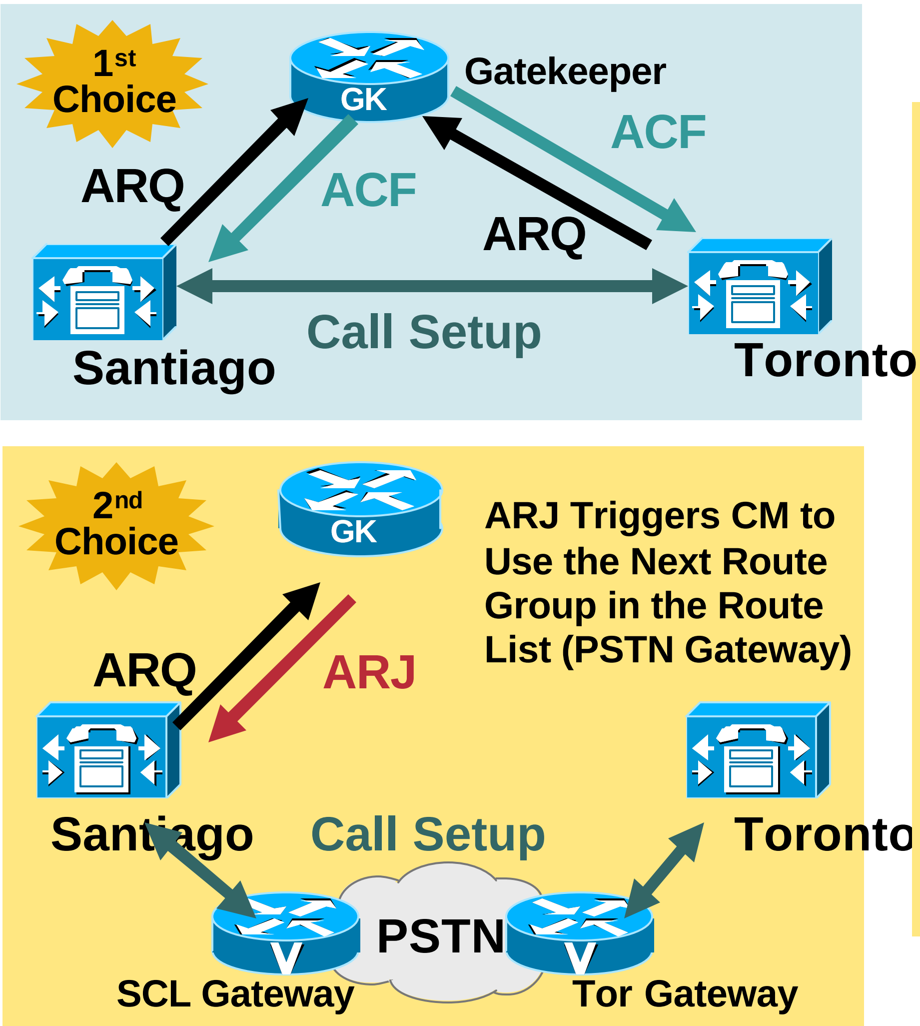
Distributed Call Processing Deployments
Gatekeeper for Dial Plan Resolution



- Gatekeeper provides call admission control in presence of multiple CallManager clusters (distributed call processing deployments)
- CallManager configured with "anonymous device"—Uses gatekeeper also to resolve E.164 addresses
- Lower dial plan administration, highly scalable distributed model

Distributed Call Processing Deployments
Automatic Reroute with Gatekeeper

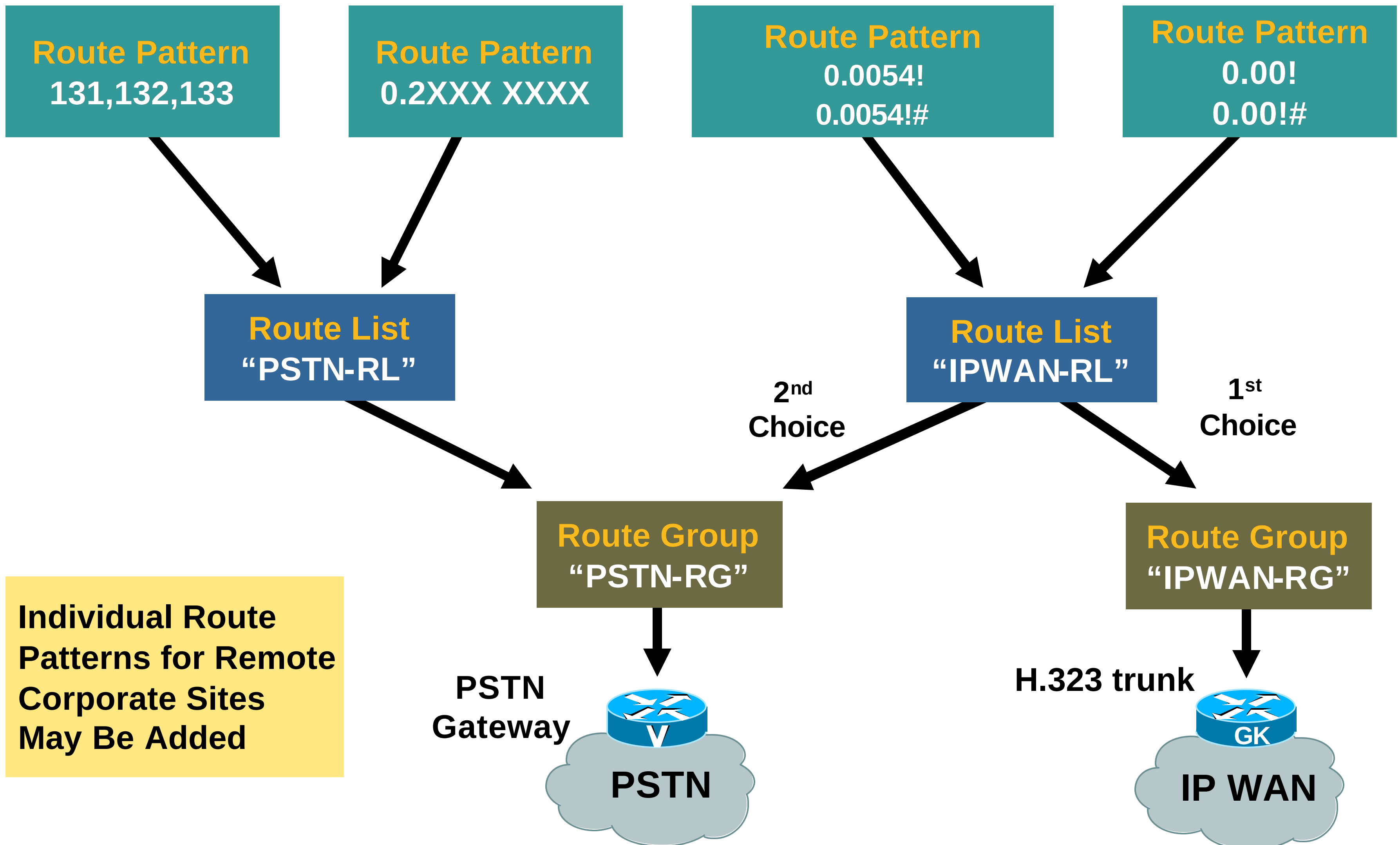
Cisco.com




```
gatekeeper
  zone local SCL cisco.com
  zone local TOR cisco.com
  zone prefix SCL 56243149..
  zone prefix SCL 56243148...
 [...]

  zone prefix TOR 14165551...
  zone prefix TOR 151955568..
 [...]

  gw-type-prefix 1#* default-
                     technology
  bandwidth interzone zone SCL 480
```

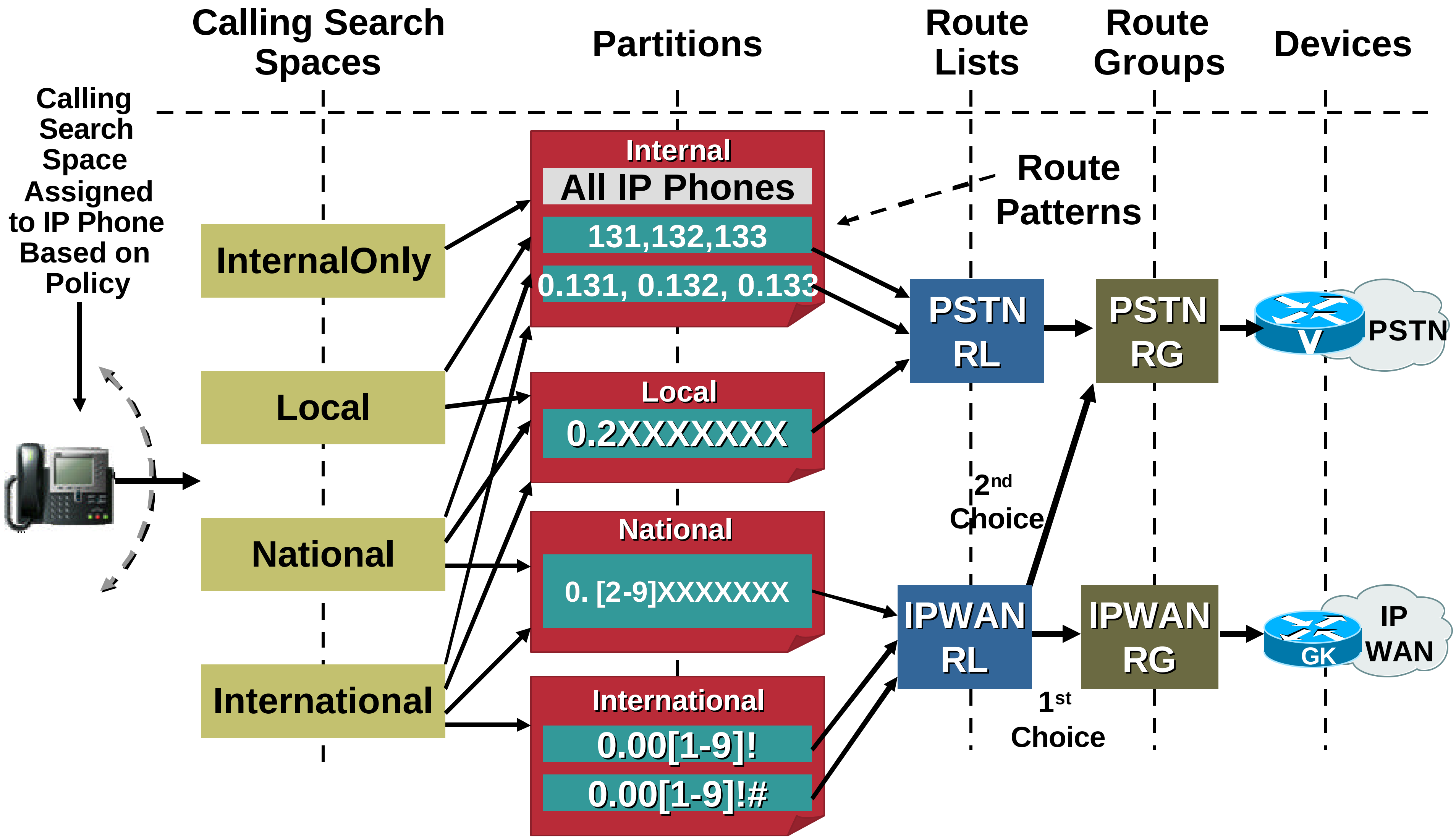
Distributed Call Processing Deployments
Typical Route Patterns

Cisco.com



Distributed Call Processing Deployments
Composite Dial Plan View

Cisco.com

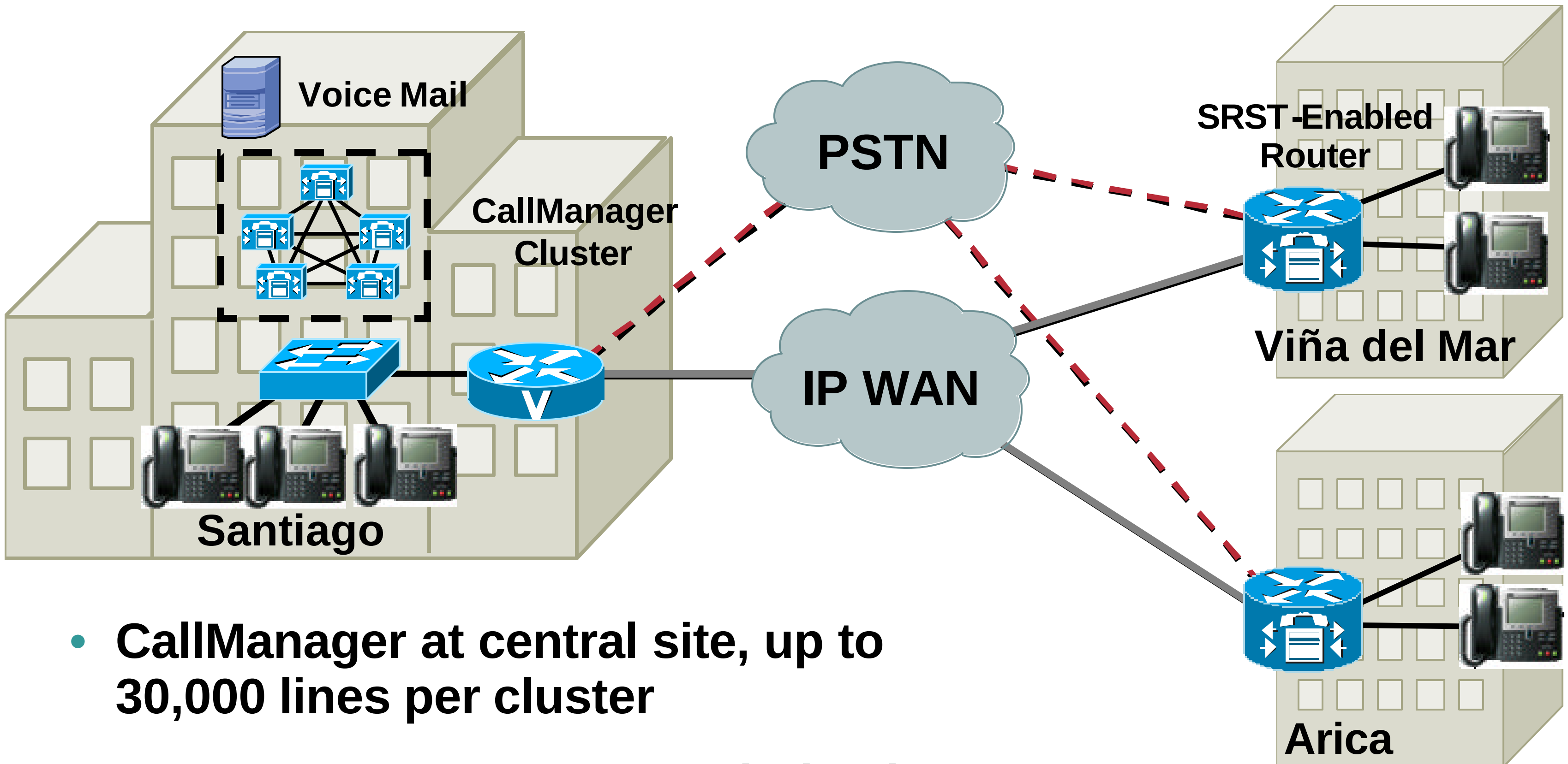


Dial Plan Agenda

- Defining External Routes
- Building Classes of Service
- Distributed Call Processing Deployments
- Centralized Call Processing Deployments
- Tail-End Hop-Off (TEHO)

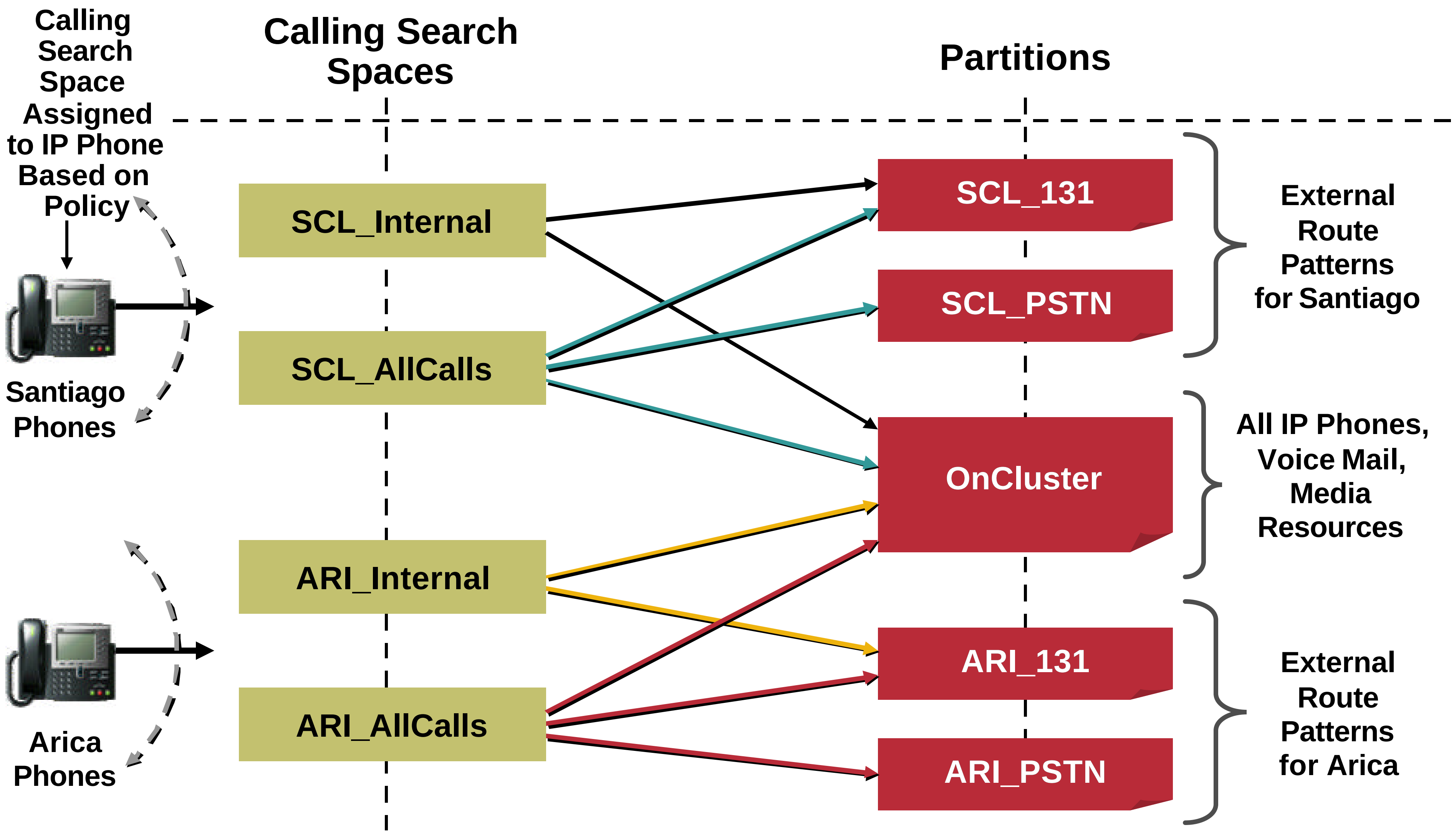
Centralized Call Processing Deployments
Dial Plan Assumptions

Cisco.com



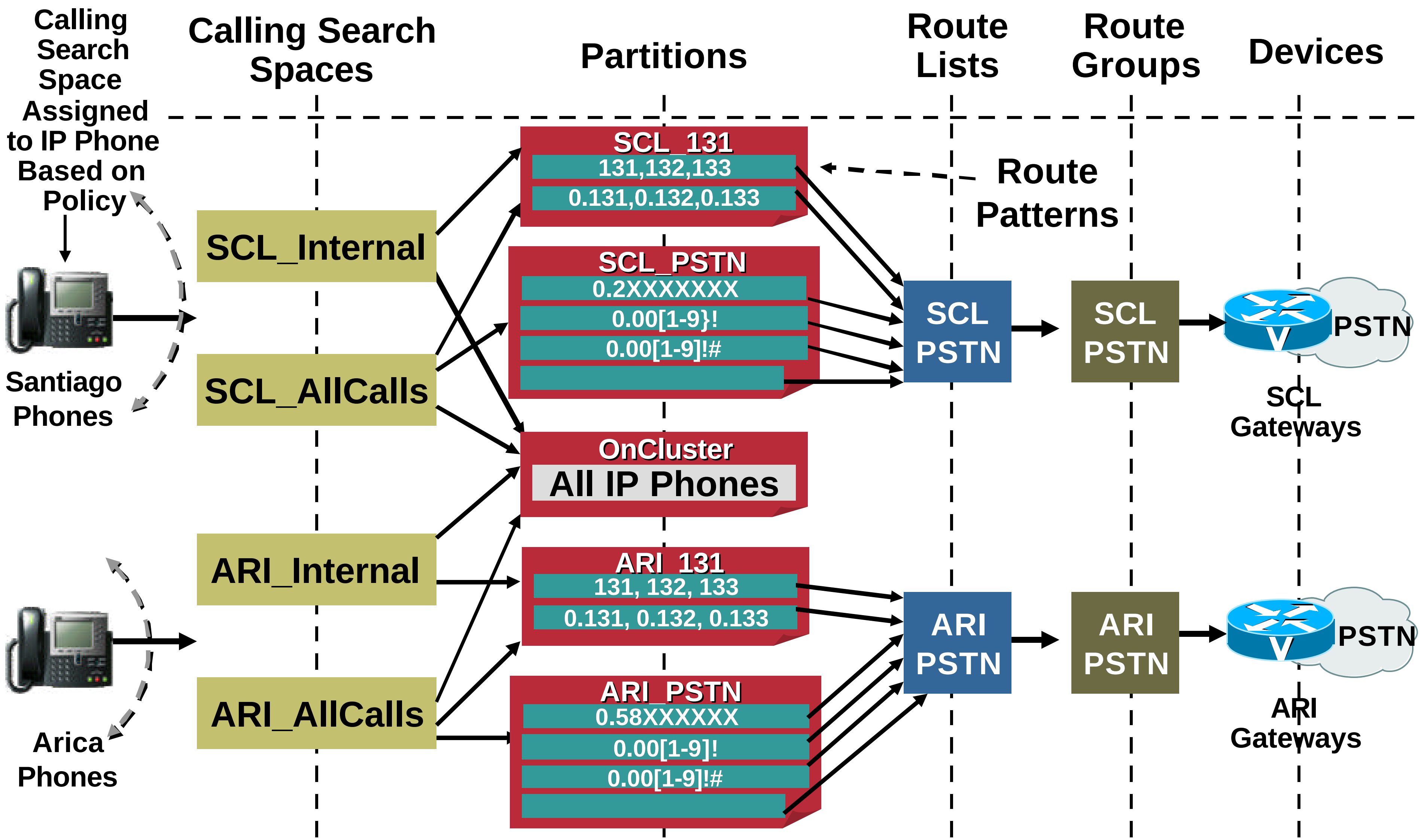
- CallManager at central site, up to 30,000 lines per cluster
- Common PSTN access code (“0”)
- 131,132,133 and PSTN calls use each site’s local gateway
- Non-overlapping extensions

Centralized Call Processing Deployments
View of Partitions/Calling Search Spaces



Centralized Call Processing Deployments
Composite Dial Plan View

Cisco.com



Dial Plan

General Recommendations

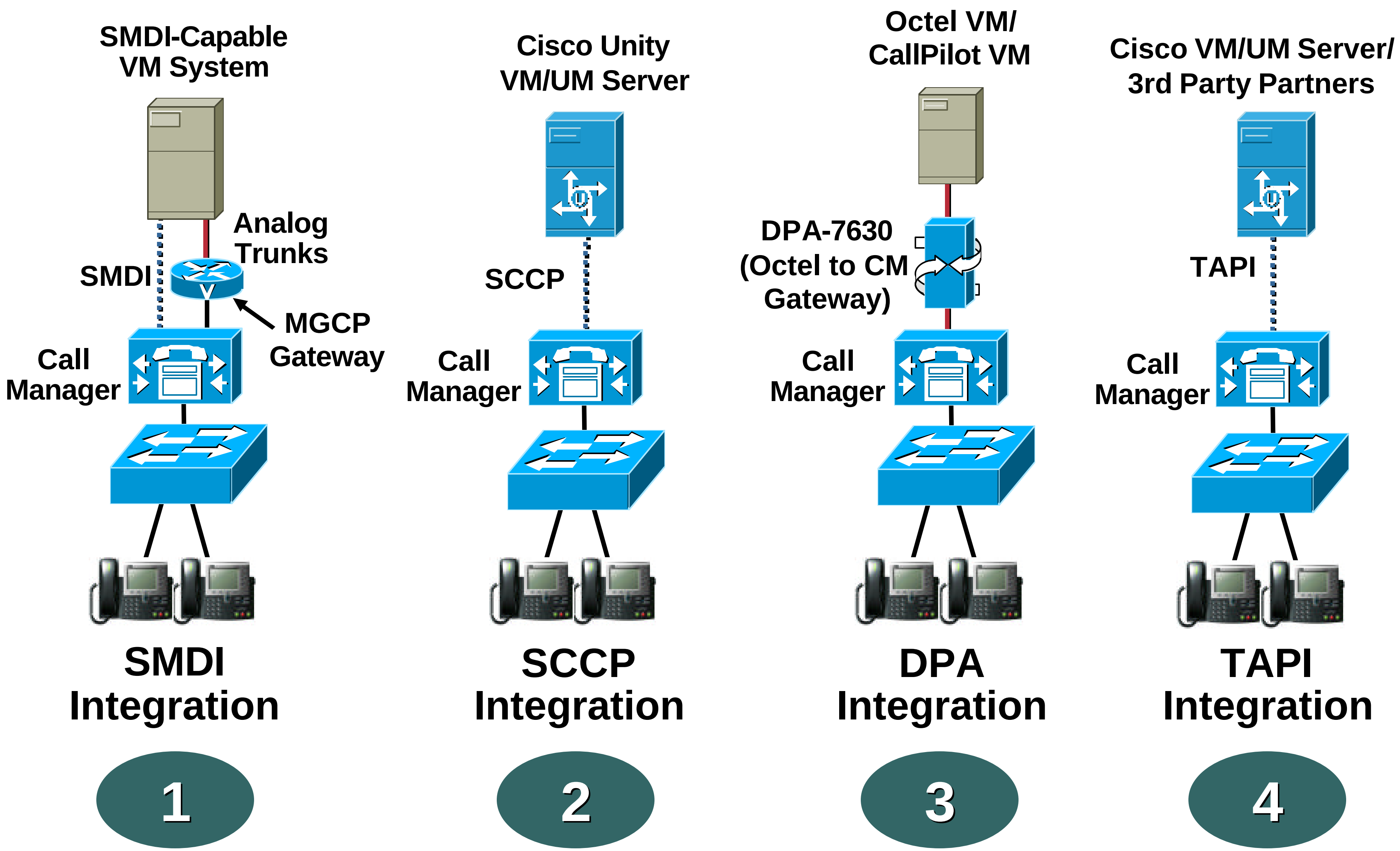
- Keep it simple
- Plan for future growth
- Use a gatekeeper-controlled trunk when more than two CallManager clusters are present
- Normalize DNs to the full E.164 when using gatekeeper for dial plan resolution

Telephony Infrastructure Agenda (2/2)

- Call Admission Control
- Survivable Remote Site Telephony
- Call Manager Express
- Dial Plan
- Voice Mail Integration
- Security
- Video Telephony
- Management
- LDAP Directories

Voice Mail Integration
Integration Methods

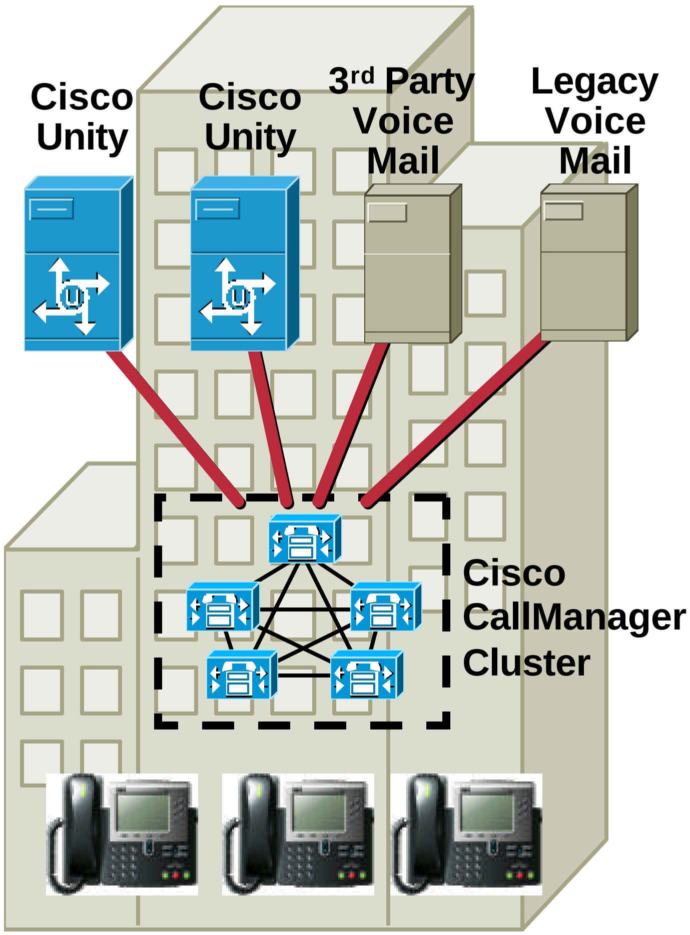
Cisco.com



Voice Mail Integration General Considerations

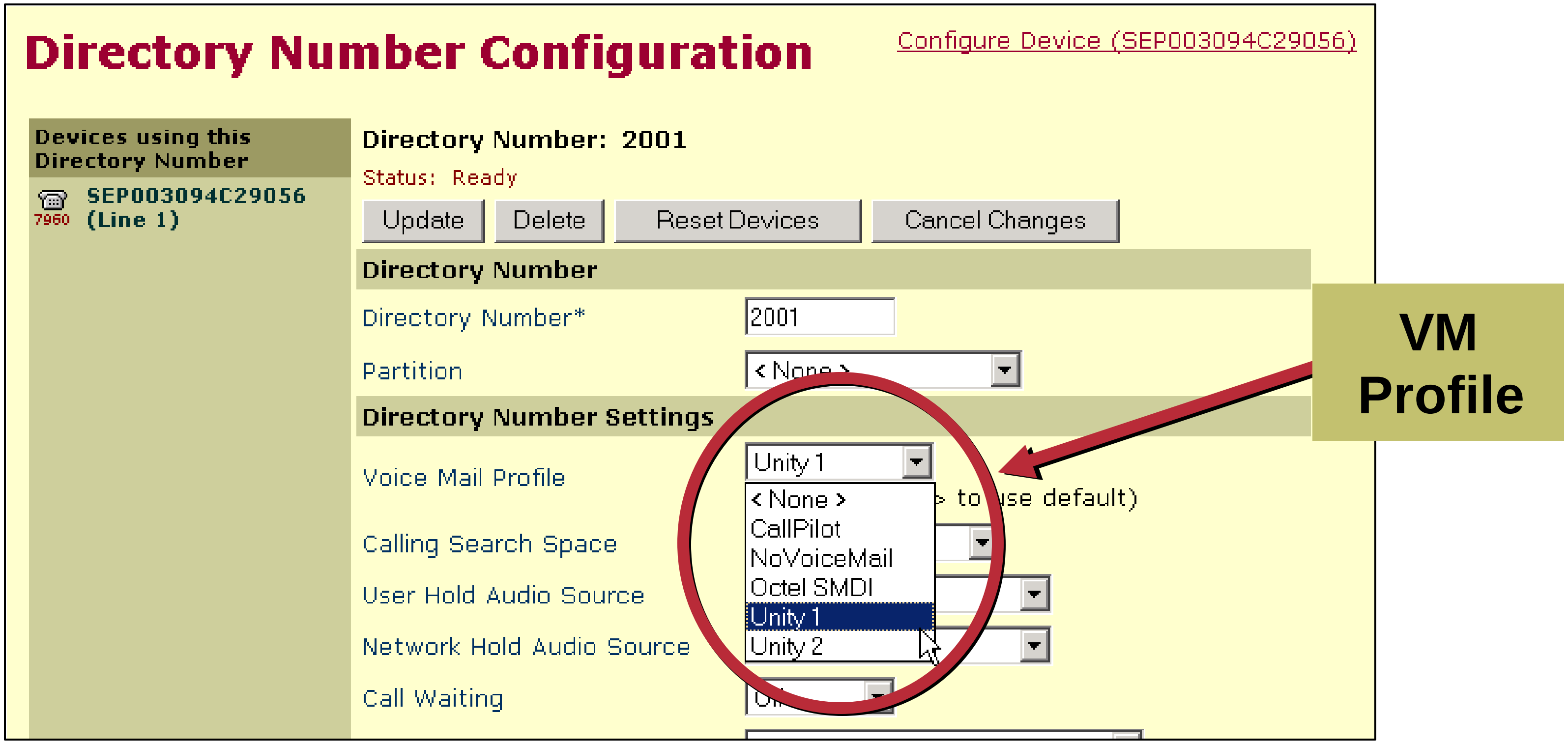
Cisco.com

- **Support for multiple voice mail systems per CallManager cluster (up to 4)**
- **Voice mail system selection configurable per DN**
- **Message Waiting Indicator (MWI) light behavior configurable per IP phone**
- **Simplified VM integration for multi-tenant deployments**



Voice Mail Integration
Each DN Can Use a Different VM Profile

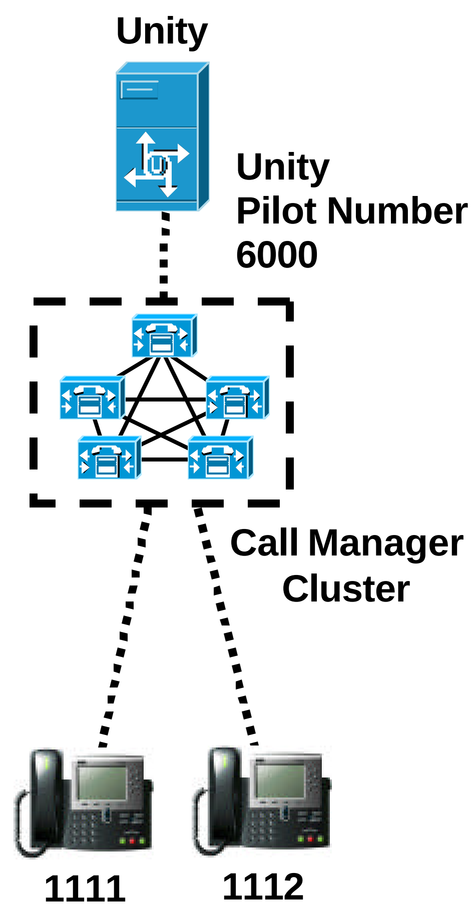
Cisco.com



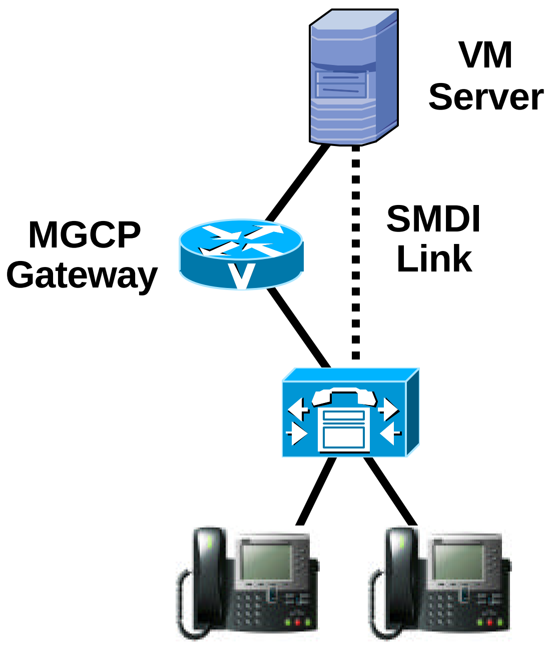
- **Directly pressing “Messages” button calls primary DN’s voice mail pilot number**
- **Pressing line appearance button and then “Messages” button calls that line’s voice mail pilot**

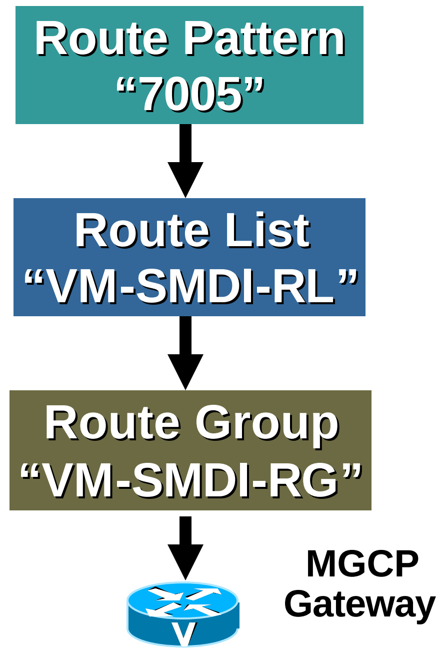
Voice Mail Integration
SCCP (Unity)

- **Unity integrates with Call Manager via SCCP (like an IP phone)**
- **Assign DN and define VM ports using the "Voice mail port wizard" on CallManager**
- **"Messages" button on IP phones dials VM pilot number (according to VM profile assigned to each DN)**
- **Multiple MWI On/Off DNs can be configured in the same CallManager cluster**



Voice Mail Integration
SMDI Integration



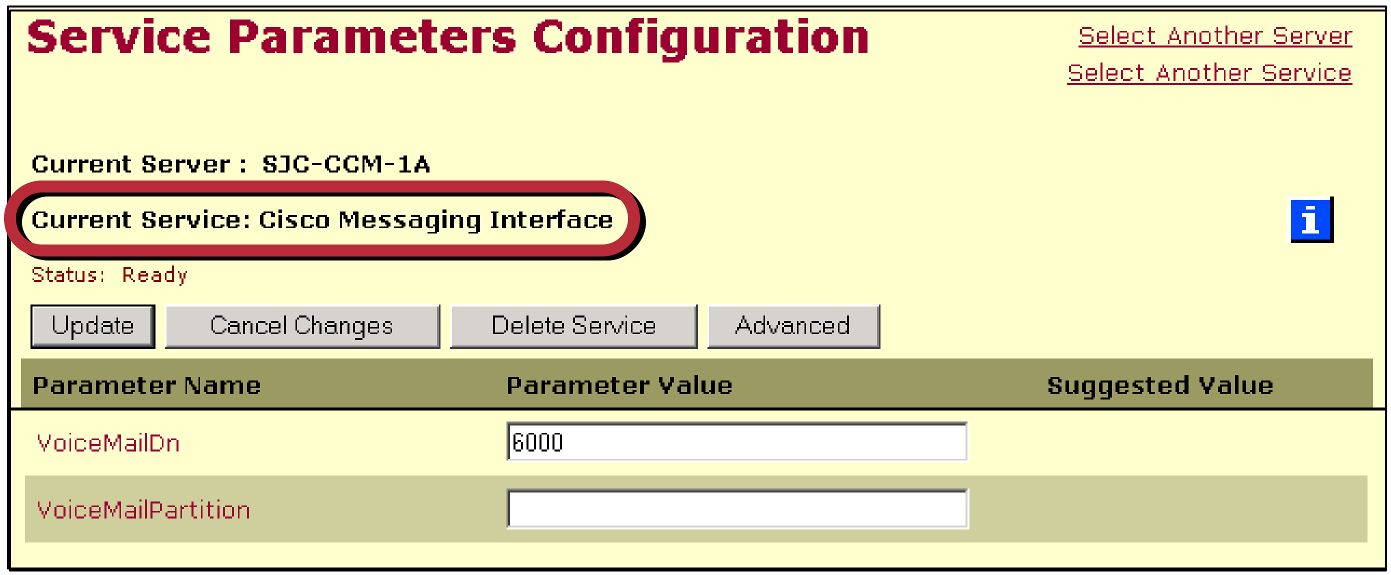


- **Need to create a VM Route Pattern/List/Group**
- **VM system is connected through an MGCP gateway and an SMDI serial link to CallManager**
- **Note: MGCP gateway is required (no H.323), since CallManager needs to be in control of the VM ports**

Voice Mail Integration
SMDI: Binding Voice Mail DN to SMDI Port

Cisco.com

Service:
CMI



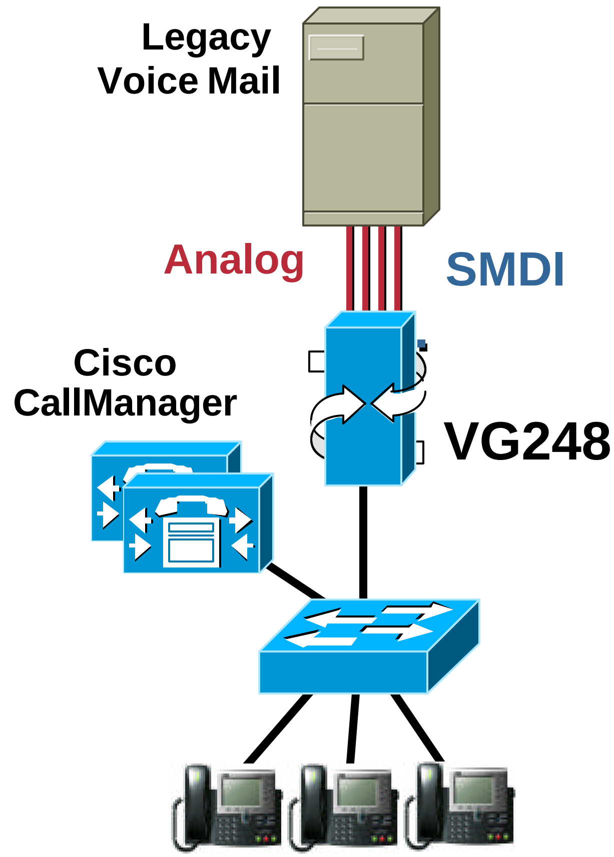
- **Defines the voice mail Route Pattern DN and the partition it resides in**
- **Calls directed to this DN trigger SMDI messaging on the SMDI port**
- **Defining this parameter "awakens" SMDI on CallManager**

Voice Mail Integration

Cisco.com

SMDI—Note on VG248 Integration

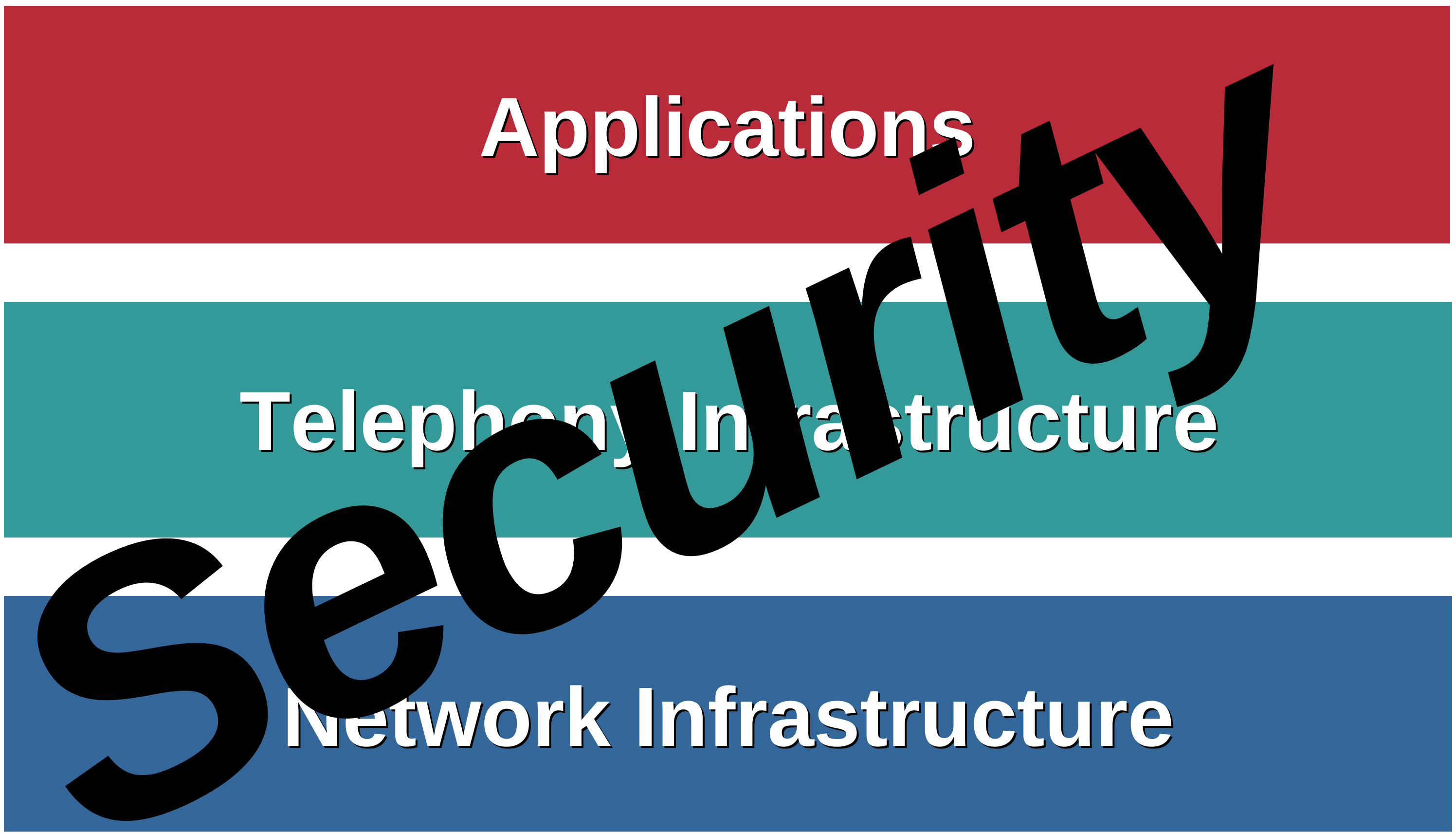
- **VG248 analog phone gateway has SMDI port for voice mail integration**
- **SMDI configured on VG248**
- **From CallManager dial plan perspective, this is equivalent to integration via SCCP**



Telephony Infrastructure Agenda (2/2)

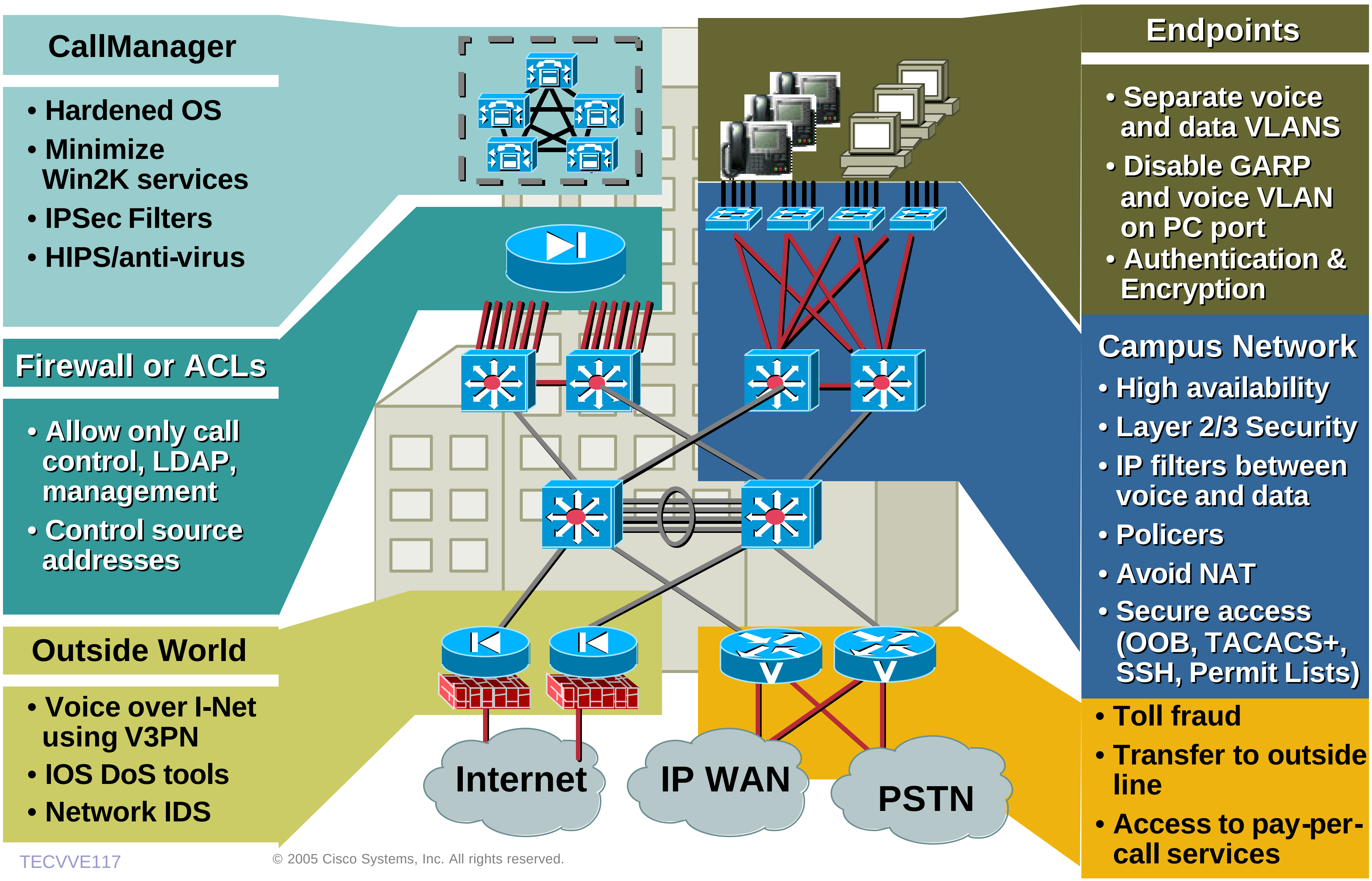
- Call Admission Control
- Survivable Remote Site Telephony
- Call Manager Express
- Dial Plan
- Voice Mail Integration
- Security
- Video Telephony
- Management
- LDAP Directories

Overall Impact



IP Telephony Security: Build It in Layers

Cisco.com



NetworkWorldFusion 05/24/04 Declares Cisco IPT is Secure !!!

"Cisco's maximum-security VoIP configuration earned our most Secure rating. Our attack team couldn't disrupt, or even disturb, Cisco's phone operations after three days of trying."

VoIP security rating scale

Overall rating	Maximum impact that assault team could achieve
Secure	No perceptible disruption to voice service.
Resistant	Only minor and/or temporary disturbance(s).
Vulnerable	Phone service affecting many phone users could be disrupted for a protracted period, via a sophisticated or coordinated attack.
Open	Phone service affecting most phone users could be significantly disrupted, indefinitely, via a fairly straight-forward assault.
Unsecure	Phone system or service affecting all users could be readily and indefinitely disabled.

"Security weaknesses earned the basic Avaya configuration a so-so Vulnerable rating, while the hardened package fared better with an overall Resistant rating."

What Are We Worried About?

Cisco.com

- **Eavesdropping**
  - With TDM, Butt Set or Digital Analyzer: Requires knowledge and access to a specific pair of wires
  - With VoIP, Sniffer, dsniff, ettercap: Anywhere in the broadcast domain
- **DoS, Worms, and the Virus-De-Jour**
  - Targeted or Anonymous Attacks against Windows
  - TCP Vulnerabilities, L2/L3 Exploits
- **Toll Fraud Exploits – Similar to a PBX**

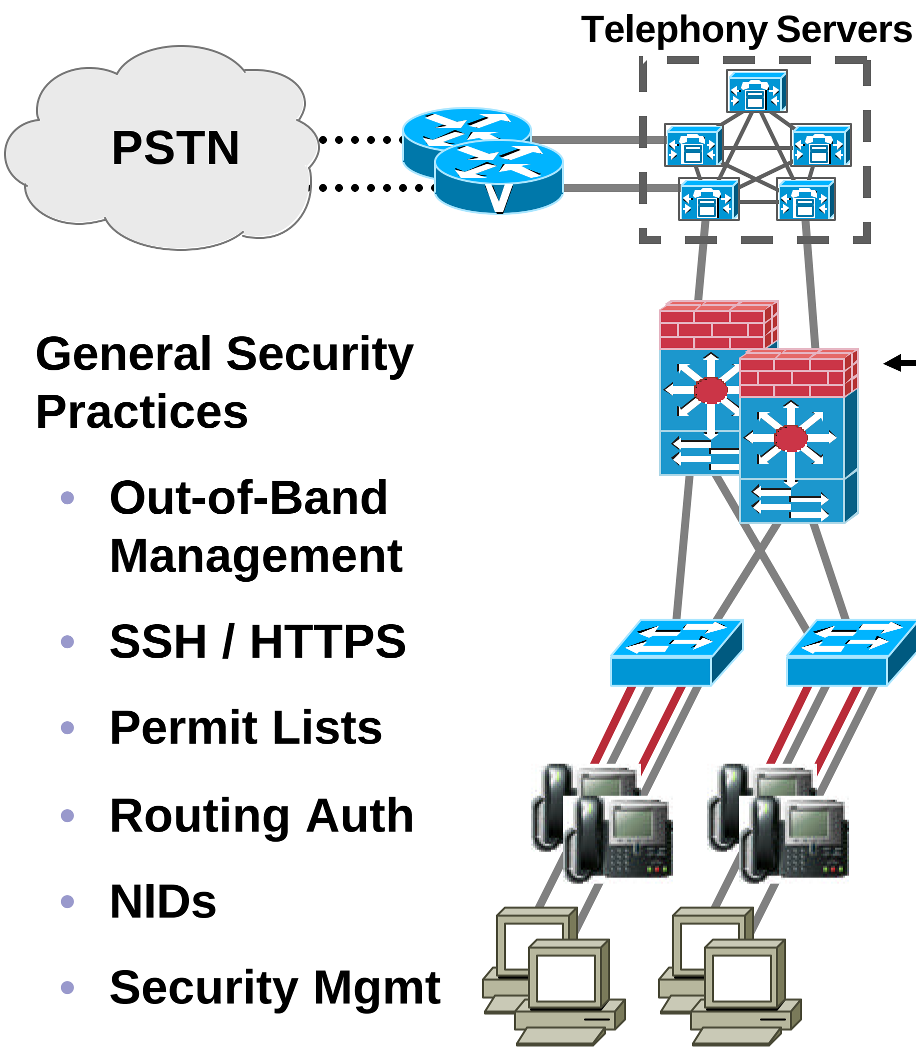
Security Agenda

- Secure the Infrastructure for Voice
- Protect IP Phones
- Harden the Operating System
- Prevent Toll Fraud

Securing the Infrastructure for Voice

Single Site

Cisco.com



Refer to SAFE and SRND for more detailed information

General Security Practices

- Out-of-Band Management
- SSH / HTTPS
- Permit Lists
- Routing Auth
- NIDs
- Security Mgmt

Firewall or ACL in front of telephony servers with Rate Limiting

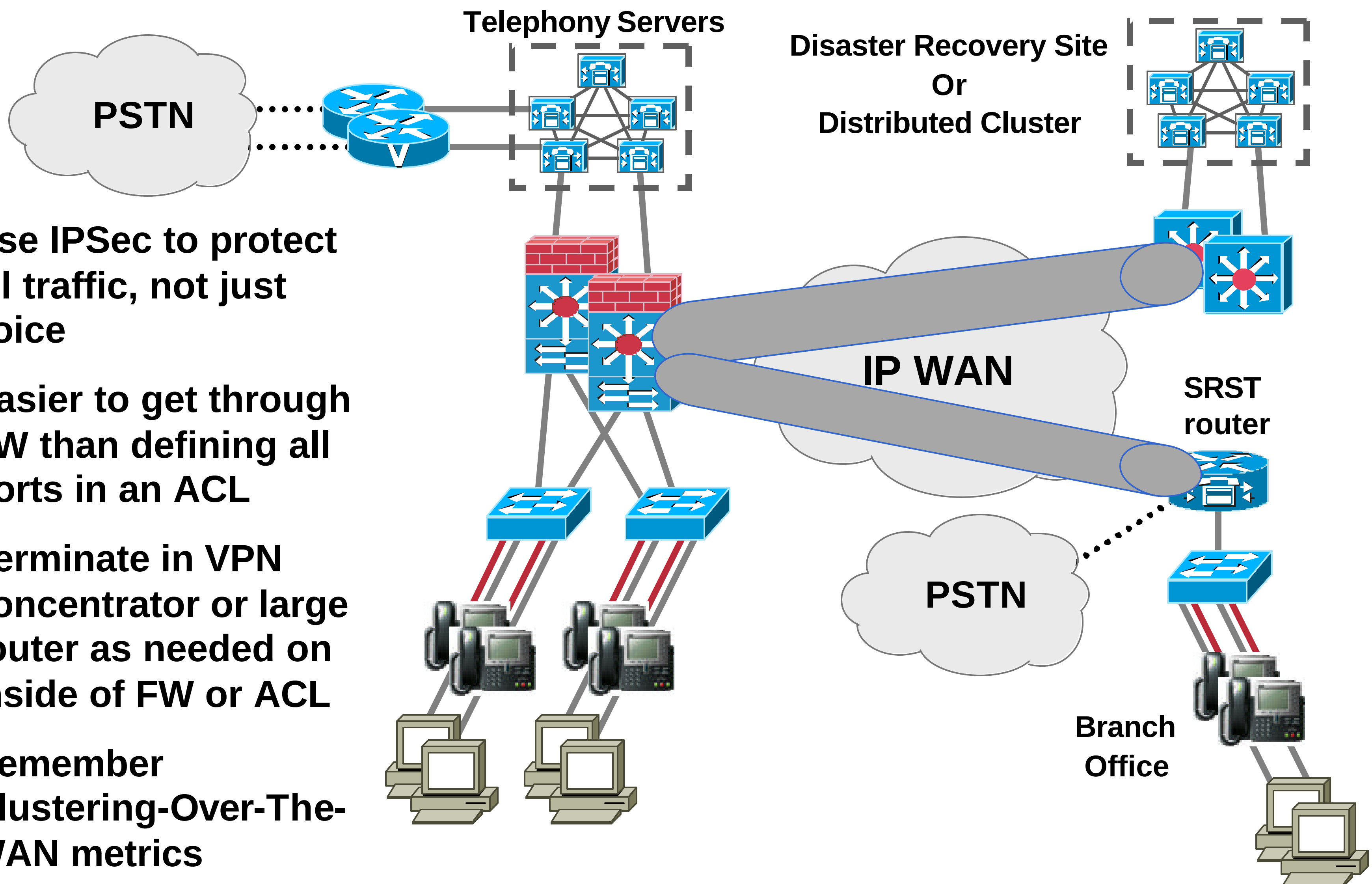
Layer 2 Best Practices

- Separate voice & data VLANs
- VLAN ACLs (VACLs)
- DHCP Snooping
- Dynamic ARP Inspection
- IP Source Guard
- Port Security
- Conditional Trust

Connecting to a Branch Office or DR Site

Cisco.com

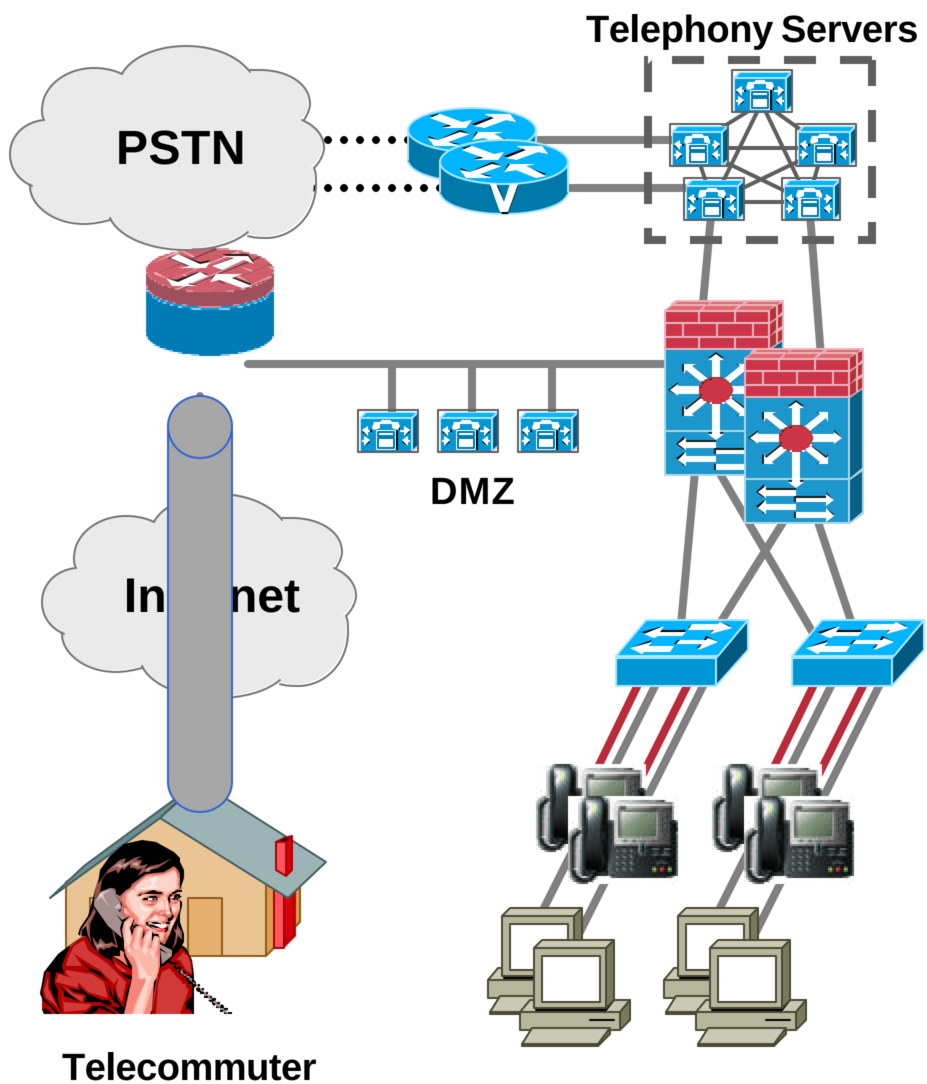
- Use IPSec to protect all traffic, not just voice
- Easier to get through FW than defining all ports in an ACL
- Terminate in VPN concentrator or large router as needed on inside of FW or ACL
- Remember Clustering-Over-The-WAN metrics



Connecting Telecommuters over the Internet

Cisco.com

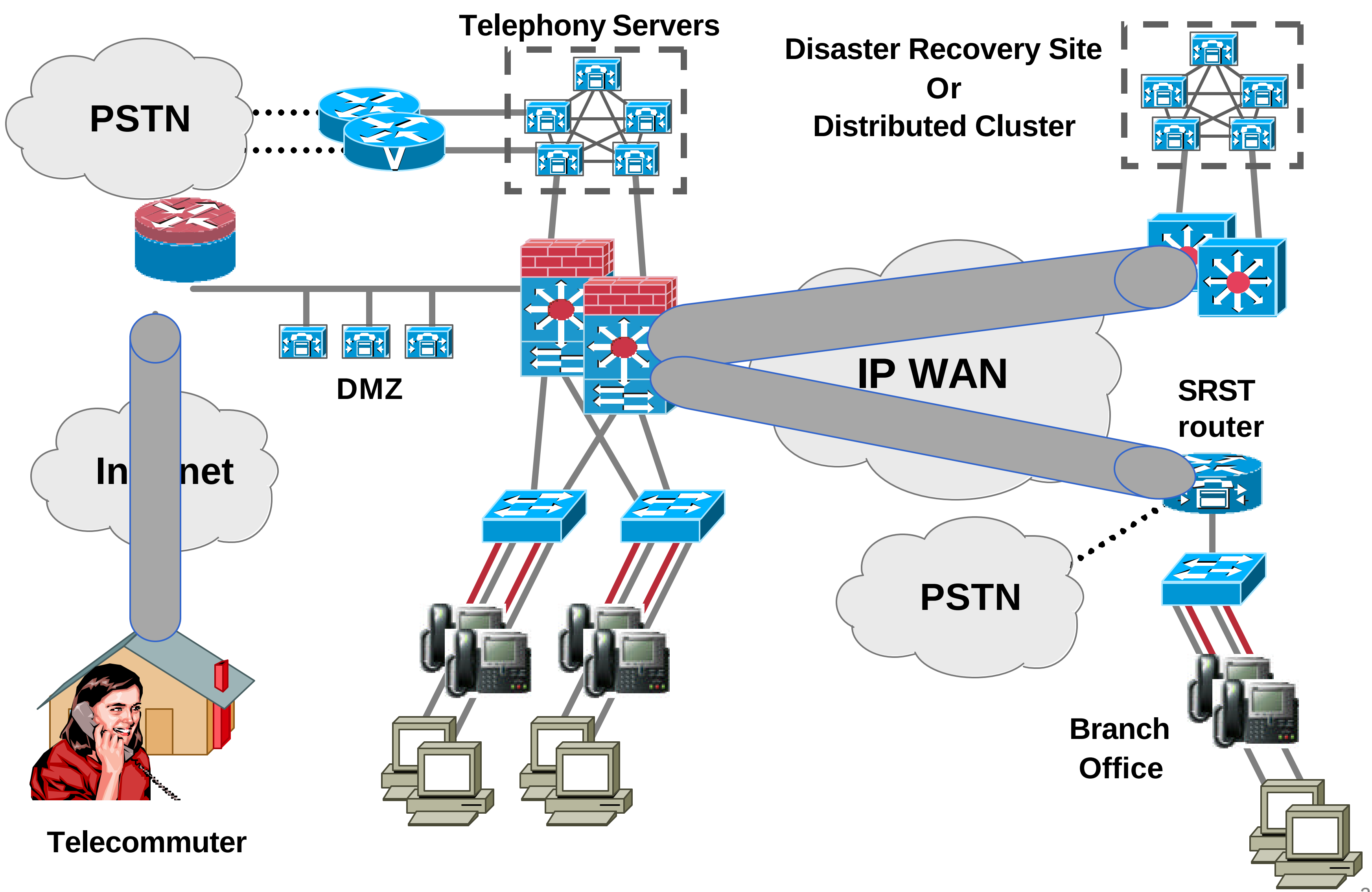
- Use V3PNs with IPSec to protect all traffic from SOHO location, not just voice
- Terminate at HQ end in VPN concentrator or large router



Putting it all Together

www.cisco.com/go/safe & www.cisco.com/go/srnd

Cisco.com



Firewall & NAT Voice ALGs

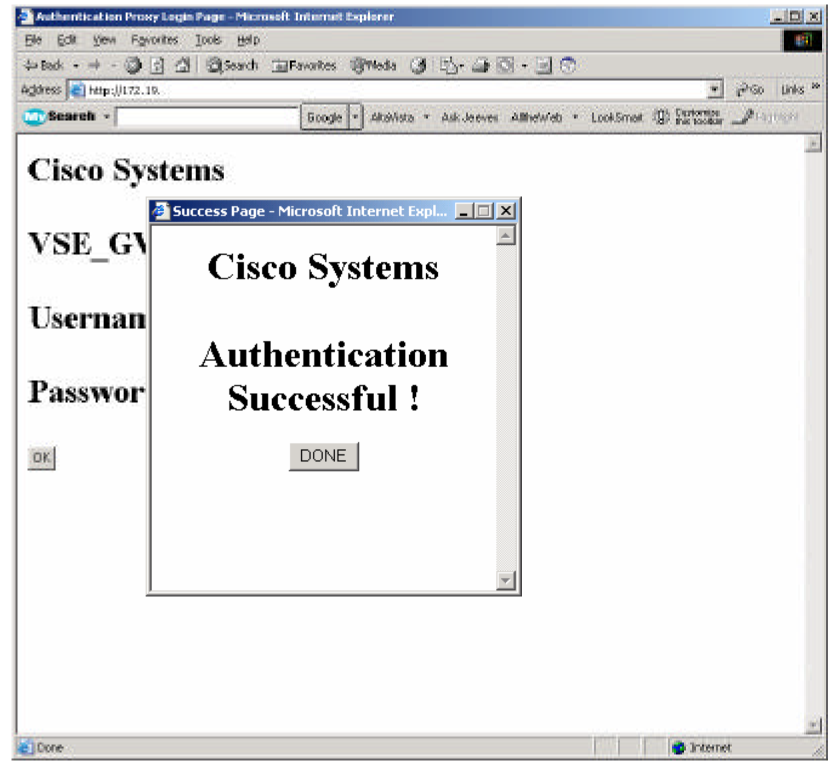
ALG = Application Layer Gateway = Fixup

- Stateful inspection of voice signaling protocols
- Exist for SIP, SCCP, H.323, and now MGCP on PIX and IOS Firewalls & NATs
- Firewall ALG
  - Inspects signaling packet to discover what UDP port the RTP stream is going to use
  - Dynamically opens pinhole for that UDP port
  - Watches for end-of-call signaling to close pinhole
- NAT ALG
  - Modifies the private originating source IP address and port number in the signaling packet to a publicly addressable NAT'ed IP address and port
- Note: Current ALGs not applicable when voice is authenticated or encrypted!!!

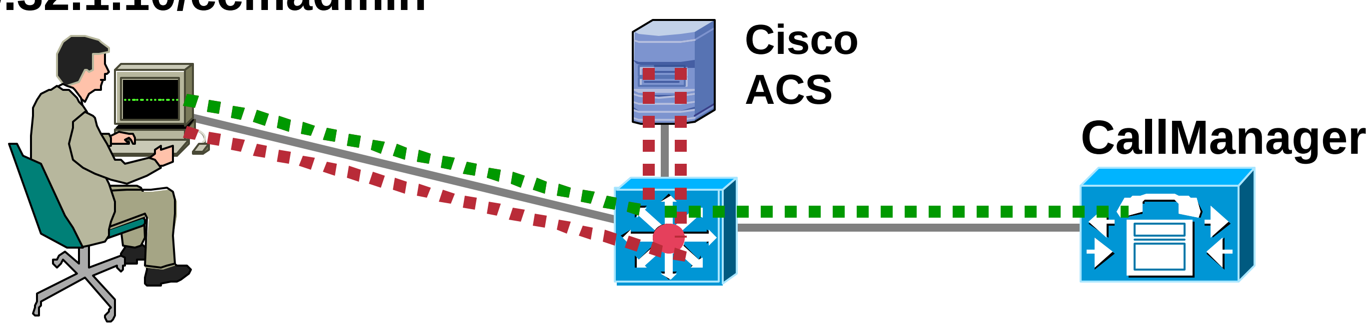
Lock Down Most Vulnerable Ports

Cisco.com

- Authentication Proxy - Dynamic ACL in IOS
- Allows vulnerable ports to be opened after a AAA challenge when a user makes a connection through a router
- HTTP, FTP, Netbios, etc.
- Authorization persists for configurable time
- Can be put in L3 in front of CCM for admin and users



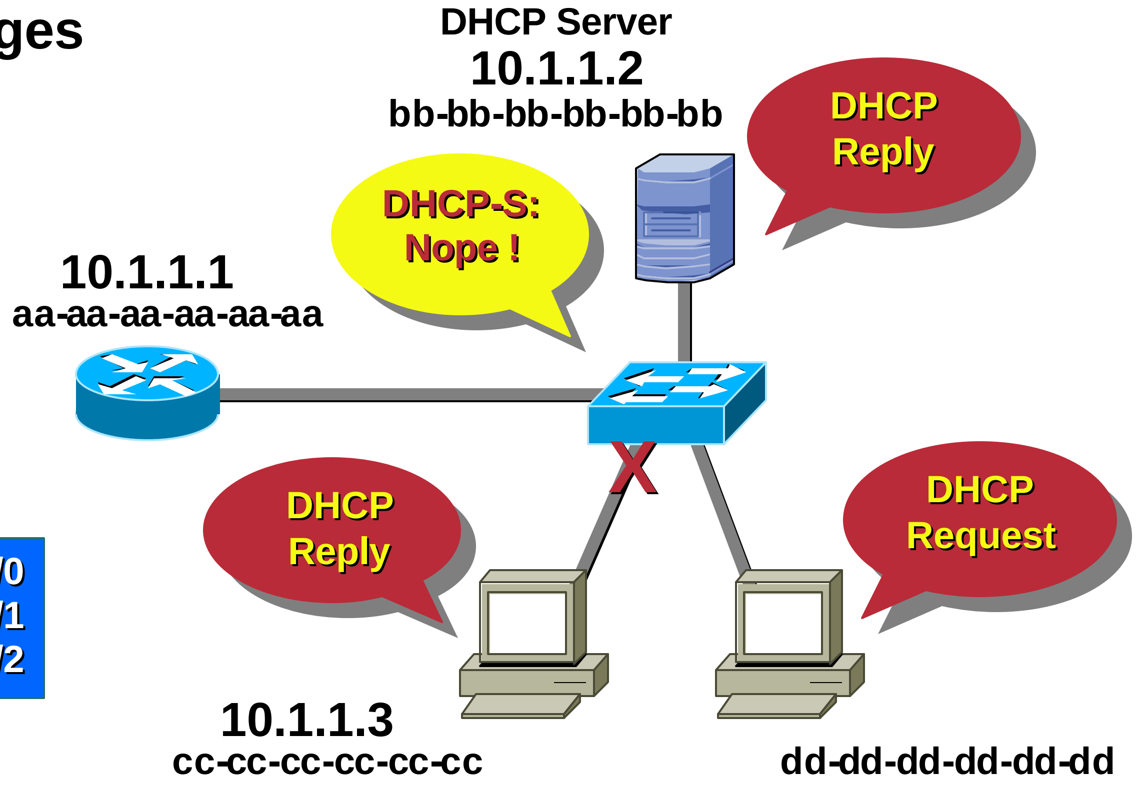
http://10.32.1.10/ccmadmin



Prevent DHCP Spoofing and Exhaustion

Cisco.com

- DHCP Snooping creates binding of IP address to MAC address
- Defines ports that can DHCP Reply
- Rate limit DHCP messages
- Resets with loss of link



10.1.1.1	aa-aa-aa-aa-aa-aa	1/0
10.1.1.2	bb-bb-bb-bb-bb-bb	1/1
10.1.1.3	cc-cc-cc-cc-cc-cc	1/2

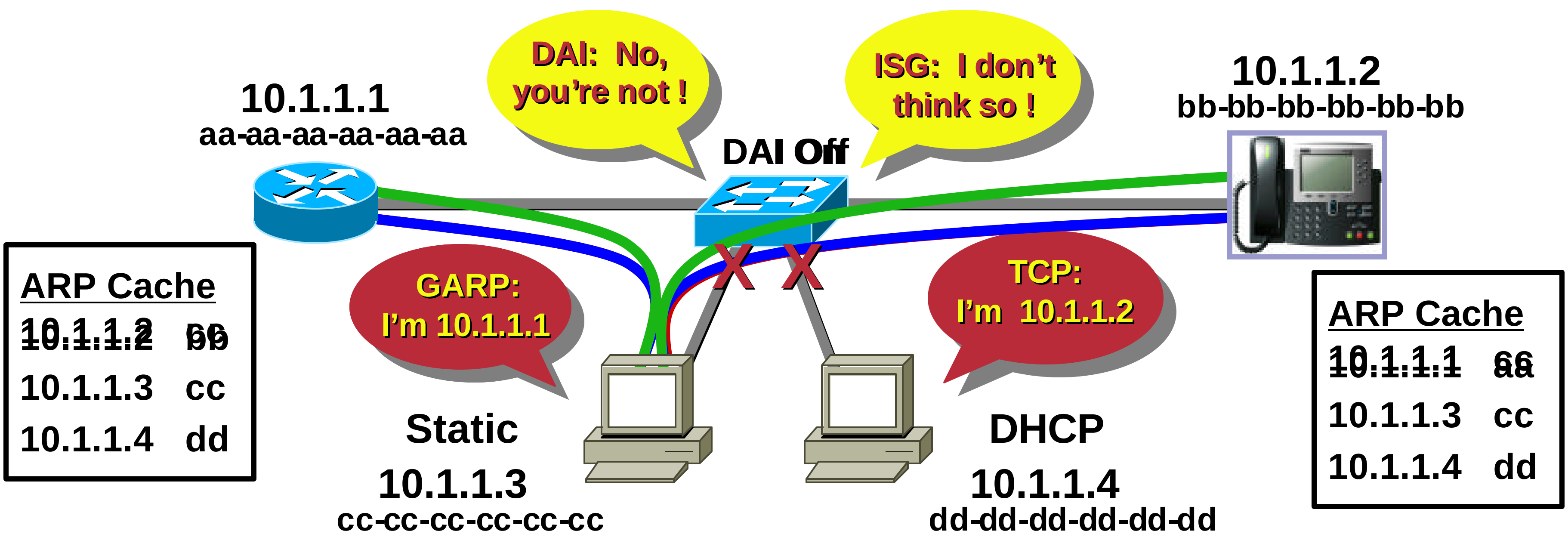
Stop Man-in-the-Middle Attacks

Cisco.com

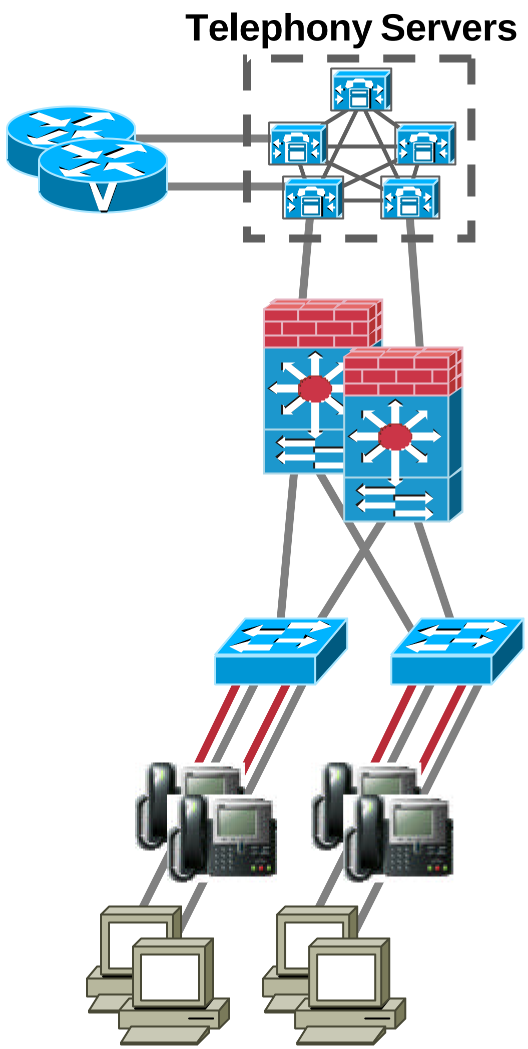
- **Built on DHCP Binding Table**
- **Dynamic ARP Inspection watches ARP / GARP for violations**
- **IP Source Guard examines every packet**
- **Will shun packets or disable port**

Successfully stops ettercap, dsniff

10.1.1.1	aa-aa-aa-aa-aa-aa	1/0
10.1.1.2	bb-bb-bb-bb-bb-bb	1/1
10.1.1.4	dd-dd-dd-dd-dd-dd	1/3



Stop Attacks at the Edge

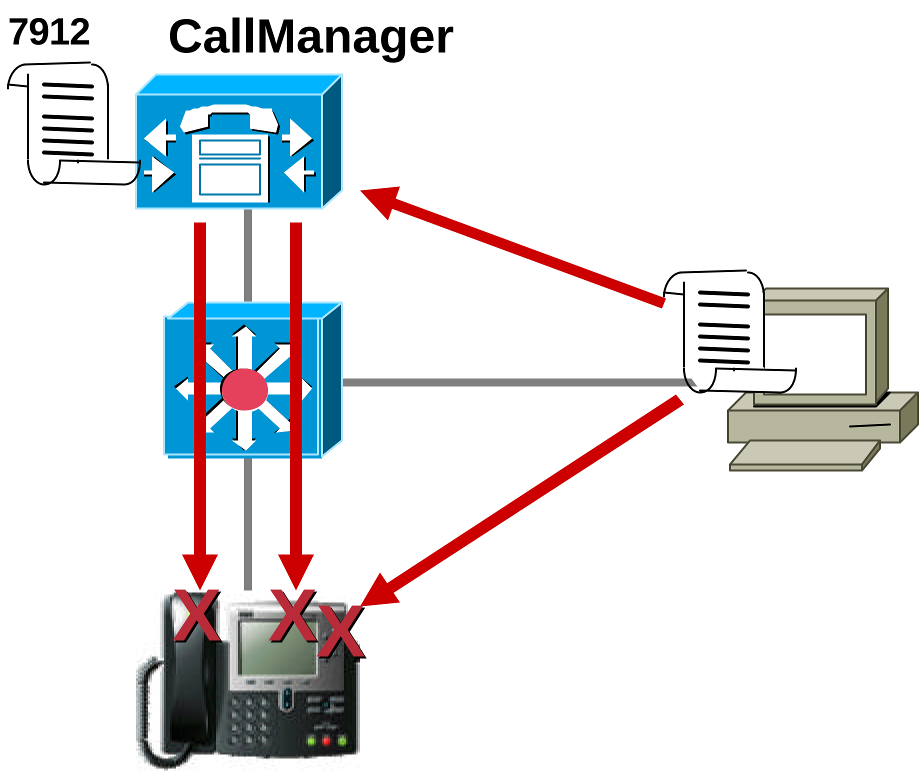


- Phones only need to send RTP to each other and TCP to the servers
- Use a simple VACL to limit traffic to exactly that
- Stops any and all TCP attacks against the phones !!!

Protecting Cisco IP Phones

Stop Rogue Images From Entering Phones

- **Signed Firmware Images**
  - Guaranteed from Cisco
  - Unique signature for each phone model
  - Can't subvert security features!
  - CCM 3.3(3)
- **Signed Config Files**
  - 7940, 7960 and 7970
  - CCM 4.0



Protect the Phone at Layer 1 and 2

Configurable Options:

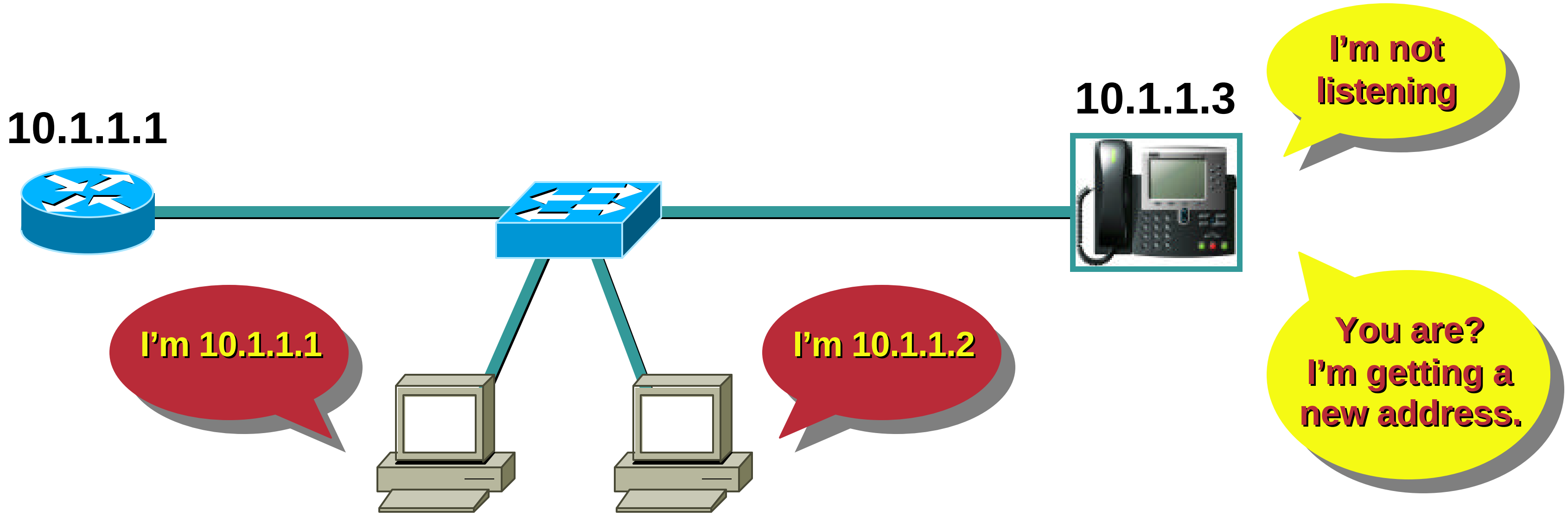
- **Disable**
  - **PC Port**
  - **"Settings" Button**
  - **Speakerphone**
  - **Web Access**
- **Ignore Gratuitous ARPs (GARPs)**
- **Block voice VLAN from PC port**

Product Specific Configuration	
Disable Speakerphone	☐
Disable Speakerphone and Headset	☐
Forwarding Delay*	Disabled
PC Port*	Disabled
Settings Access*	Disabled
Gratuitous ARP*	Disabled
PC Voice VLAN Access*	Disabled
Video Capabilities*	Disabled
Auto Line Select*	Disabled
Web Access*	Disabled

These features were all introduced in CCM 3.3(3), except Signed Config Files and Disable Web Access which were introduced in CCM 4.0

Ignore Gratuitous ARP

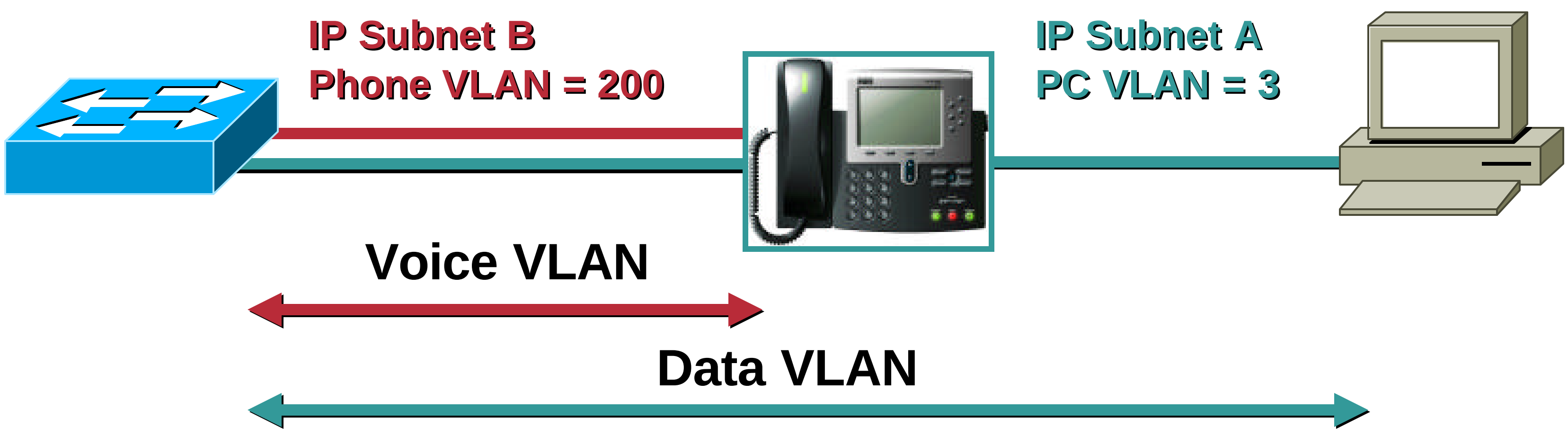
- Block acceptance of Gratuitous ARP (GARP) by the phone
- Prevents malicious device from assuming the identity of something else (default router) to become man-in-the-middle
- Doesn't really ignore it. Just doesn't update ARP cache
- Can lead to DoS attack – "I have your address"
  - Better to do this in layer two



Block PC Access to Voice VLAN

- Blocks 802.1q tagged with voice VLAN being sent to or received from the PC port on the phone.
- Blocks the malicious sniffing of voice streams from the PC port of a phone.
- Also blocks intentional sniffing in troubleshooting or monitoring situations.
- There are better ways to sniff, such as the SPAN and R-SPAN feature on Catalyst switches.

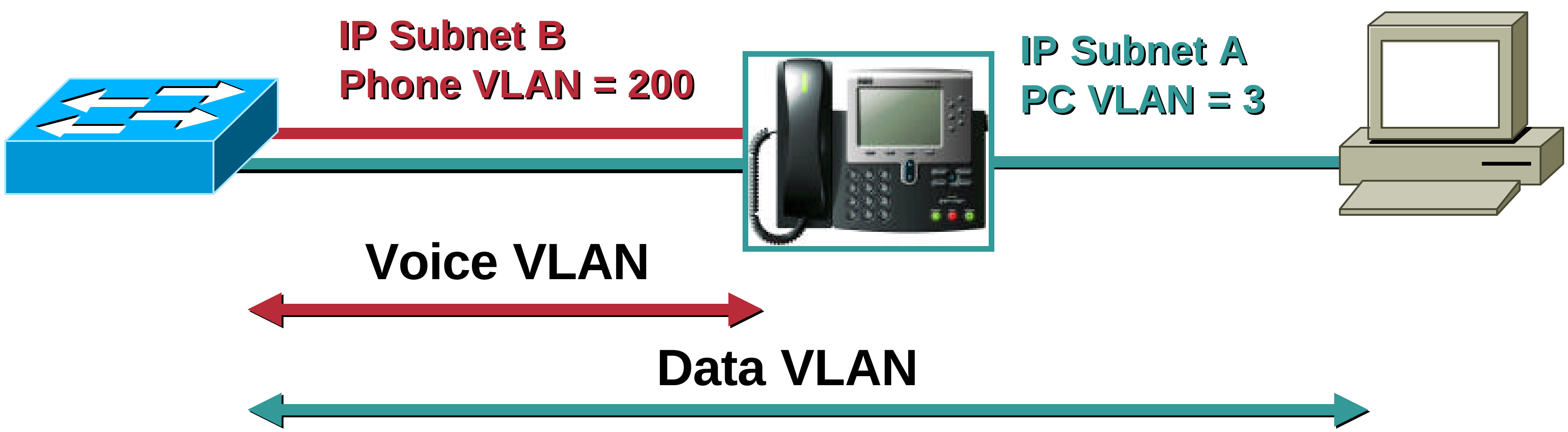
Successfully stops VOMIT



Block PC Access to Voice VLAN

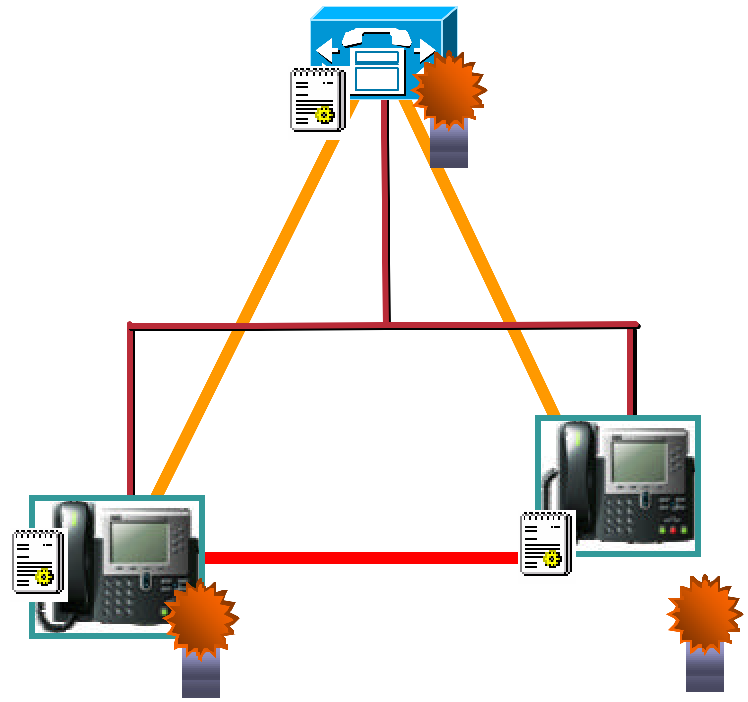
Differences between phone model implementations.

- **7940 & 7960 only block voice VLAN, allowing PC to run 802.1Q on any other VLAN. (Makes for an interesting Catalyst configuration.**
- **7970 blocks all packets containing an 802.1Q header.**
- **7912 doesn't block anything.**



Certificate-Based Authentication and Encryption

- Public Key / Private Key Pair
- X.509v3 Digital Certificate
  - Self-Signed (CCM)
  - MIC from Cisco Mnfg (7970)
  - LSC from CAPF (7940/7960)
- Certificate Trust List
  - CTL Client
- Transport Layer Security
  - RSA Signatures
  - HMAC-SHA-1 Auth Tags
  - AES-128-CBC Encryption
- Secure RTP
  - HMAC-SHA-1 Auth Tags
  - AES-128-CM Encryption



In CallManager 4.0,

- 7970 supports MIC certs with auth & encr TLS & SRTP
- 7940/7960 support LSC certs with auth TLS

Authentication and Encryption

What is Encryption?

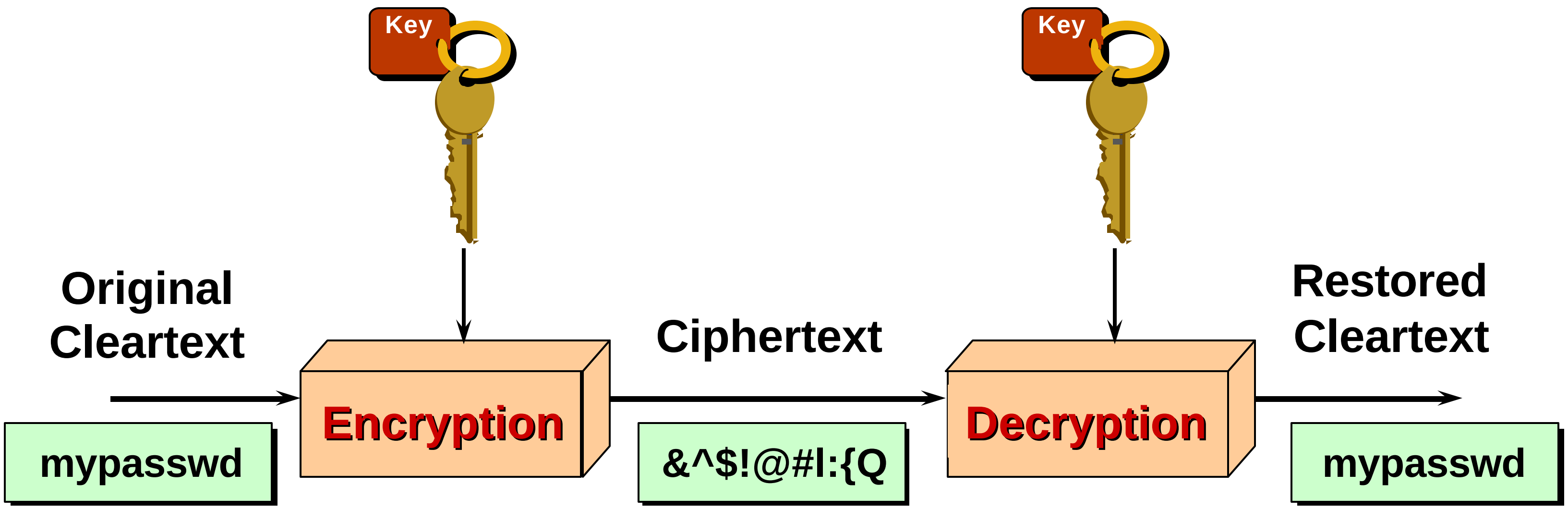
Encryption – A process whereby a message is converted to something incomprehensible by means of a cipher and key, such that it can only be reconverted back to the original message by the holder of the matching key and utilizing the same cipher .

Cipher – A system in which units of plain text are arbitrarily transposed or substituted according to a predetermined key.

Key – An initial, primary value input to a computational algorithm, producing a theoretically unique result exclusive to the input value.

Encryption – Basic Model

Cisco.com

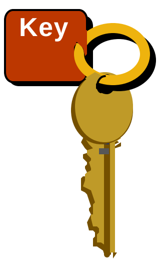


- Encryption turns cleartext into ciphertext
- Decryption restores cleartext from ciphertext
- Encryption and decryption using the same mathematical algorithm and the same key – symmetric encryption
- Examples: Digital Encryption Standard (DES, 3DES), IDEA, RC2, RC4

Soft Key

Cisco.com

Soft Key – A <u>numerical</u> value that acts as the algorithmic input to initiate the encryption or decryption process.



=

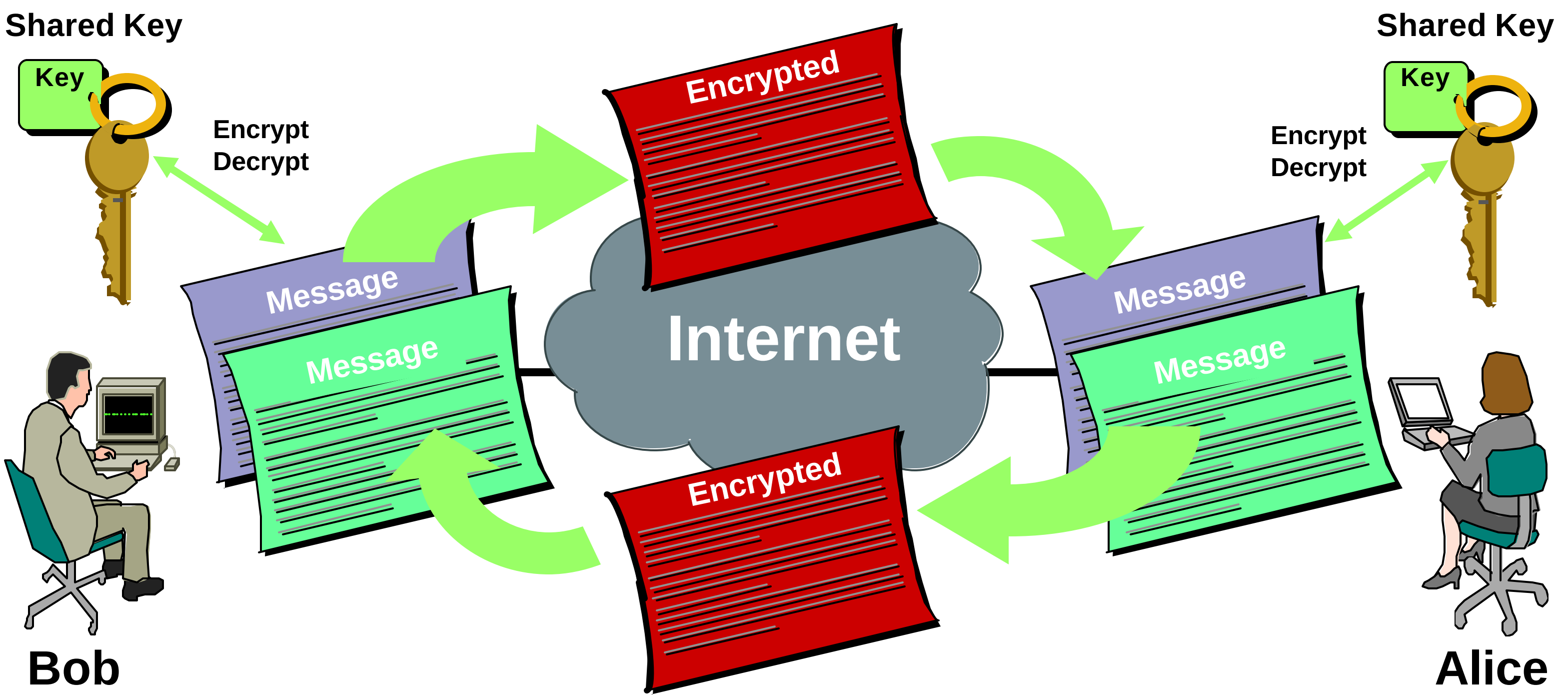
2081 8102 81A1 01AA A98B 2E27 1F0E EF1D
5747 2054 B4EE B1B3 BEDB 5676 45F3 1ED7
3737 CDD4 51B3 67AD D867 ECD0 FFC5 995B
E112 5411 7584 7F6A 3877 66FC 3C1F 45C2
7887 34A2 2413 6242 E243 6B84 6F06 1E73
B43A 9396 49C4 CB2E 9982 8AD7 B8AA 9C01
D689 9AE2 ABF3 1B84 42C0 F337 341C 42CB
1785 0B0D 8C54 C900 0B1B 6CE7 E7B5 28AD
727A 2F55 F1C1 A392 0301 0201

1024 bit RSA Key

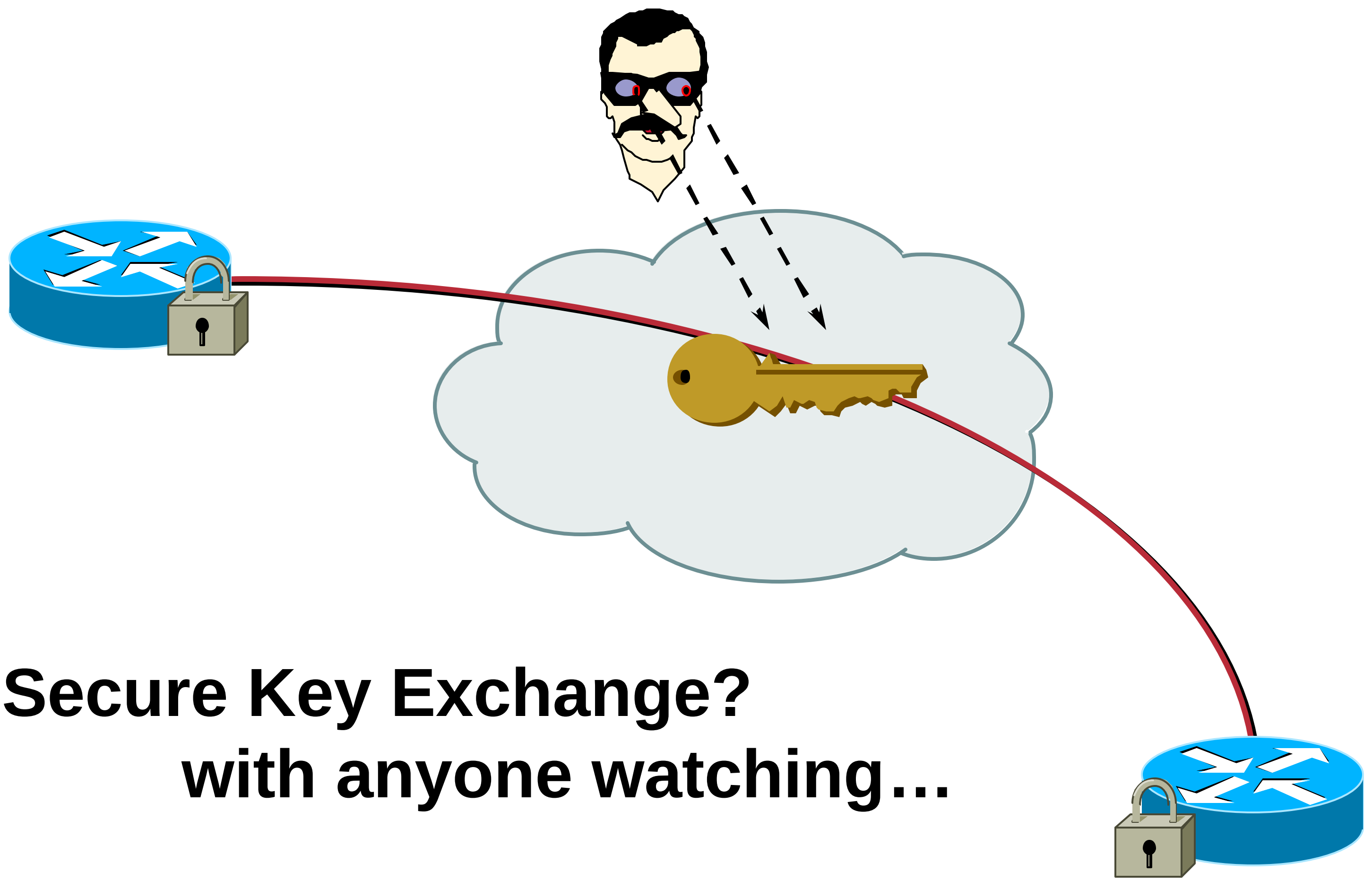
Pre-Shared Key (PSK)

Cisco.com

Symmetric Encryption – Both parties exchange encrypted messages using the *same, shared key* for both encryption and decryption.

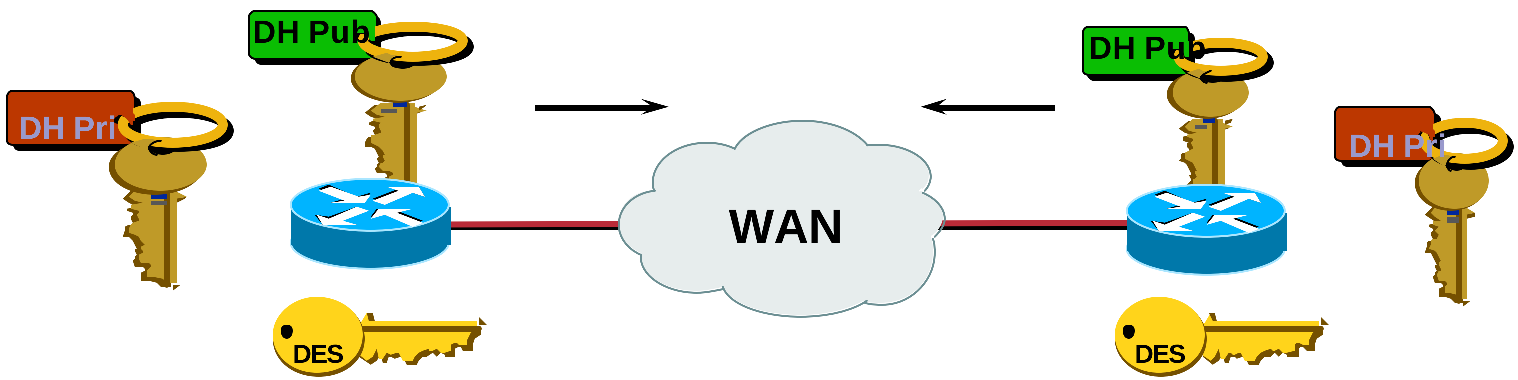


Key Exchange



Secure Key Exchange?
with anyone watching…

Deriving Secret Keys Using Public Key Technology (Diffie-Hellman)



- **Each device has three keys:**
  1. **A private key, generated by each device, which is kept secret and never shared**
  2. **A public key, calculated from the private key by each device, which is non-secret**
  3. **A shared secret key that is used to encrypt and decrypt data using a symmetric encryption algorithm (e.g. DES)**

The Diffie-Hellman Public Key Exchange

Cisco.com

Site A

Private Value, X_A
Public Value, Y_A
Message, m

$Y_A = m^{X_A} \bmod p$

Y_A →

Site B

Private Value, X_B
Public Value, Y_B
Message, m

← Y_B

$Y_B = m^{X_B} \bmod p$

$Z = (Y_B^{X_A}) \bmod p$

shared secret

$Z = (Y_A^{X_B}) \bmod p$

- By exchanging numbers in the clear, two entities can derive a new unique number known only to them
- Result is a shared key which can be used as the DES key—repeated as often as required

Scalable and secure key generation

Diffie-Hellman Example

Host A

prime p = 5, primitive g = 3

Choose Xa such that

0 <= Xa < p, Xa = 2

Ya = g ^Xa mod p

= 3^2 mod 5

= 4

Exchange Values

p, g, Ya →

Ke = Yb^ Xa mod p

= 1^2 mod 5

= 1

Host B

prime p =5, primitive g = 3

Choose Xb such that

0 <= Xb < p, Xb =4

Yb = g^Xb mod p

= 3^4 mod 5

=1

Exchange Values

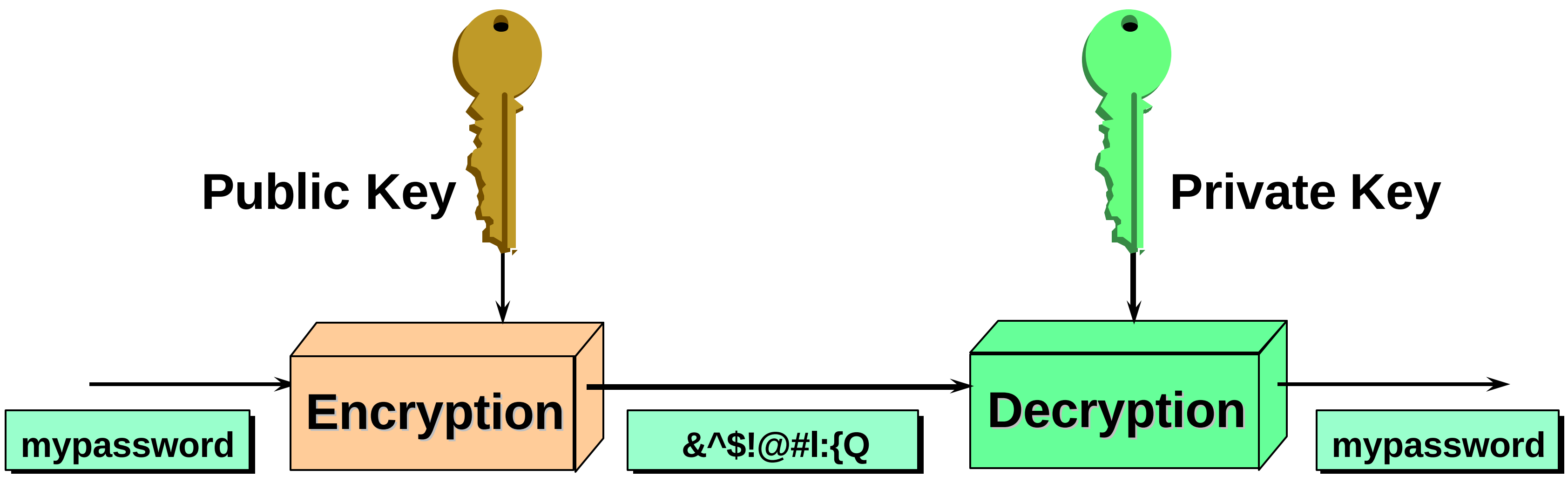
← p, g, Yb

Ke = Ya^Xb mod p

= 4^4 mod 5

= 1

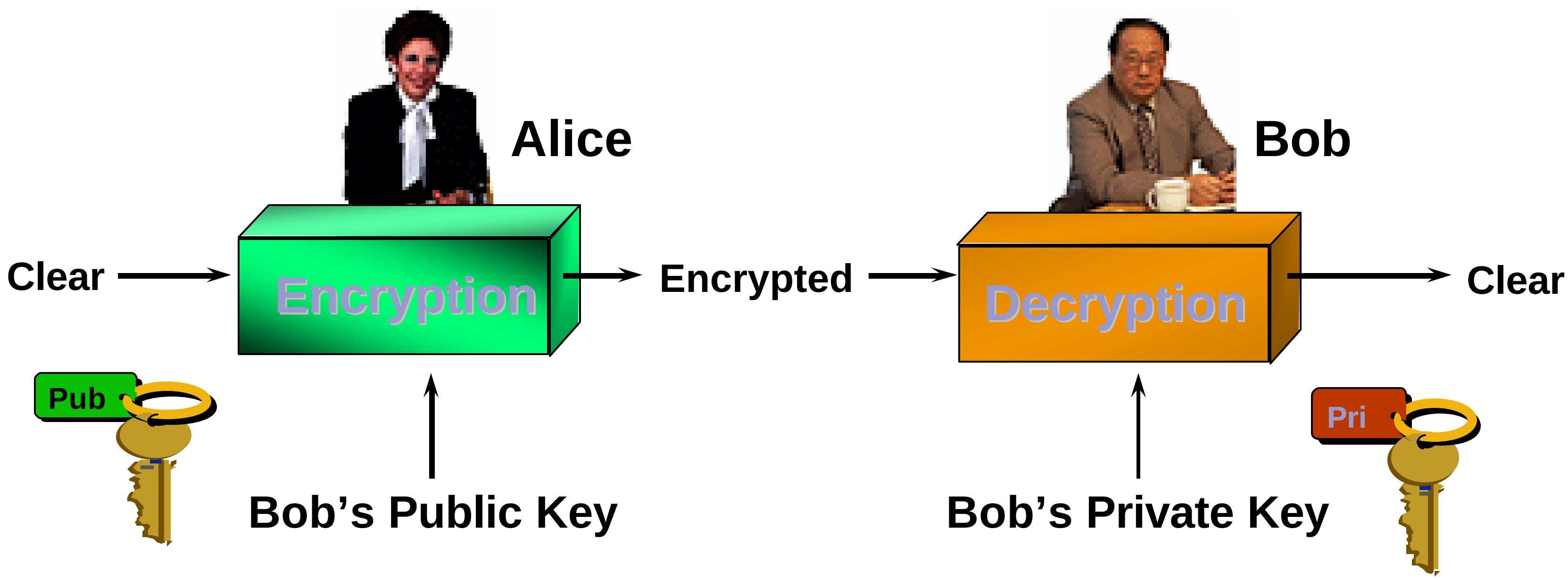
Asymmetric Encryption



- Encryption turns cleartext into ciphertext using **Public Key**
- Decryption restores cleartext from ciphertext using **Private Key**
- Encryption and decryption using the same mathematical algorithm but different keys – asymmetric encryption
- Examples: RSA and DSS

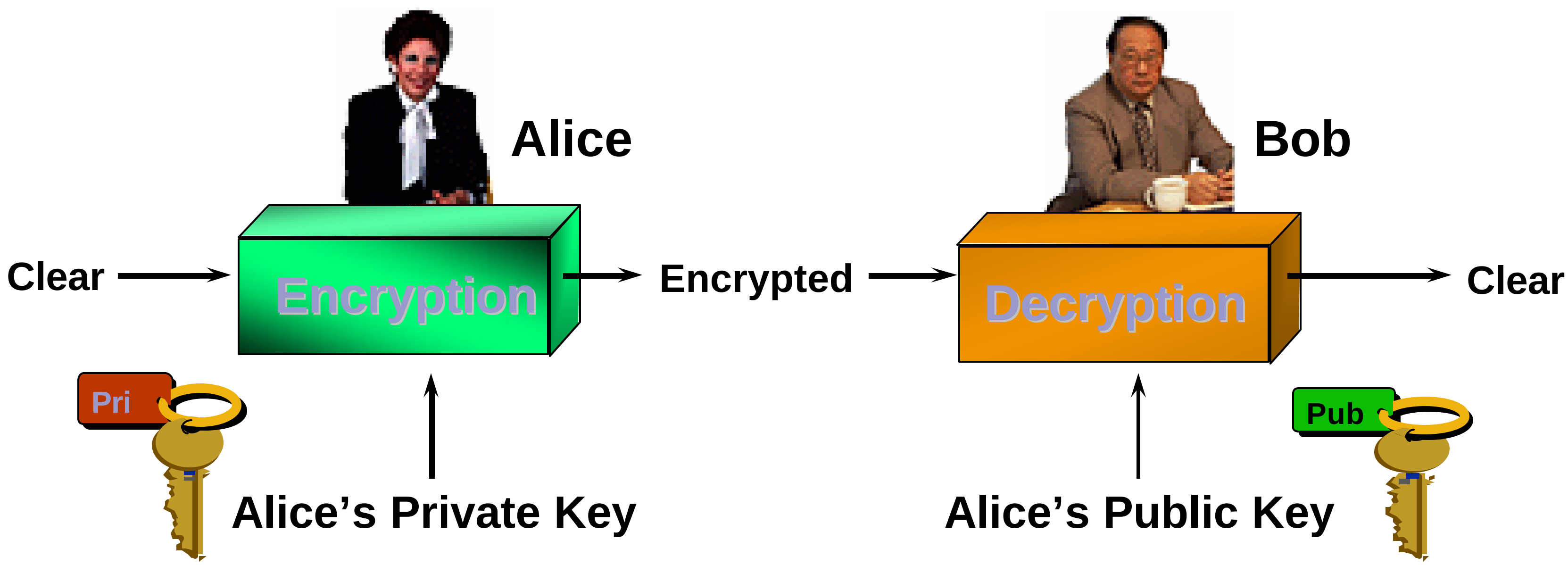
Data Confidentiality

Cisco.com



- Alice gets Bob's public key
- Alice encrypts message with Bob's public key
- Bob decrypts using his private key

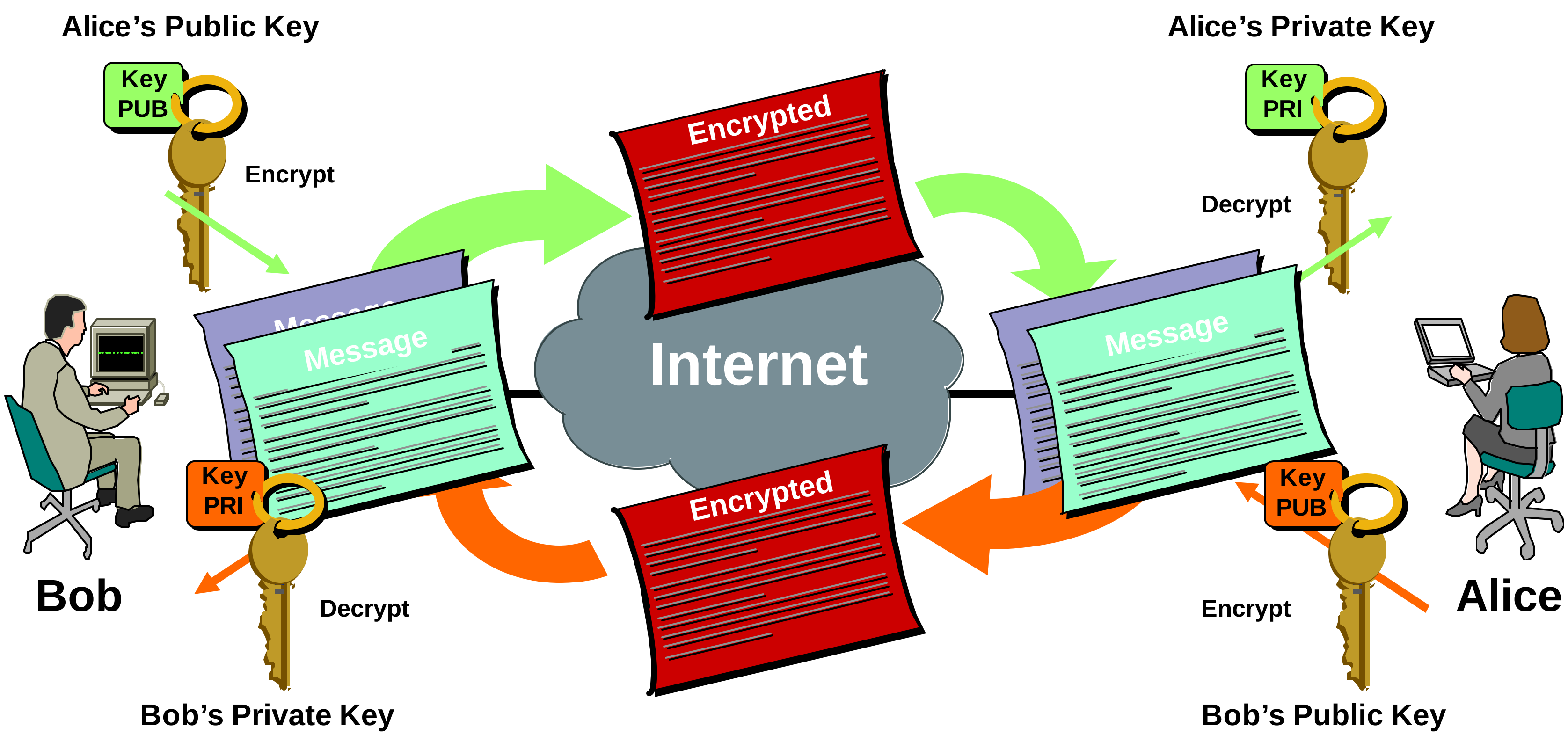
Sender Authentication



- Alice encrypts message with her private key
- Bob gets Alice's public key
- Bob decrypts using Alice's public key

Public Key Infrastructure (PKI)

Asymmetric Encryption – A distributed *public* key is used to <u>encrypt</u> messages that can only be <u>decrypted</u> with a *private* key held by the publisher of the public key.



Secret Key and Public Key Systems

- **Secret key encryption**
  - A single key
  - Encryption key = decryption key
  - Symmetric key
- **Public key encryption**
  - A pair of keys
  - Public key and private key
  - Asymmetric key

Secret Key Encryption Algorithms

- AES-128 (Advanced Encryption Standard)
- DES (Data Encryption Standard)
- Triple DES
- Others: IDEA, Blowfish, CAST-128, ...

DES/3DES Vulnerability

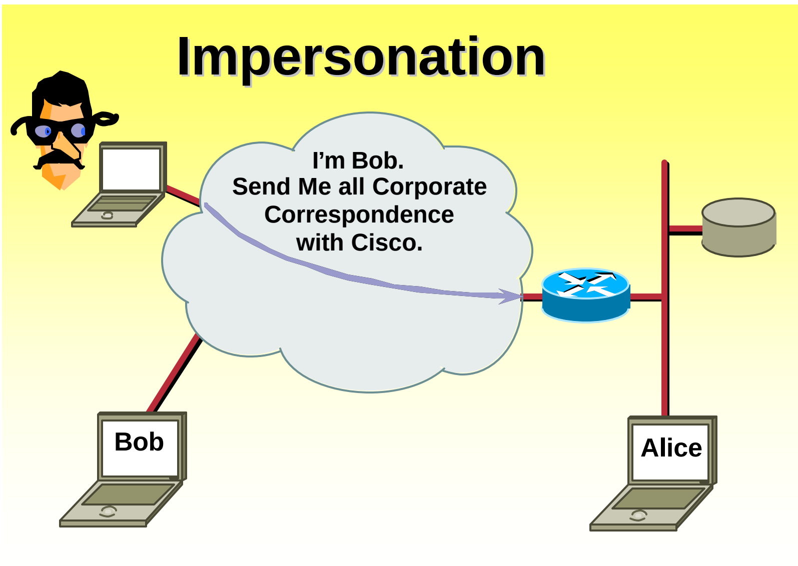
By brute force attack:

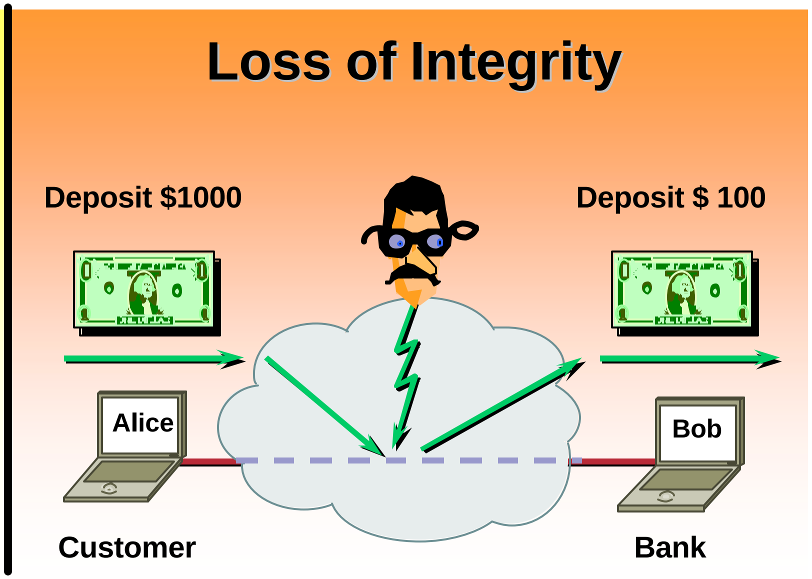
- **A single Pentium III class workstation can break a DES key in *less than* <u>10 hours</u>**
- **A million Pentium III class workstations can break a (3-key) 3DES key in <u>10,000,000,000,000 years</u>**

3DES is subject to crypto-analytical attacks by insertion of a “known” payload.

Hashing

Hash/Signature Protection





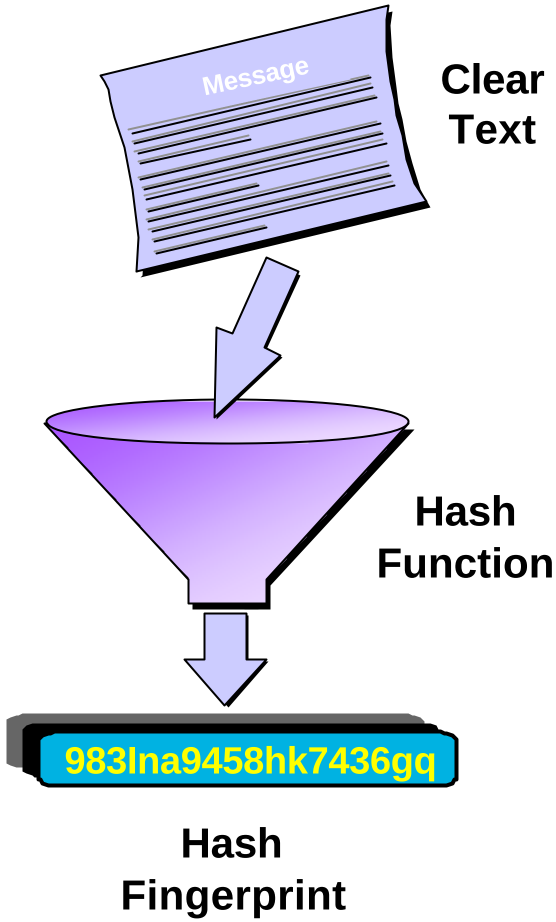
Hashes and **Signatures** guarantee identity of peers and message integrity during transport over un-trusted or public networks

Integrity—ensuring that data is transmitted from source to destination without undetected alteration

Authentication—knowing that the data received is the same as the data that was sent and that the claimed sender is in fact the actual sender

What is a Hash?

Hash – A one-way mathematical summary of a message such that the hash value cannot be (easily) reconstituted back into the original message – even with knowledge of the hash algorithm.



Two popular hash functions

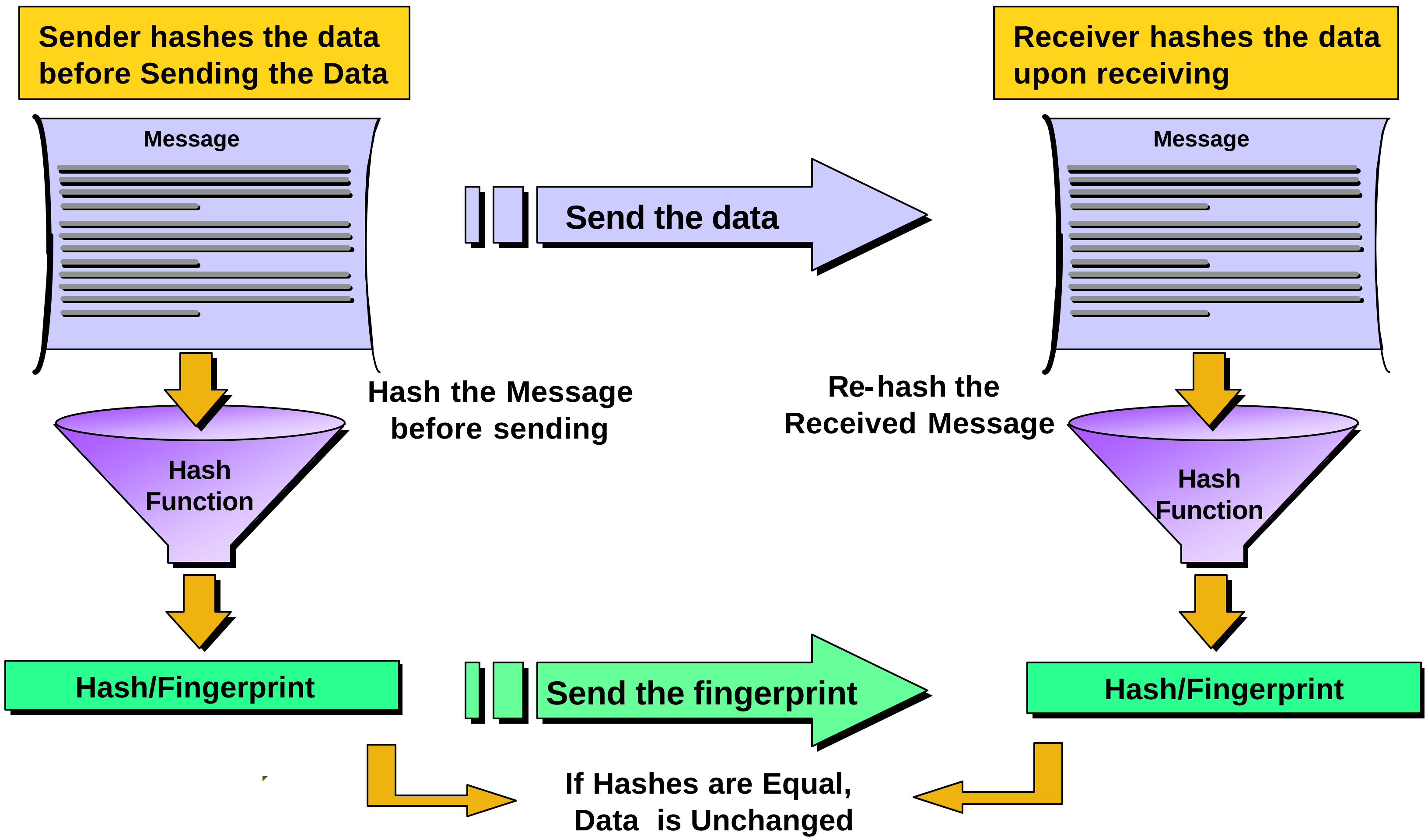
MD5: Produces 128 bit fingerprints

SHA: Produces 160 bit fingerprints

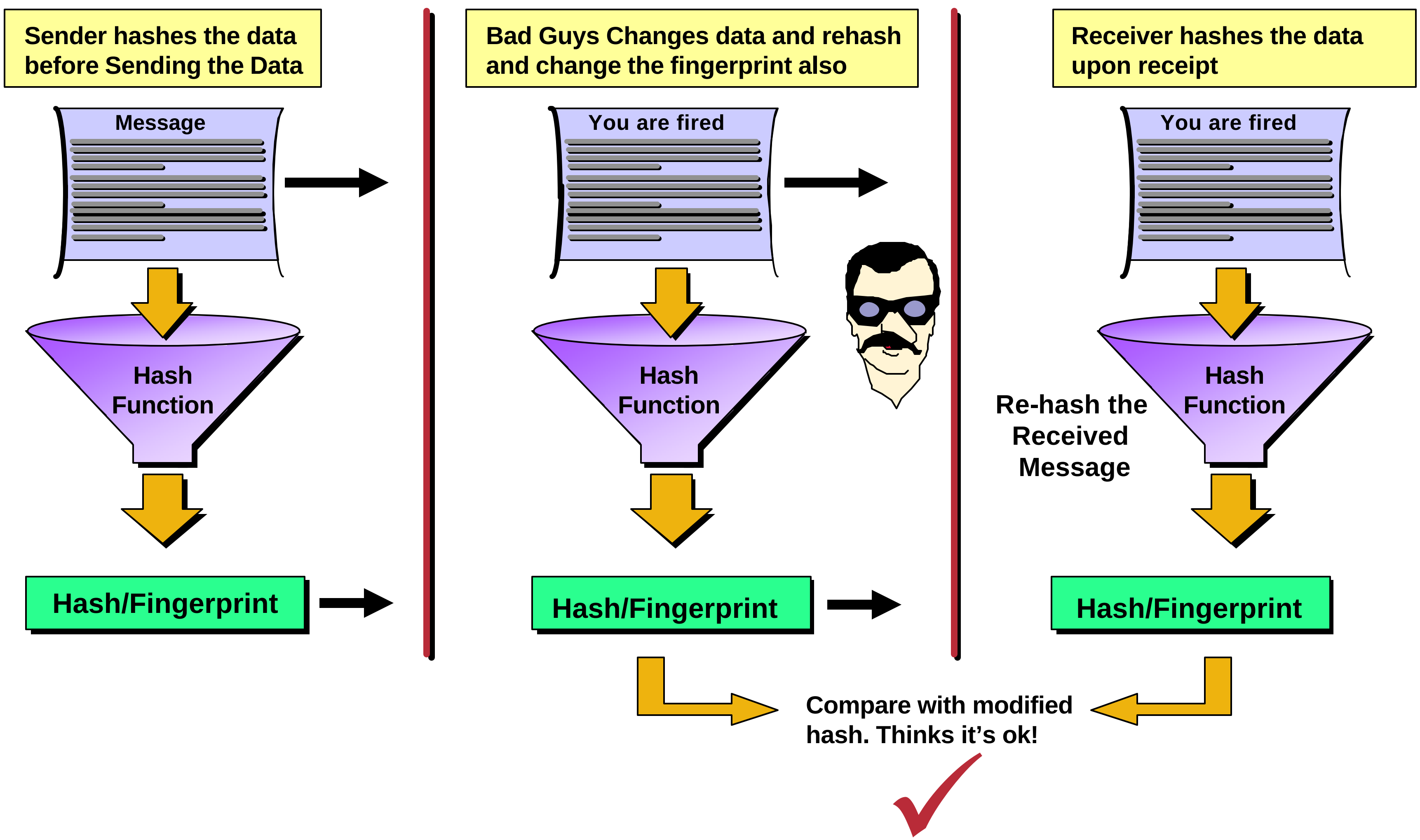
Using a Hash

Cisco.com

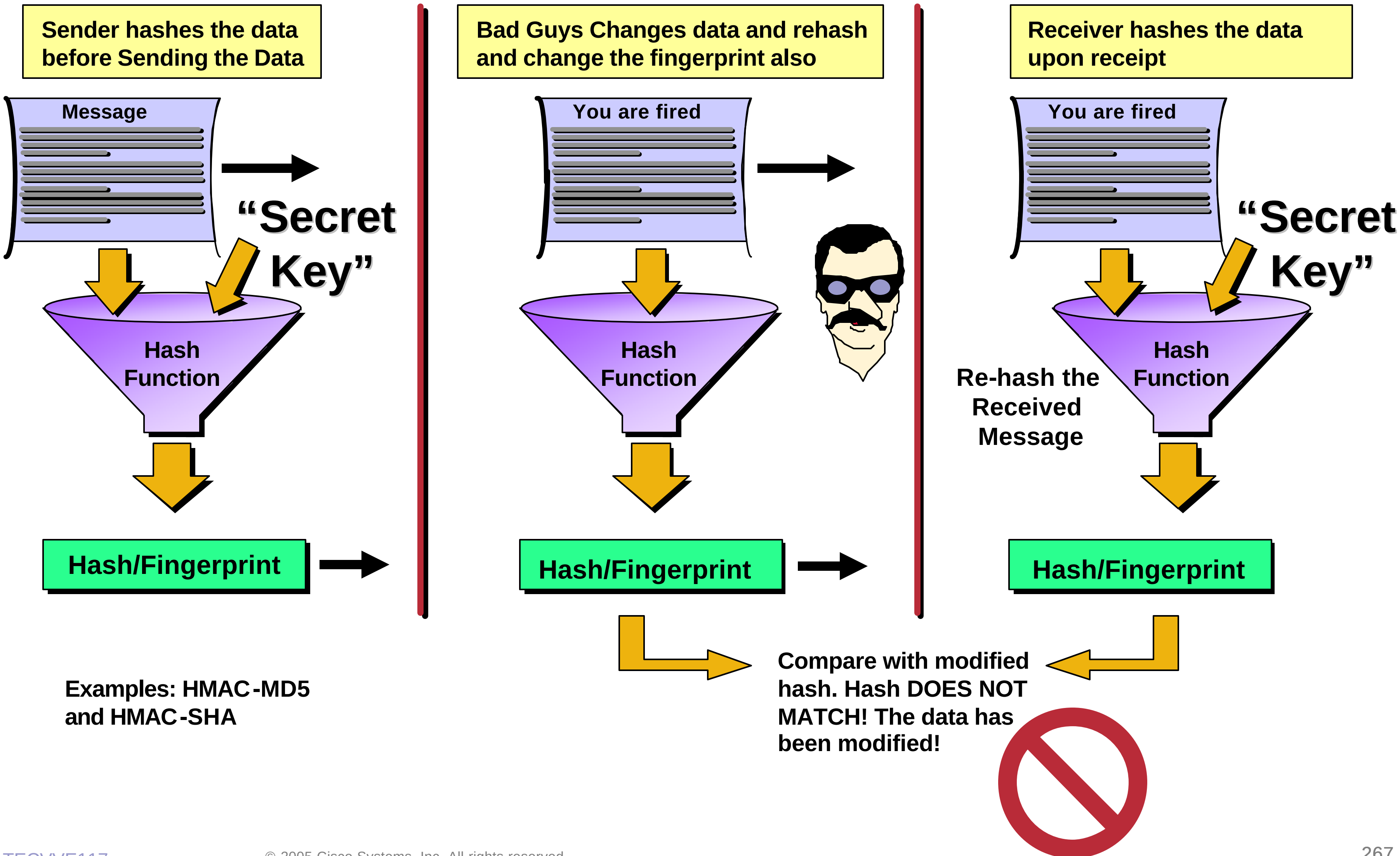
Check that ensure data has not been changed!



Problem with basic hashing



Proving integrity



Examples: HMAC-MD5 and HMAC-SHA

Hashing Algorithms

- **MD5** (Message Digest v5)

  Older but most widely supported hash algorithm

- **SHA** (Secure Hashing Algorithm)

  Newer and more secure hash than MD5

- **HMAC** (Hash-based Message Authentication Code

  Mechanism for two parties to sign hash values, providing for proof of sender identity

HMAC-MD5 and HMAC-SHA are used by IPSec to authenticate data

Signature Algorithms

- **RSA** (Rivest, Shamir, Adelman)
  - **Most popular and widely implemented signature algorithm**
  - **Can be used for both signatures and message encryption**
  - **Typically slower than DES for message encryption**

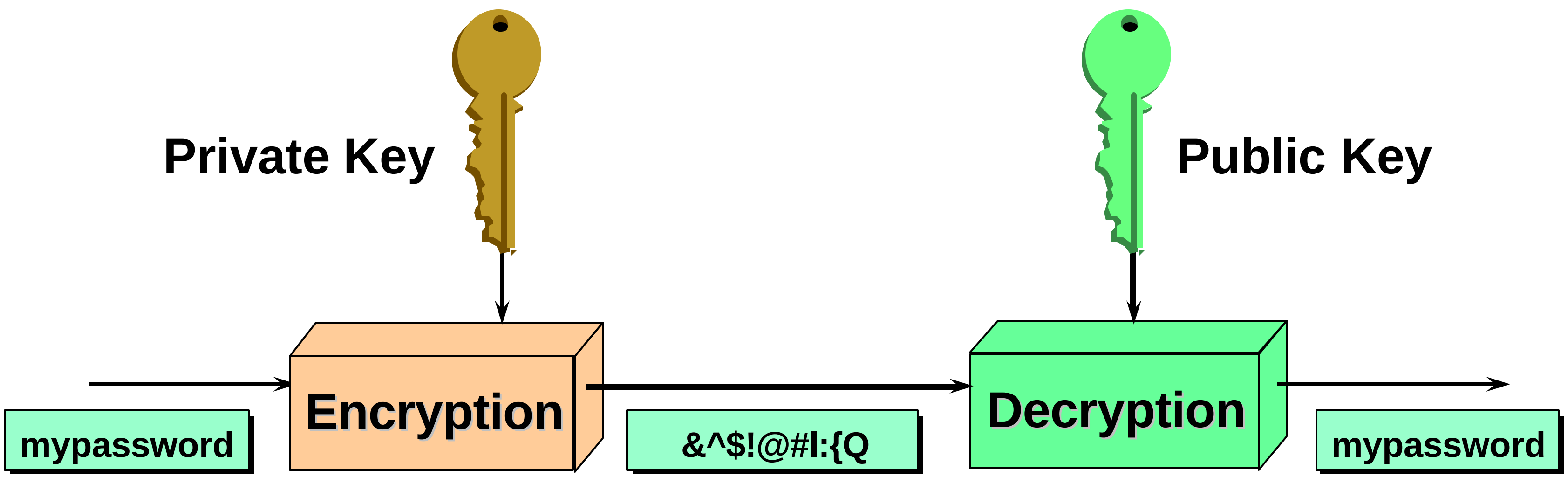
- **DSA** (Digital Signature Algorithm)
  - **Proposed by NIST (National Institute of Standards) as FIPS (Federal Information Processing Standard) digital signature standard (DSS)**
  - **Slower signature verification than RSA and 512 or 1024 bit key size**
  - **Plagued by patent infringement issues (Schnorr – expires 2008)**

Authentication and Encryption In Cisco IP Communications

Authentication and Encryption In Cisco IP Communications

- Public Key / Private Key Pair
- Certificate
- Certificate Trust List
- Transport Layer Security (TLS)
- Secure RTP (SRTP)

Public Key / Private Key Pair

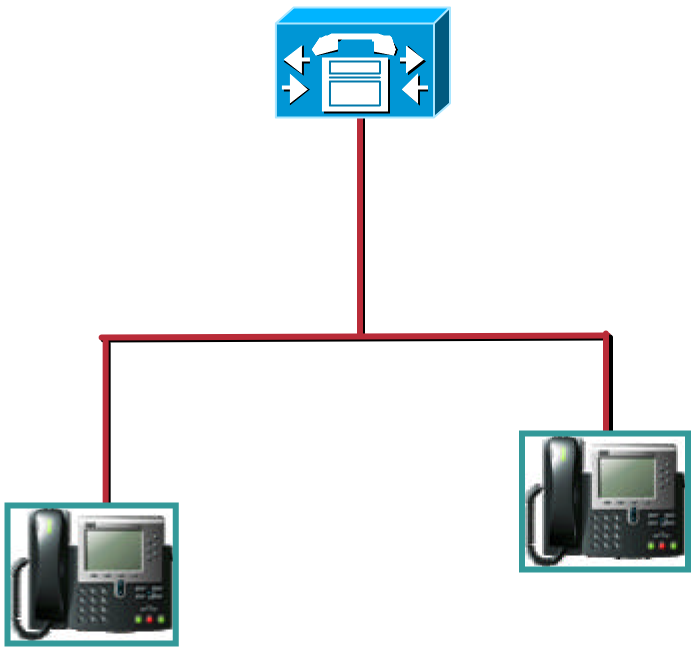


Asymmetric Key Pair

- Anything encrypted with a private key can only be decrypted by it's corresponding public key
- Anything encrypted with a public key can only be decrypted by it's corresponding private key pair
- Devices keep their private key strictly private and share their public key with all interested parties

Public Key / Private Key Pair

- Every device has a Public Key / Private Key pair
- Derived internally so Private Key never crosses the wire
- Can be 1024 or 2048 bits
- Used for identity and signatures
- Asymmetric keying is too CPU intensive for sustained encryption



Authentication and Encryption In Cisco IP Communications

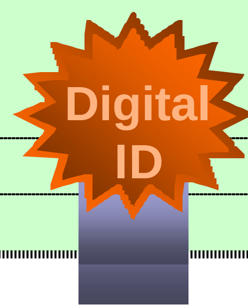
- Public Key / Private Key Pair
- Certificate
- Certificate Trust List
- Transport Layer Security (TLS)
- Secure RTP (SRTP)

X.509v3 Digital Certificate

Cisco.com

A *digital document* that establishes the *identity* of a subject and provides their <u>public encryption key</u> issued by a trusted Certificate Authority

Version	V3	Certificate Version
Serial Number	5B74 F440 66CC 70CD B972 4C5B 7E20 68D1	Certificate ID
Signature Algorithm	md5RSA	Encryption Algorithm
Issuer	CN = VeriSign Class 1 CA Individual Subscriber-Persona Not Validated OU = www.verisign.com/repository/RPA Incorp. By Ref.,LIAB.LTD(c)98 OU = VeriSign Trust Network O = VeriSign, Inc.	Certificate Authority
Valid From	Thursday, June 22, 2000 8:00:00 PM	
Valid To	Saturday, June 23, 2001 7:59:59 PM	Certificate Lifetime
Subject	E = jmccloud@cisco.com CN = Joshua McCloud OU = Digital ID Class 1 - Microsoft Full Service OU = Persona Not Validated OU = www.verisign.com/repository/RPA Incorp. by Ref.,LIAB.LTD(c)98 OU = VeriSign Trust Network O = VeriSign, Inc.	Certificate User ID
Public Key	3481 8B02 9181 01AC AF8B...	RSA 1024 bit Public Key
Thumbprint	7A52 28D0 1A0C FFD6 859A...	Digital Signature



Certificate Infrastructure Entities

Cisco.com

Certificate: Digital identity document signed by a Certificate Authority

Certificate Authority (CA): Trusted, third party responsible for authorizing certificate

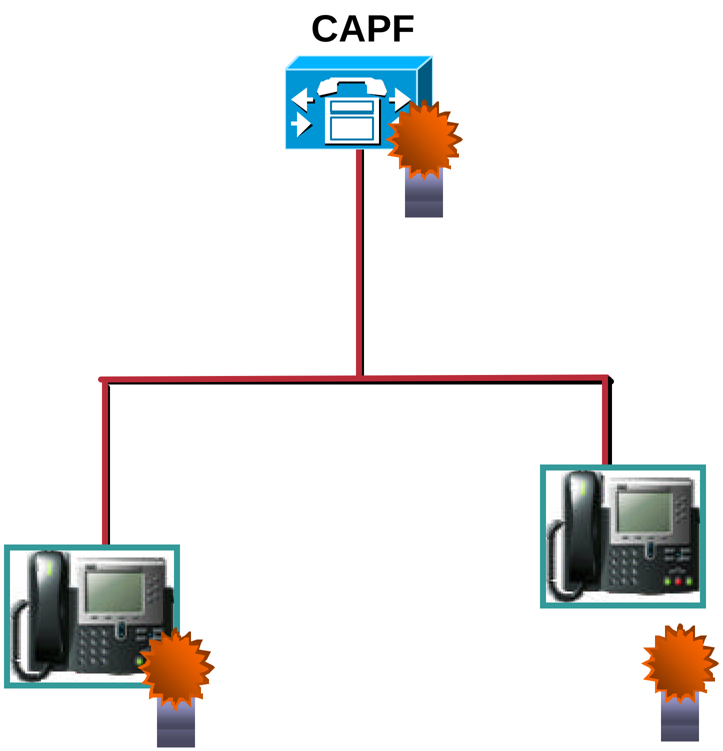
Certificate Authority Proxy Function (CAPF): Trusted party delegated authority for authorizing certificate from CA for phones

Certificate Trust List (CTL): List of trusted devices used by the certificate holder

Where do Phone Certificates Come From ?

- **Cisco – for Manufacturing Installed Certs (MIC) in 7970**
  - Installed by Cisco in non-erasable, non-volatile memory
  - Rooted in Cisco Certificate Authority
  - In 7970 and all future phone models
- **CAPF – for Locally Significant Certs (LSC) in 7940/7960**
  - Runs co-resident with Publisher
  - Installed by customer in erasable memory
  - Self-Signed Certificate Server bundled with CAPF
  - Customer's own Certificate Authority
    - Microsoft Certificate Services Manager
    - Keon from RSA

X.509v3 Certificates



- Every Device has a unique certificate
- How device advertises its Public Key
- Signed by a trusted Certificate Authority to establish validity
- Come from a variety of sources
  - CCM – Self-signed
  - 7970 – MICs installed by Cisco
  - 7940/60 – LSCs from CAPF

Authentication and Encryption In Cisco IP Communications

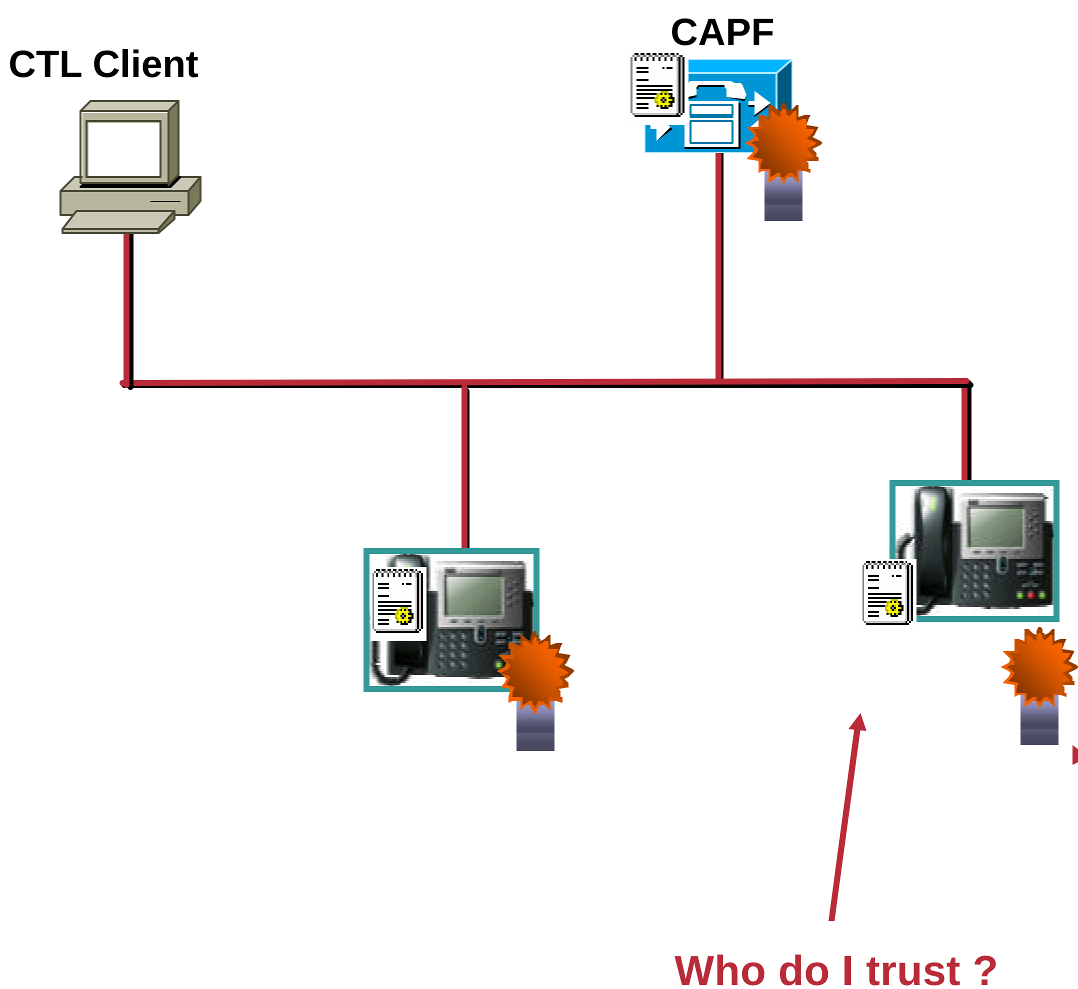
- Public Key / Private Key Pair
- Certificate
- Certificate Trust List
- Transport Layer Security (TLS)
- Secure RTP (SRTP)

Certificate Trust List

Cisco.com

- List of devices (certificates) that a device should trust on the network and the roles they perform
- Similar to the list of Trusted Root CAs in IE
- You have to trust who you're talking to – like a third-party introduction
- Phones need to trust CCM, TFTP, CAPF, etc.
  - Created by CTL Client on admin workstation
  - Signed by USB eToken
  - Loaded to phone during TFTP

Certificate Trust List



- Certificate Trust List contains list of trusted devices
- Generated by CTL Client
- Loaded into phones during TFTP download
- All phones in a cluster have the same CTL file
- CCM has a dynamic CTL file
  – Populated during TLS registration
  – Contained in OpenSSL database

Authentication and Encryption In Cisco IP Communications

- **Public Key / Private Key Pair**
- **Certificate**
- **Certificate Trust List**
- **Transport Layer Security (TLS)**
- **Secure RTP (SRTP)**

TLS: Transport Layer Security

Cisco.com

Formerly known as SSL: Secure Sockets Layer 3.0

Supports any application protocol

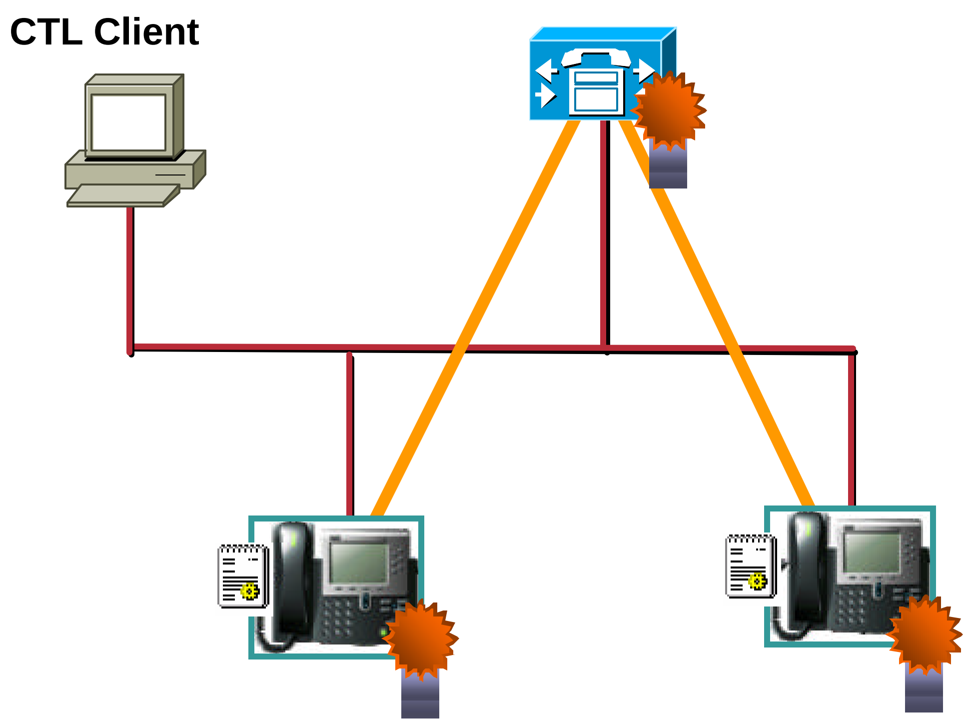
HTTP	SCCP	FTP	LDAP
TLS			
TCP			
IP			

- Bi-directional exchange of certificates establishes Identity
- HMAC provides Integrity
- Encryption offers Privacy

- Needs secure method to exchange shared secret
  - Bi-directional PKI pairs for mutual authentication
  - Trust based on certificates
  - Shared secret using RSA
- Computes Hashed Message Authentication Code (HMAC)
  - Allows MD5 or SHA1
- Conventional cryptography using shared secret
  - DES, 3DES, AES
  - RC2, RC4
  - IDEA

TLS: Transport Layer Security

- **Cisco uses TLS for secure signaling between CCM and IP phones**
  - **Bi-directional exchange of certificates for mutual authentication**
  - **RSA Signatures**
  - **Encryption of session keying material**
  - **HMAC-SHA-1 authentication tags insure packet integrity**
  - **AES-128-CBC encryption protects session keys, DTMF tones & other data**



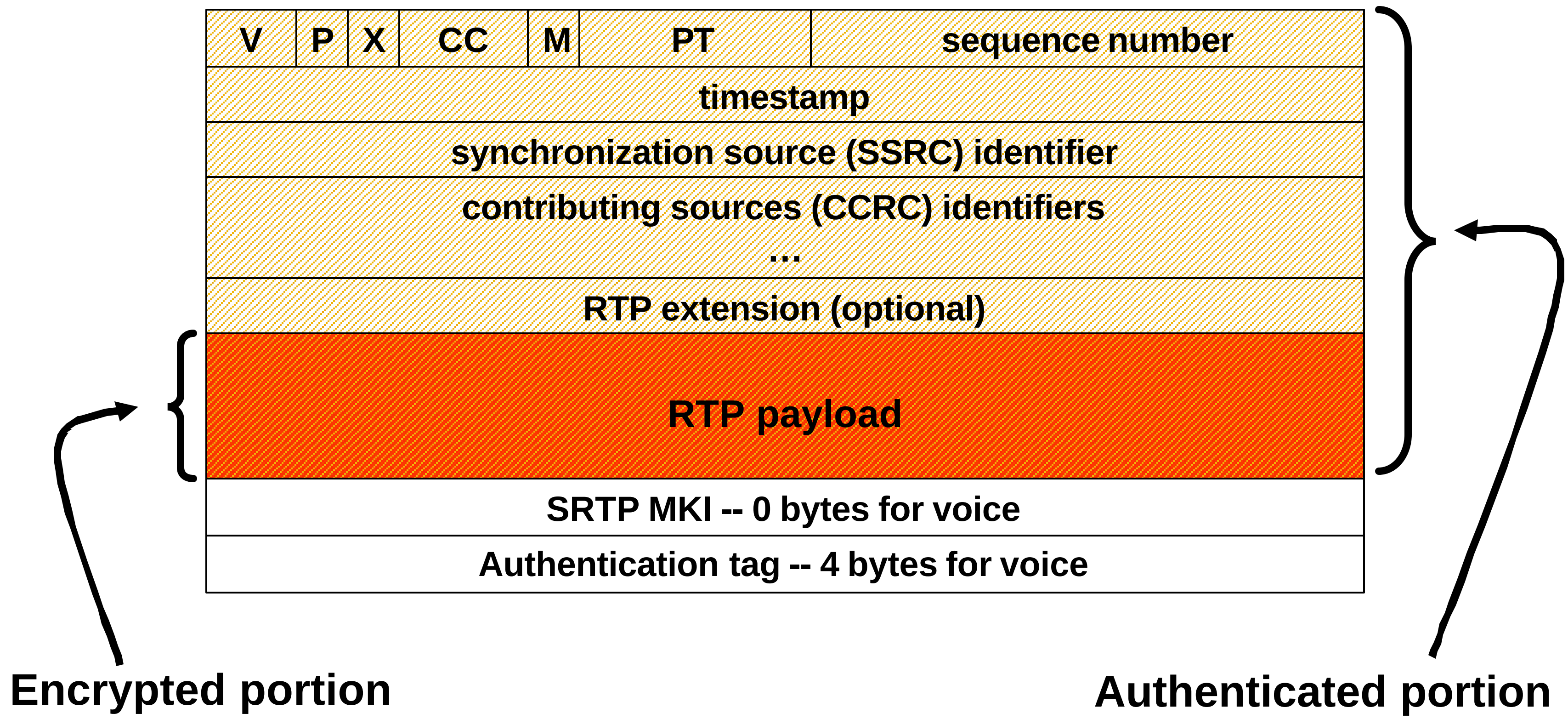
A phone running TLS has a 20-25% greater impact on CCM than a phone not running TLS

Authentication and Encryption In Cisco IP Communications

- **Public Key / Private Key Pair**
- **Certificate**
- **Certificate Trust List**
- **Transport Layer Security (TLS)**
- **Secure RTP (SRTP)**

SRTP: Secure RTP

- IETF RFC3711 for transport of secure media
- Uses AES-128 for both authentication and encryption
- High throughput, low packet expansion



SRTP Comparison with GRE and IPSec (G.729)

Cisco.com

(1) Original packet – 60 bytes

IP Hdr	UDP	RTP	Payload
20	8	12	20

(2) With SRTP – 64 byes

IP Hdr	UDP	RTP	Payload
20	8	12	24

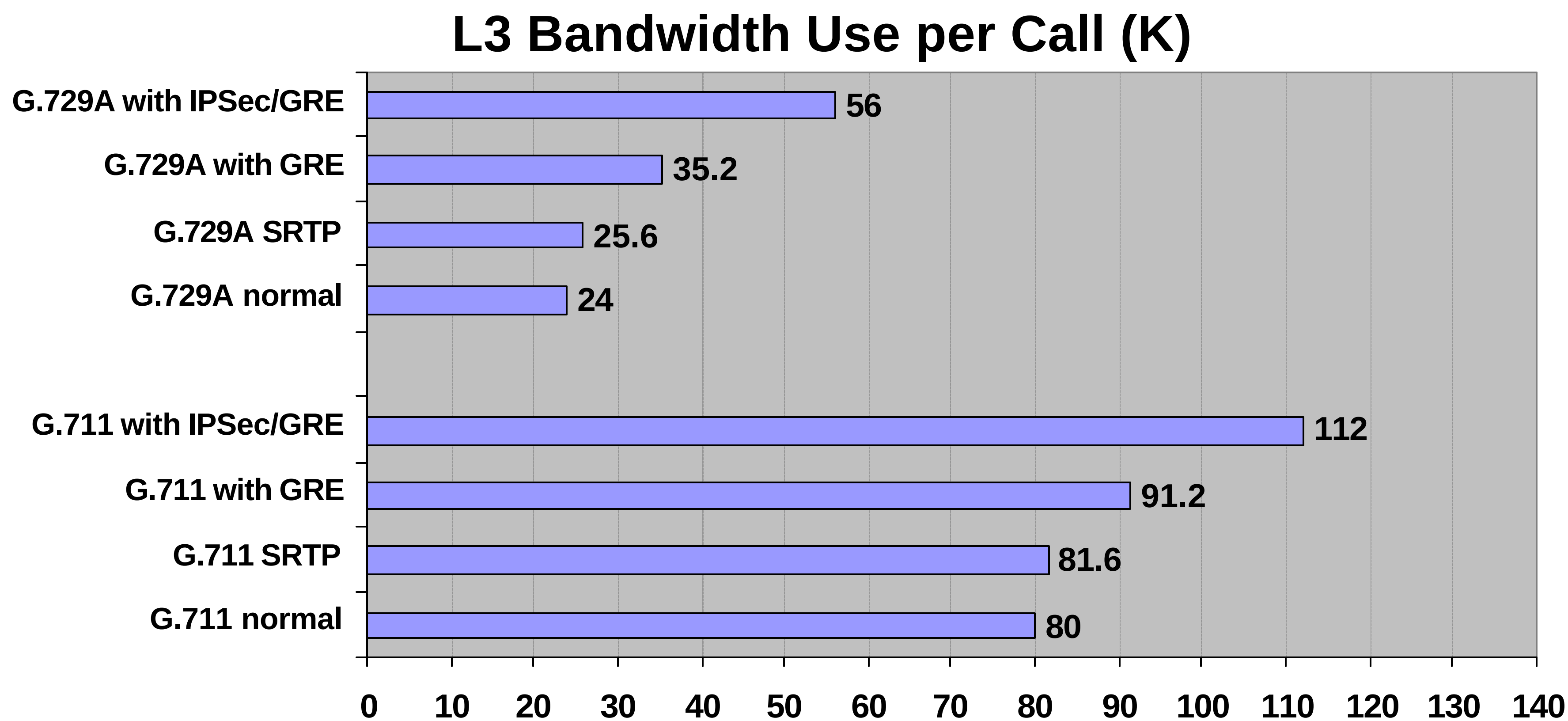
(3) With IP GRE – 84 Bytes

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

(4) IPSec ESP Tunnel Mode – 136 Bytes

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

Call Bandwidth Use



- V3PN solutions significantly bloat BW use per call, especially for G.729 calls
- SRTP offers significant BW savings, as well as e2e encryption

TI-5510 DSP Channel Capacity with SRTP

	Regular Mode	With SRTP 12.3(5th)T
Flex Complexity G.711	16 calls	10 calls
Medium Complexity	8 calls	8 calls
High Complexity	6 calls	6 calls

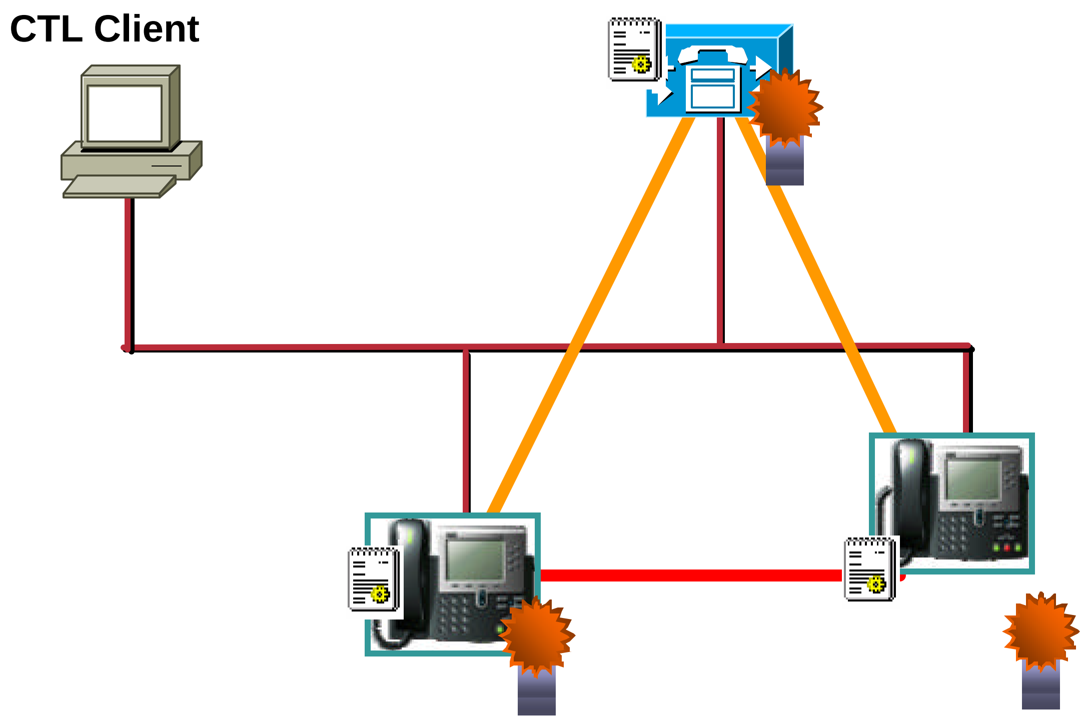
The only channel density impact is for Flex mode and all calls G.711

Scalability and Delay

- **No increase in delay**
  - Call setup delay: Key exchange is done as part of normal MGCP call setup – no extra messages introduced, i.e. no extra call setup delay
  - Voice media delay: SRTP encryption is done in the DSP, and not by the router CPU – i.e. no extra CPU for SRTP
- **Scalability**
  - SRTP encryption is in the DSPs and a DSP is available per call
  - Very scalable solution as more GWs and voice interfaces are added, more DSP power is automatically added too and no extra scalability engineering is needed
  - Scalability impacts of IPSec tunnels on the CCM servers, but the traffic in these tunnels is low (signaling only) and one tunnel per GW is needed, not one per call

SRTP: Secure RTP

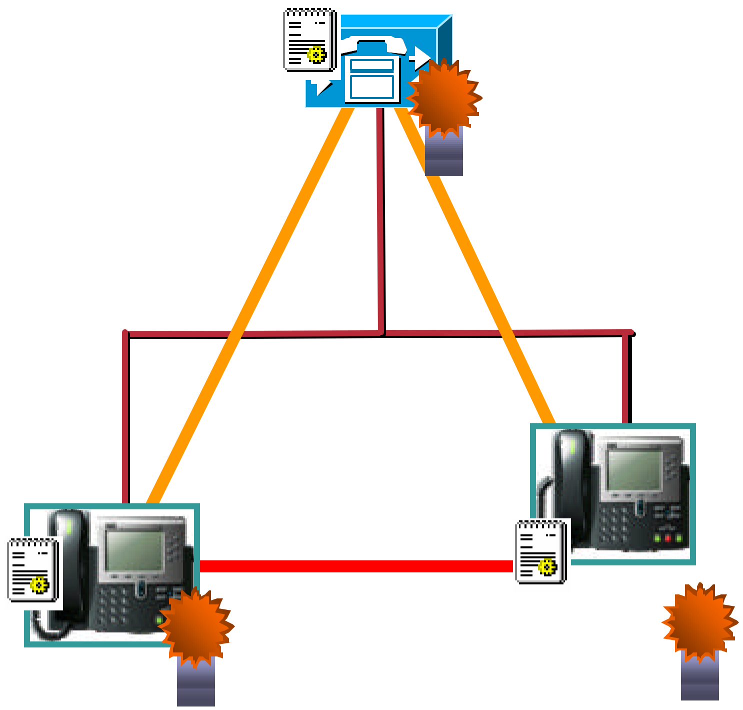
- SRTP is the transport for authenticated and encrypted media
- IETF RFC3711
- Uses HMAC-SHA-1 for authentication & AES-128-CM for encryption
- Keys derived in CCM – sent to phones over TLS
- Supported on 7940, 7960 7970, Cisco Gateways and Cisco Unity



SRTP packets add 15 microseconds to latency and are 4 bytes bigger than RTP packets

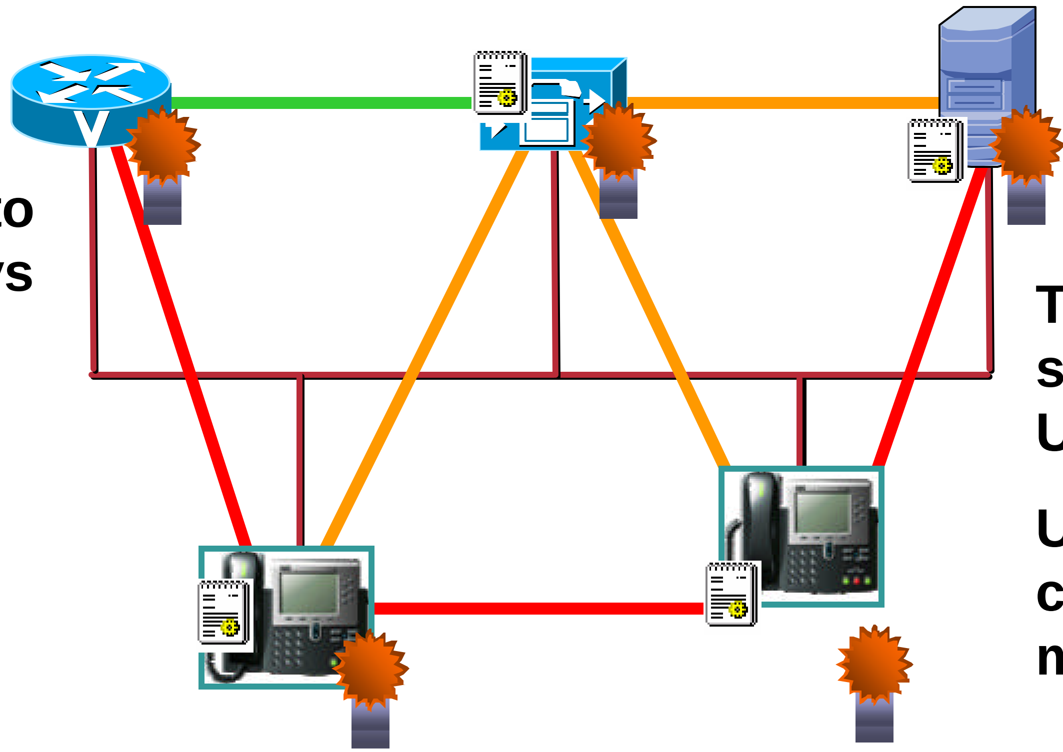
Certificate-Based Authentication and Encryption

- **Public Key / Private Key Pair**
- **X.509v3 Digital Certificate**
  - Self-Signed (CCM)
  - MIC from Cisco Mnfg (7970)
  - LSC from CAPF (7940/7960)
- **Certificate Trust List**
  - CTL Client
- **Transport Layer Security**
  - RSA Signatures
  - HMAC-SHA-1 Auth Tags
  - AES-128-CBC Encryption
- **Secure RTP**
  - HMAC-SHA-1 Auth Tags
  - AES-128-CM Encryption



Expanded Certificate-Based Authentication and Encryption in CCM 4.1

Cisco.com



IPSec & SRTP to MGCP Gateways (12.3.11T1)

- VG224
- 2600-XM
- 2691
- 2800
- 3640a
- 3660
- 3700
- 3800

* SRTP in SRST mode – Q105

TLS and SRTP supported to Unity 4.0(5)

User-Defined confidential messaging

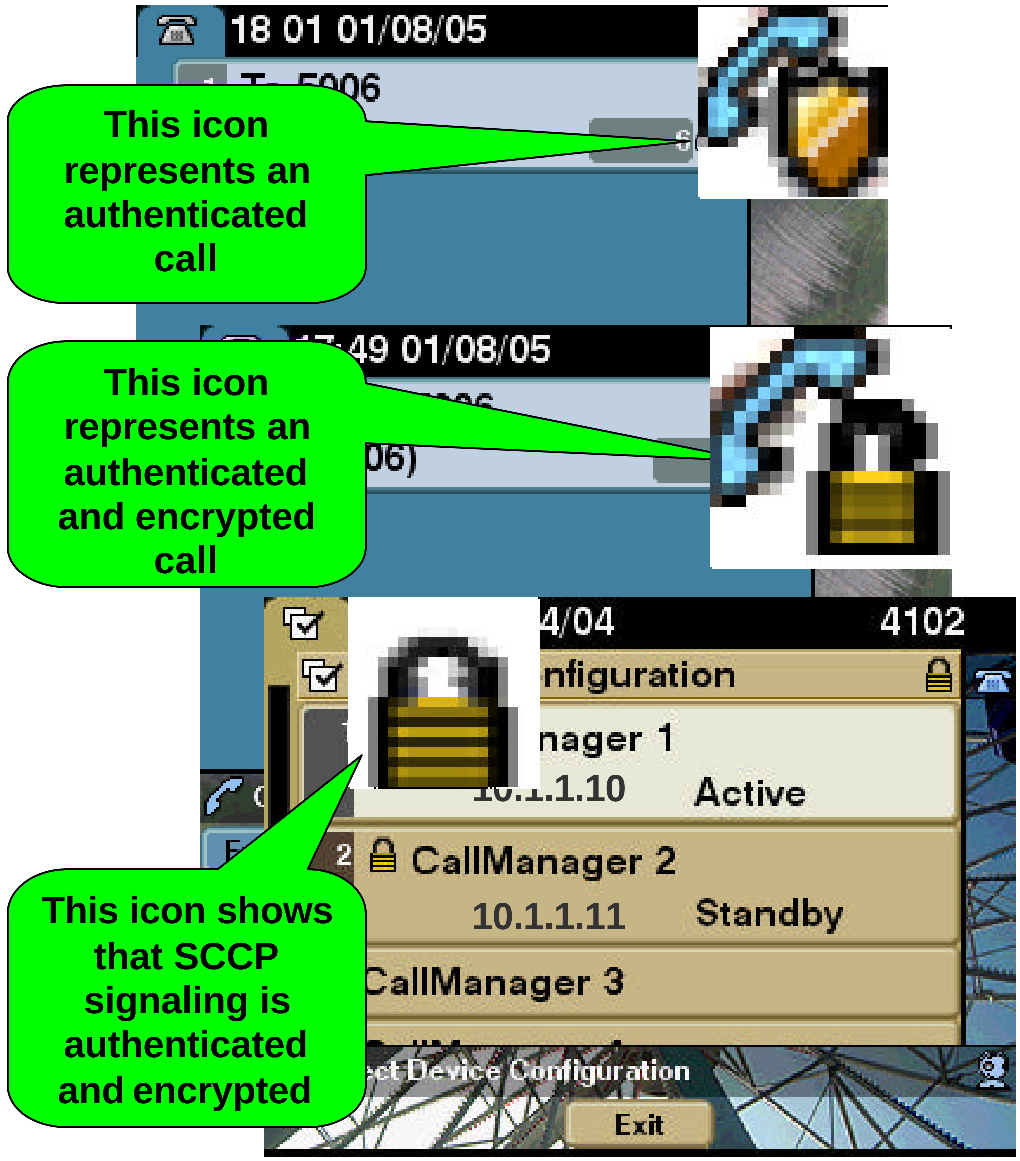
Full TLS and SRTP support in 7940 / 7960 / 7970

TLS
IPSec
SRTP

Authentication and Encryption Summary

Cisco.com

- “Device Identity” establishes mutual authentication using RSA signatures
- "Signaling Integrity" - SCCP messages authenticated using HMAC-SHA-1
- "Signaling Privacy" - SCCP message contents encrypted using AES-128-CBC
- “Media Integrity and Privacy” – SRTP packets authenticated and encrypted with AES-128-CM
- Mixed-Mode Support – CCM and phones do negotiate highest common capability
- User interface notification (via phone icon) of phone security status



Hardening the Windows Operating System

Hardening the Operating System

- **Hardened Win2K OS Shipped By Default, and downloadable from Cisco Connection Online**

  Every version gets incrementally more secure

- **Aggressive Security Patch and Hotfix Policy**
  - **Critical: Tested and posted to CCO within 24 hours**
  - **Others: Consolidated and posted once per month**
  - **New email alias tells you when new patches are available**

    (http://www.cisco.com/warp/public/779/largeent/software_patch.html)

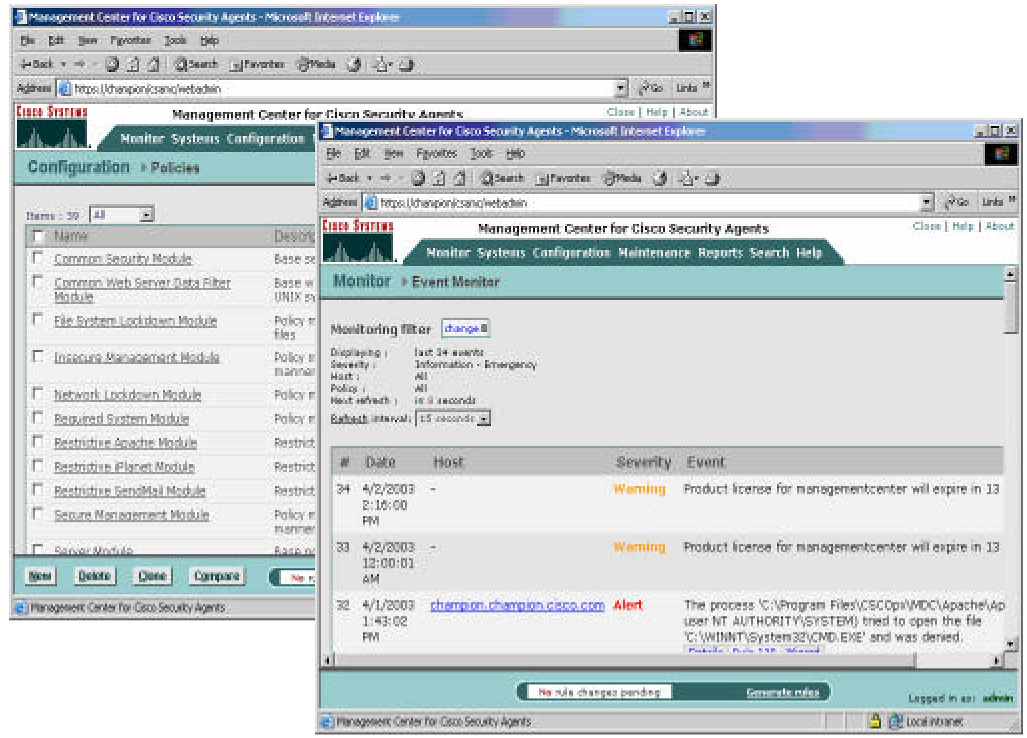
  Sasser patch was available on CCO two weeks before it hit the Internet!

- **Install McAfee 7.1, Symantec 8.1, or Trend Micro ServerProtect5 Anti-Virus Protection**

  Disable heuristic scanning – if not - the web pages may not work!

Host-Based Intrusion Prevention
Cisco Security Agent

- **Available for all telephony applications**
  - **Headless Bundled**
  - **Managed Optional**
- **Policy-Based, not signature based**
- **Zero Updates**
- **“Day Zero” support**
- **Centrally administered, with distributed, autonomous policy enforcement**
- **Effective against existing & previously unseen attacks**
- **Stopped Slammer, nimda & code red sight unseen with out-of-the-box policies**



CSA Server Protection:

- **Host-based Intrusion Protection**
- **Buffer Overflow Protection**
- **Network Worm Protection**
- **Operating System Hardening**
- **Web Server Protection**
- **Security for other applications**

Optional OS Security Script

Cisco.com

- **Additional password restrictions, event logs, NTLM auth., registry settings, file & IIS ACLs, deletes un-needed files & folders, etc.**
- **C:\Utils\SecurityTemplates directory**

  CCM-OS-OptionalSecurity.cmd

  CCM-OS-OptionalSecurity-Readme.doc

- **C:\Utils directory**

  Before-CallManager-Upgrade.htm

  IPSec-W2KSQL-Readme.htm

- **Part of OS Build 2.6 – April 2004**
- **Can be run on CallManager 3.3(2) or greater**
- **Not supported on other applications.**

Manual Security Settings

- Create individual users placed in Administrators group
- Rename Administrator – Must be named back to administrator prior to upgrades
- Create a decoy Administrator account ?
- Create an Auditors group
  - Give Auditors very little privilege, but full access to logs
  - Give Administrators read-only access to logs
- Add Screensaver, CMOS & iLO Passwords
  - Disable iLO if not used
- Remove Everyone group from Share permissions
- Scripted IP Security Filter – Blocks fixed Windows & SQL ports
- Details in the OptionalSecurity Readme

Protect Windows Against Common Exploits

Cisco.com

Most XML apps go to the Internet to get data

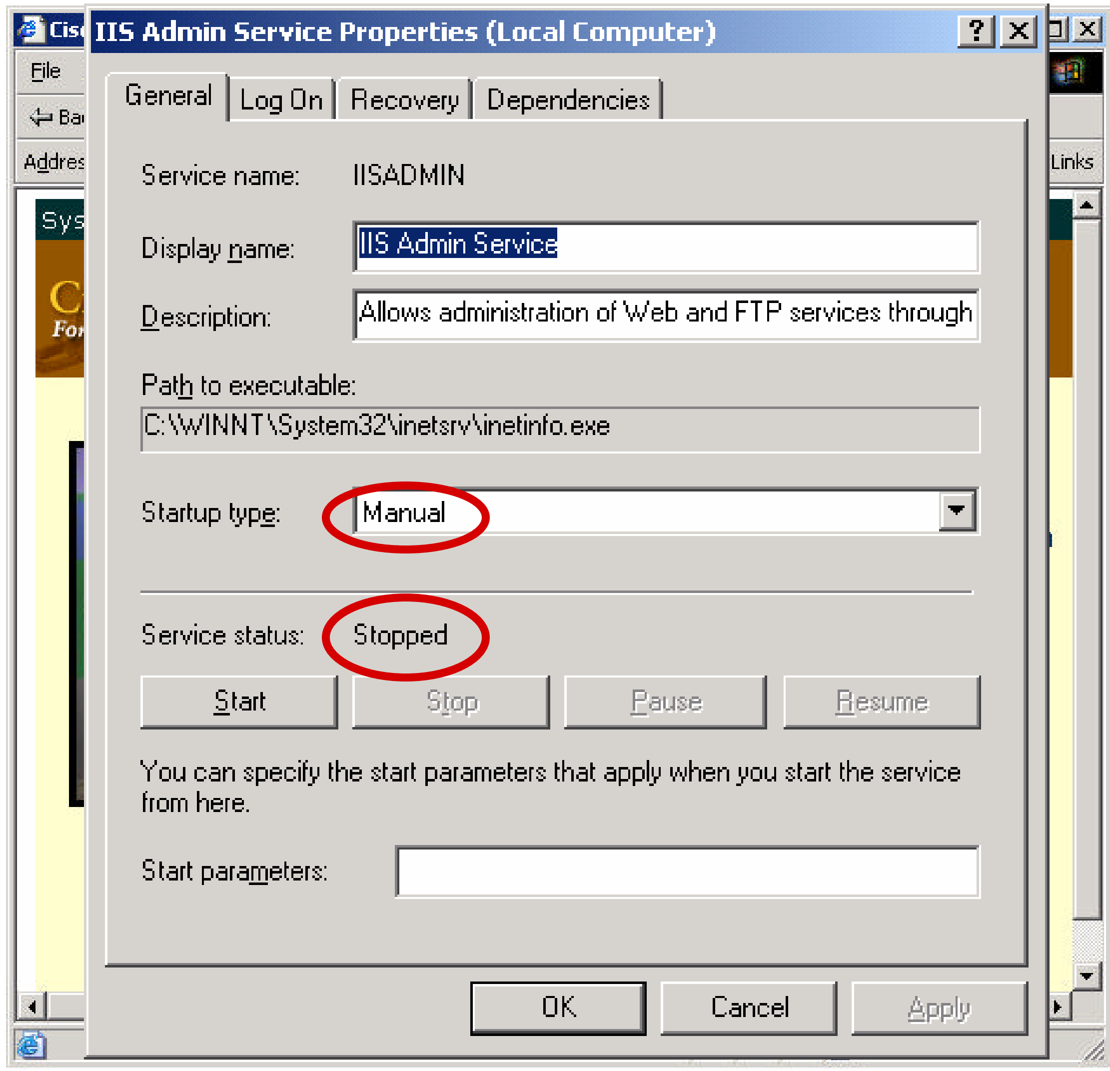
- **Offload XML to dedicated server**

DHCP can be served from the infrastructure

- **Deploy DHCP close to the endpoints**

80% of attacks against Windows are targeted at IIS !!!

- **Turn off IIS on the Subscribers - Set to Manual for Installer**
- **Change Script Error Message setting to not detailed**



Multi-Level Admin (MLA)

Cisco.com

– **Users are added to LDAP directory and assigned to "User Groups".**
– **User Groups are then given access to "Functional Groups".**
– **Functional Groups have access to individual pages**

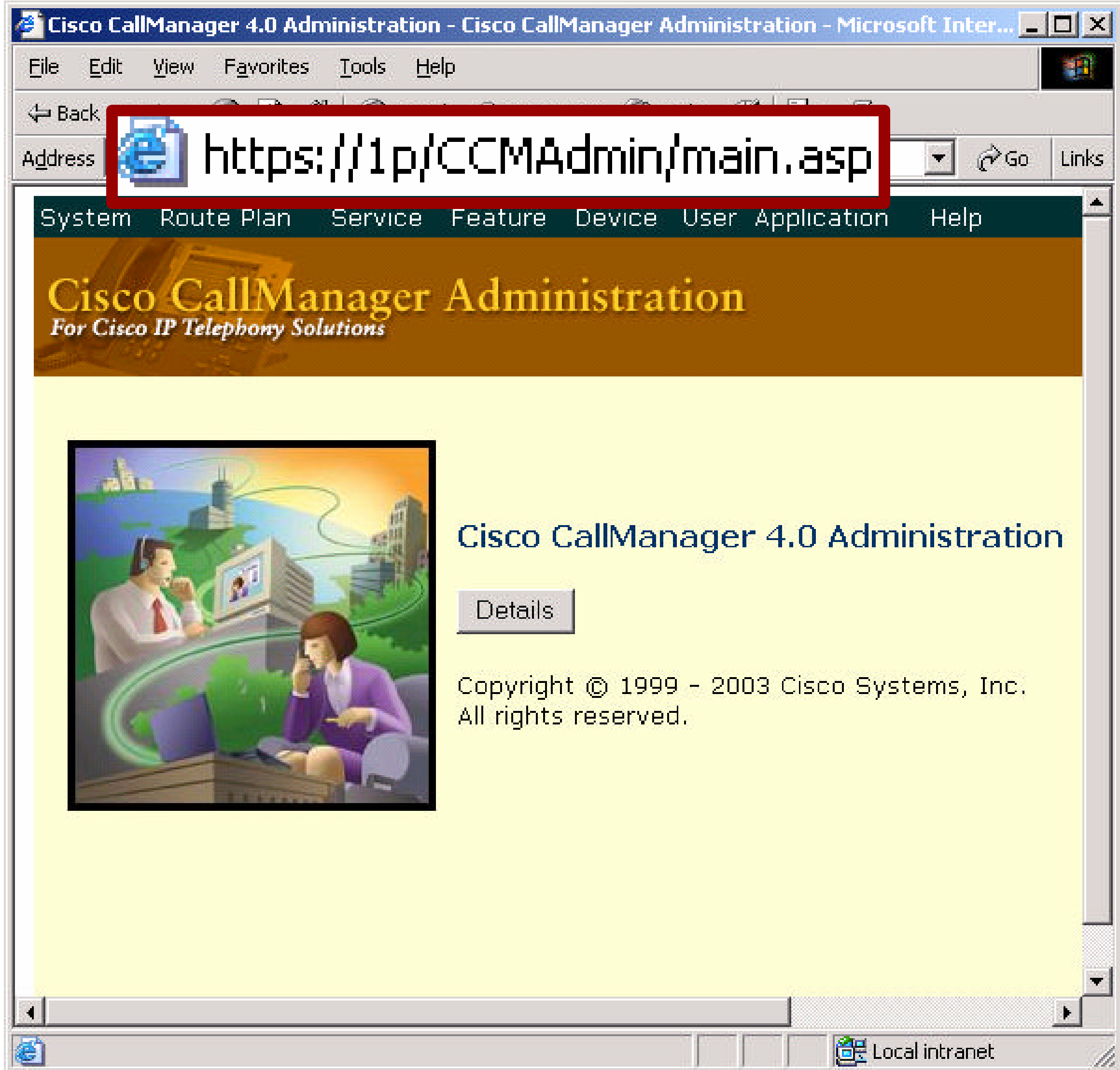
Secure Remote Access

New in CCM 4.1

All CallManager Administrator and User Webpages over HTTPS

- **Usernames and Passwords**
- **Configuration changes**
- **Serviceability**
- **Speed dials, call forwarding**

On by default – Not configurable



Multi-Level Admin (MLA)

New in CallManager 4.1

- **LDAP lookups to DC Directory and AD Plug-in over SSL (SLDAP)**

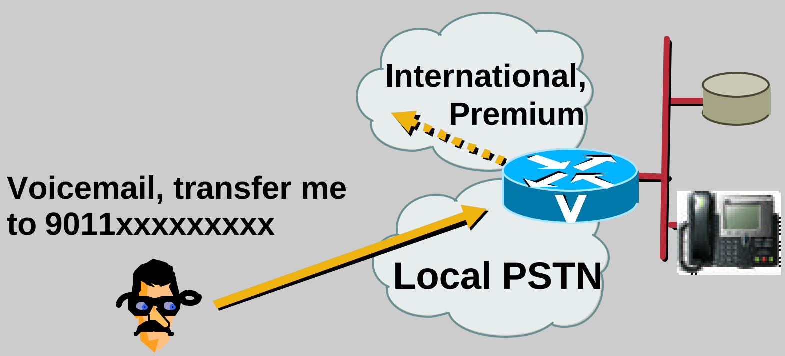
On by default – Not configurable

- **Users are added to LDAP directory and assigned to "User Groups".**
- **User Groups are then given access to "Functional Groups".**
- **Functional Groups have access to individual pages**

CallManager
Toll Fraud Prevention

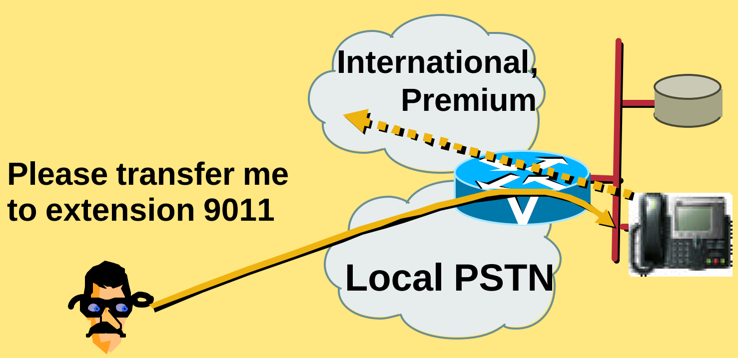
Exploits of Toll Fraud

Toll Fraud 1: Transfer from Voicemail

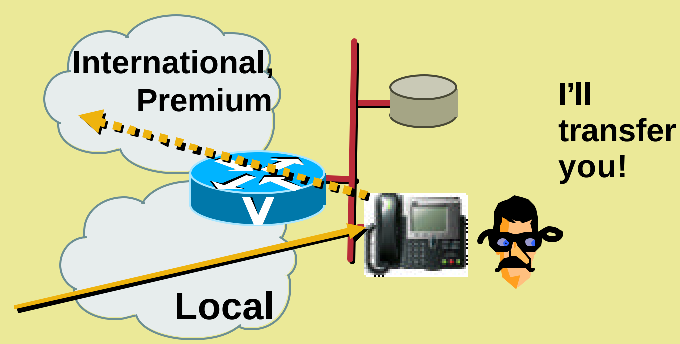


Toll Fraud 2: Call Forward All

Toll Fraud 3: Social Engineering



Toll Fraud 4: Inside Facilitators

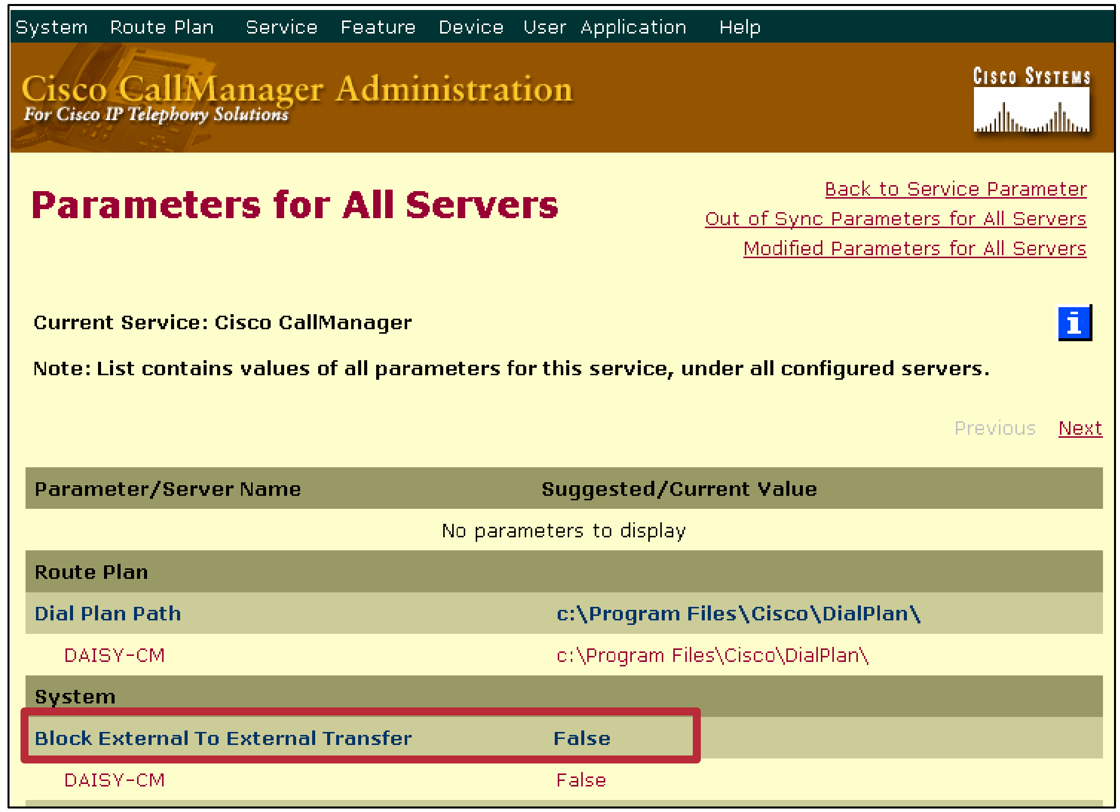


Prevent Authenticated User Toll Fraud

- Essentially a dial plan control exercise
  - May not be a need to allow CFALL to Bermuda…
  - Call Forward All CSS controls these exploits
- Exploits of Voicemail (similar to Call Forward All)
  - Restricted CSS on VM ports to on-net destinations only

Prevent External Transfer

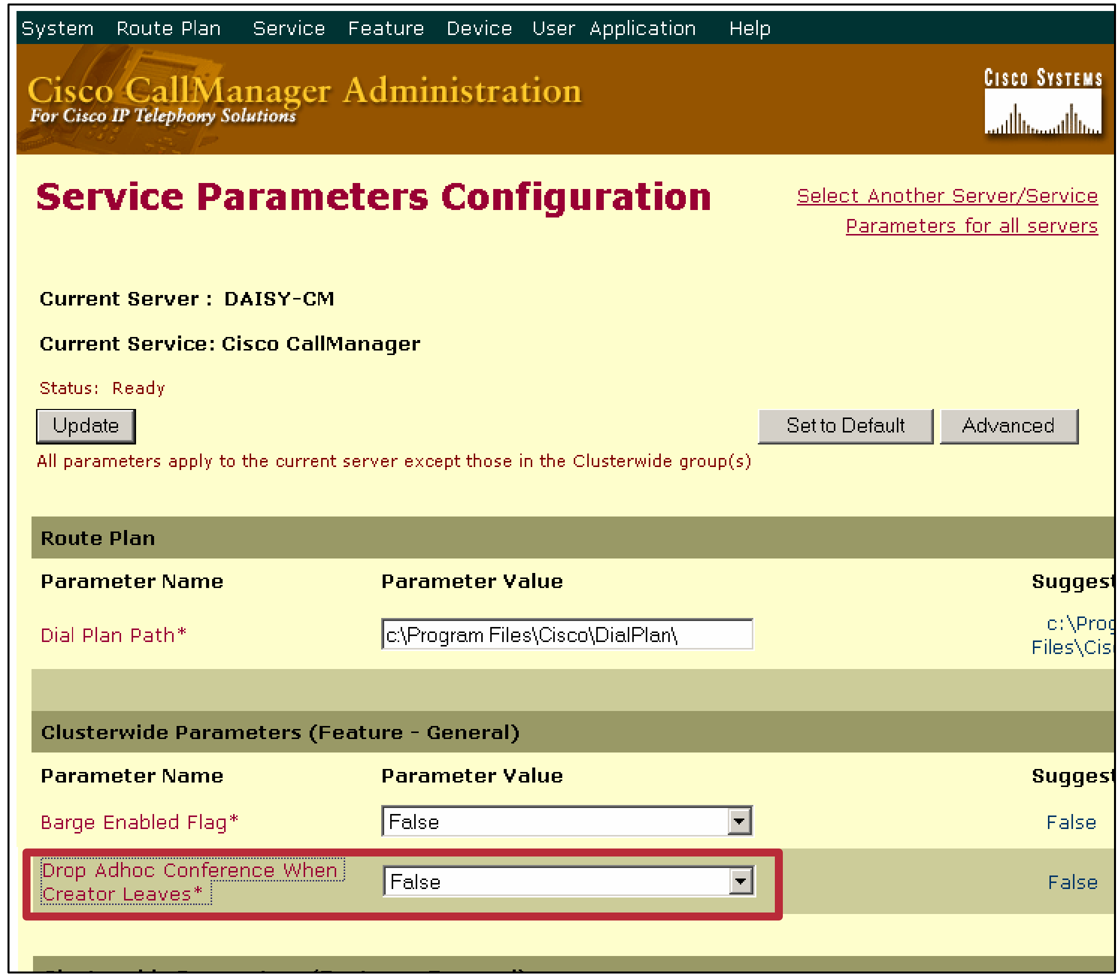
- **Prevents users from transfering calls from one external device to another external device**
- **Disabled by default**
- **Internal devices:**
  - **SCCP (StationD, NCallStationD)**
  - **MGCP FXS (MGCPStationD)**
  - **H323 Phone (NetMeeting)**
  - **Conference Bridge (UnicastBridgeControl)**
- **External devices:**
  - **H323 Gateway device**
  - **MGCP FXO trunk**
  - **MGCP E1/E1 trunk**
  - **Inter cluster trunk**



In CCM 3.3(4)

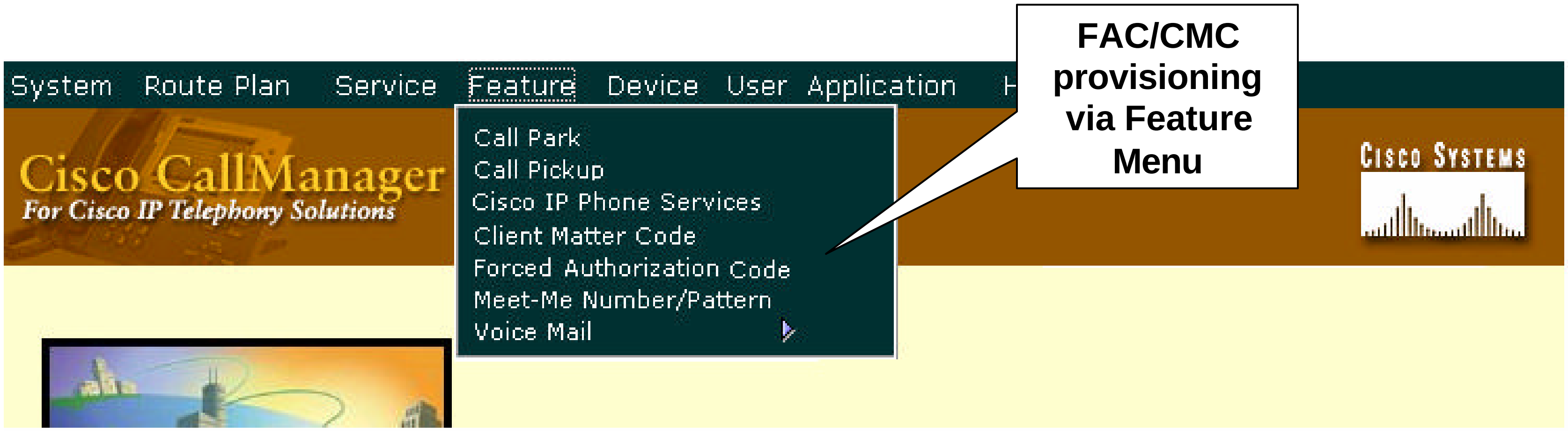
Drop Conference Call When Originator Hangs Up

- Specifies whether to drop a conference when the originator leaves
- Default false
- If changed to True and the originator hangs up, the conference will be dropped
- When the originator transfers, redirects or parks the call and the retrieving party hangs up, the conference will be dropped



In CCM 3.3(4)

Forced Authorization Codes and Client Matter Codes



- **Allows a system administrator to force all calls going to a specific route pattern to enter an authorization code before the call is extended**
- **Prevents an unauthorized user from making toll calls**
- **Allows for billing and tracking of calls made**

In CCM 3.3(4)

Filter Toll Numbers from Dial Plan

- Many commonly exploited area codes
- The following list is just a start and may not apply to your organization…

Research the problem for your particular area

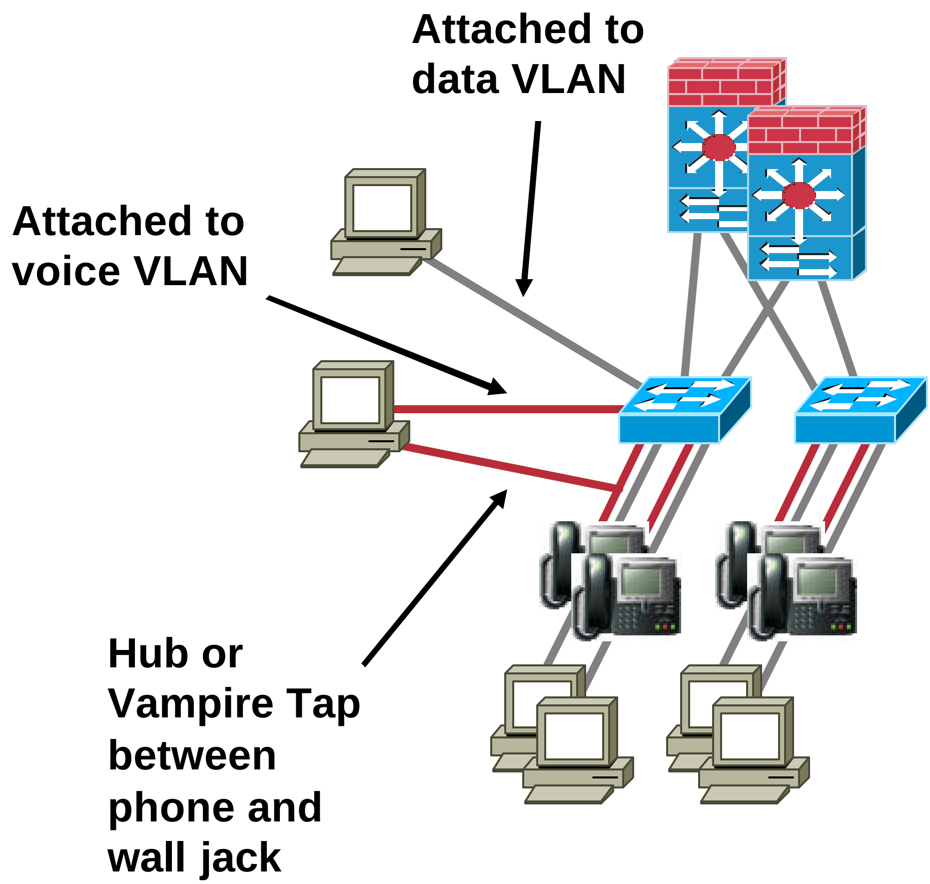
Country	Area Code	Blocked CM Pattern
Bahamas	242	9.1242xxxxxxx
Anguilla	264	9.1264xxxxxxx
Antigua/ Barbuda	268	9.1268xxxxxxx
Barbados	246	9.1246xxxxxxx
Bermuda	441	9.1441xxxxxxx
British Virgin Is	284	9.1284xxxxxxx
Cayman Islands	345	9.1345xxxxxxx
Dominica	767	9.1767xxxxxxx
Dominican Repub	809	9.1809xxxxxxx
Grenada	473	9.1473xxxxxxx

Jamaica	876	9.1876xxxxxxx
Montserrat	664	9.1664xxxxxxx
Puerto Rico	787	9.1787xxxxxxx
St. Kitts & Nevis	869	9.1869xxxxxxx
St. Lucia	758	9.1758xxxxxxx
St. Vincent & the Grenadines	784	9.1784xxxxxxx
Toll Charge	900 976	9.1900xxxxxxx 9.1976xxxxxxx
Trinidad & Tobago	868	9.1868xxxxxxx
Turks & Caicos Is	649	9.1649xxxxxxx
U.S. Virgin Islands	340	9.1242xxxxxxx

Summary

Mitigating Attacks Against Endpoints

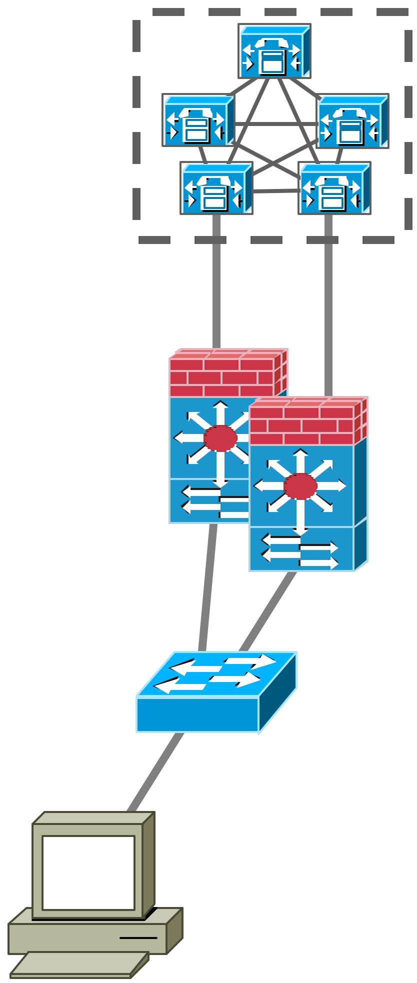
- Blocking PC access to voice VLAN stops eavesdropping attacks (VOMIT)
- DAI & Source Guard prevent man-in-the-middle attacks or traffic interception (ettercap, dsniff)
- VACLs stop directed TCP attacks
- DHCP Snooping stops DHCP spoofing and starvation attacks
- Signed firmware and config files prevent security features from being subverted
- Certificates disallow rogue CCM and phone insertion
- Encryption prevents media interpretation (if intercepted)



Mitigating Attacks Against Servers

Cisco.com

- FW, ACL & VACL prevent targeted TCP and UDP attacks & port scans
- Authentication Proxy limits access to vulnerable ports at L3
- Rate limiting prevents DoS and DDoS attacks on signaling ports to servers
- Common Windows exploits thwarted by hardened OS
- Targeted and anonymous illicit behavior stopped by CSA



How Do You Secure Your Voice Network?

	Open	Better	Best
Isolate Servers	Open	ACLs	Firewalls & Rate Limiting
Protect the OS	Open	CSA / AV / Patches / Manual Settings	Optional Script / Managed CSA
Remote Administration	Open	Authentication Proxy	Out-of-Band Management
Phone Hardening	Open	Signed Images & L1/L2 Toggles	Authentication & Encryption
Network Connectivity	Open	VACLs Ignore GARP	DHCP Snooping, DAI, ISG
Forensic Information	Open	syslog	NIDS / VMS / CWSIM

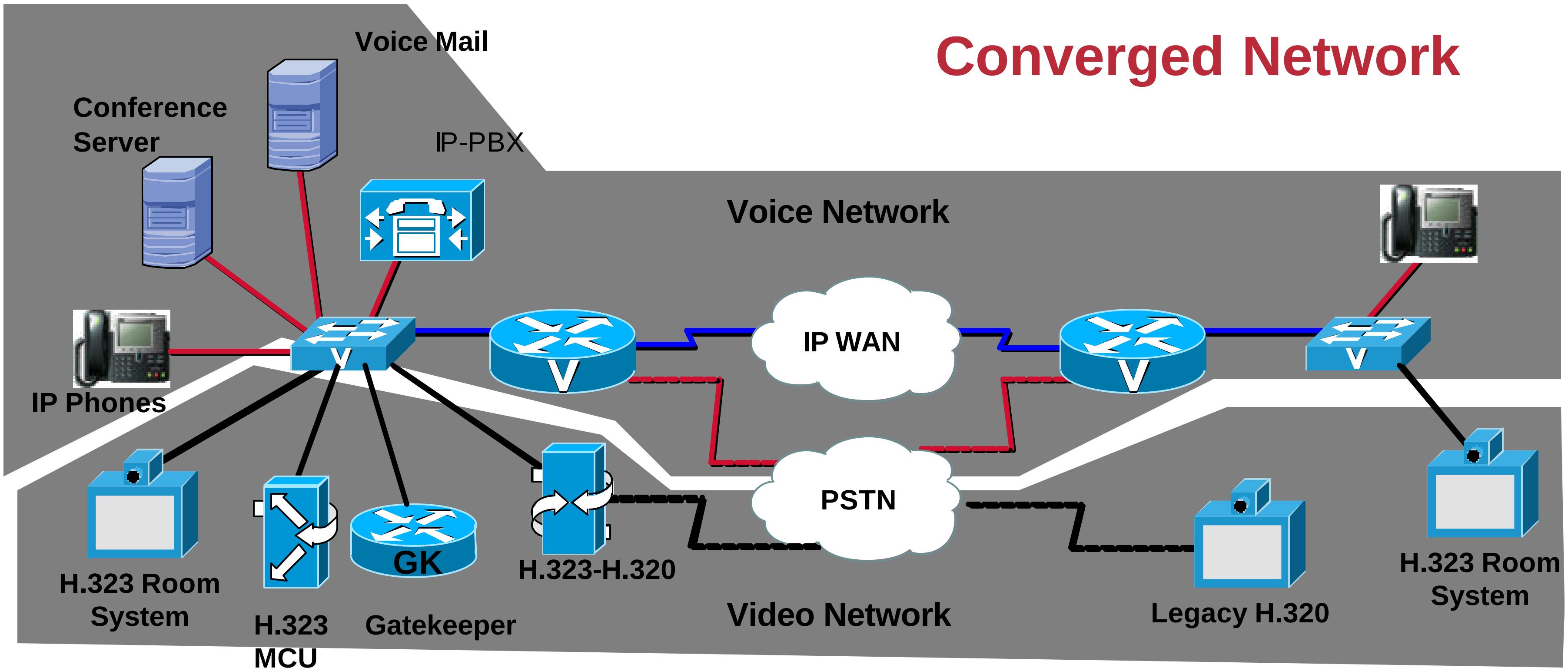
It all depends on your situation

Telephony Infrastructure Agenda (2/2)

Cisco.com

- Call Admission Control
- Survivable Remote Site Telephony
- Call Manager Express
- Dial Plan
- Voice Mail Integration
- Security
- Video Telephony
- Management
- LDAP Directories

Separate IP Voice and Video Networks



Converged Voice and Video Networks

Video

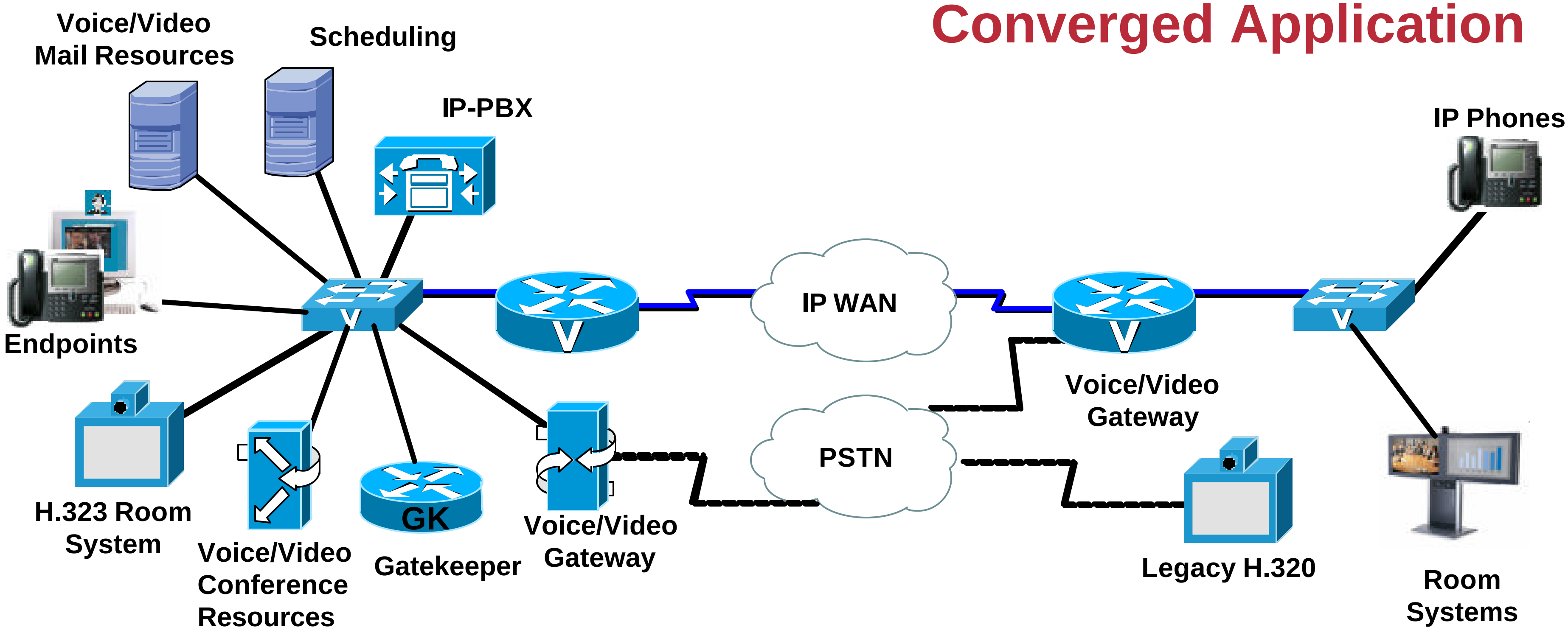
- Dial Plan Administration: Gatekeeper
- PSTN Access: H.320 Gateway
- Conferencing: Video MCU

Voice

- Dial Plan Administration: IP-PBX
- PSTN Access: Voice gateways
- Conferencing: Audio MCU

IP Video Telephony

Converged Application



Voice/Video Telephony

- **Dial Plan Administration: IP-PBX**
- **PSTN Access: Common Gateway Platform**
- **Conferencing: Common Platform**

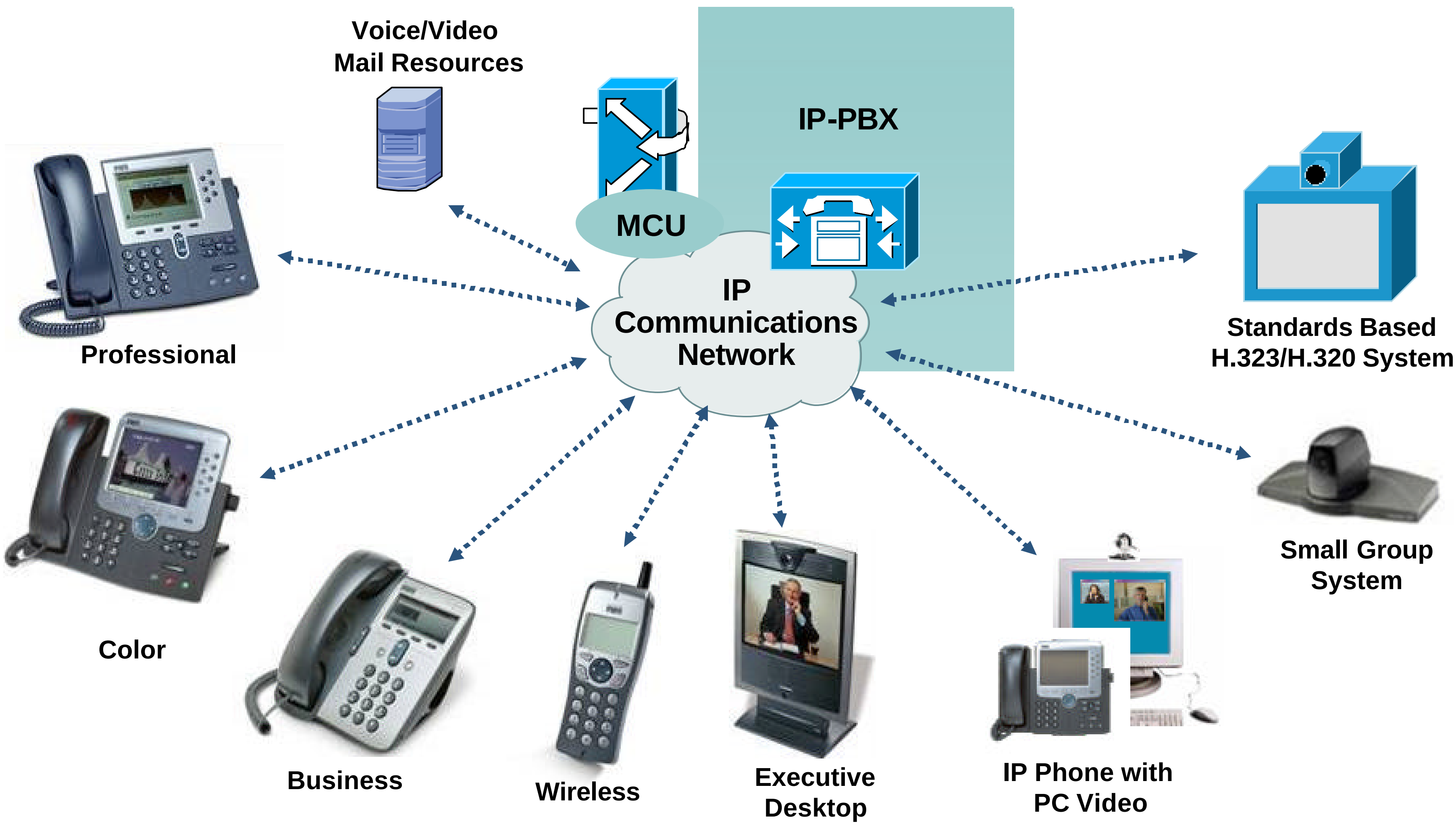
Why Is Video Telephony Different Than Videoconferencing?

Application Layer Integration

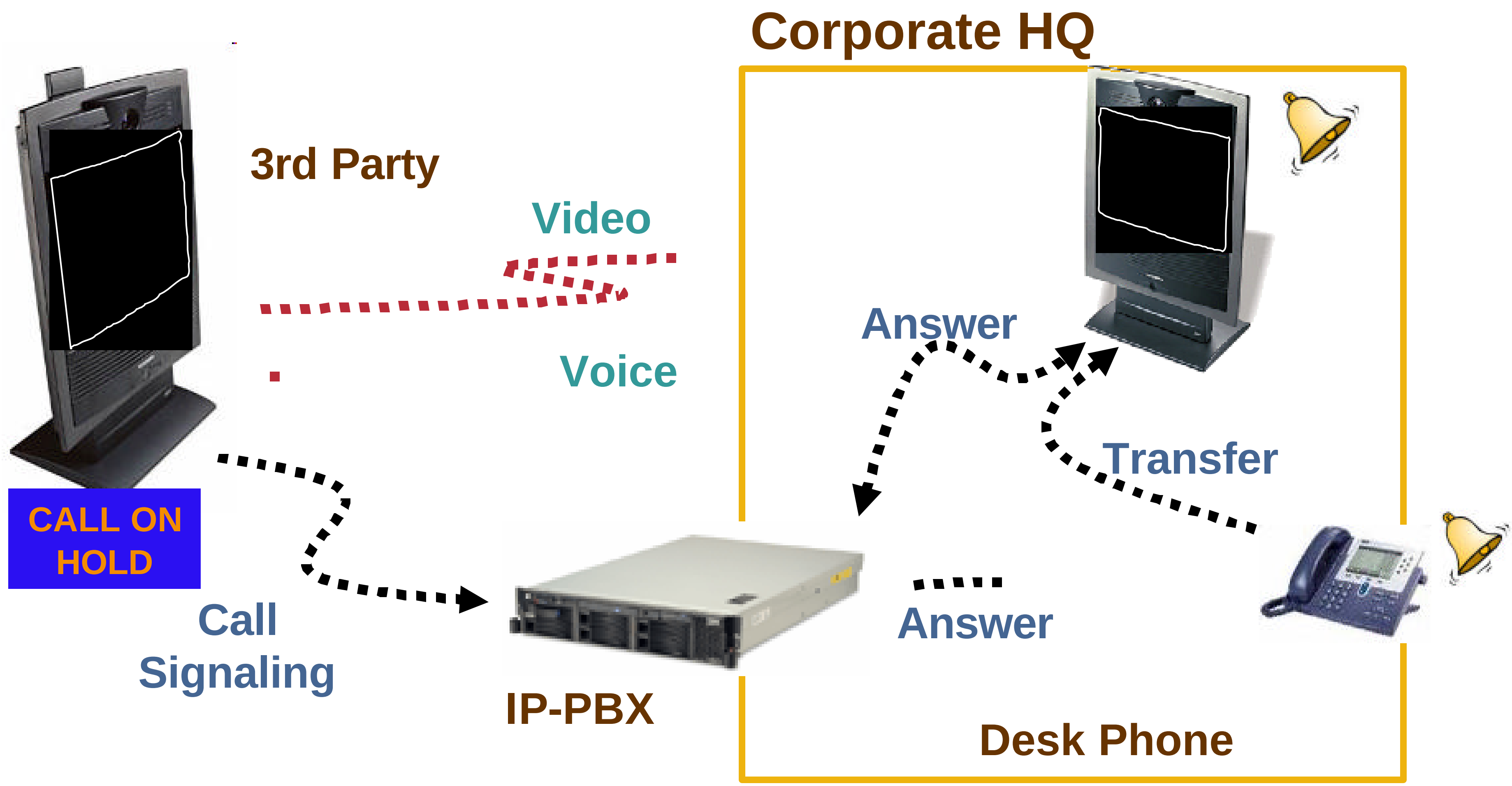
- Common Call Control
- Common Bridging Resources
- Common Gateway Resources
- Common Network Services
  - Voice/Video Mail
- Common Features/Experience
  - Conference, transfer, park, CFW

Allows Ease of Use Through Unified Experience
Leverages Infrastructure and Tools Allowing Efficiencies in Scale

Elements of IP Video Telephony

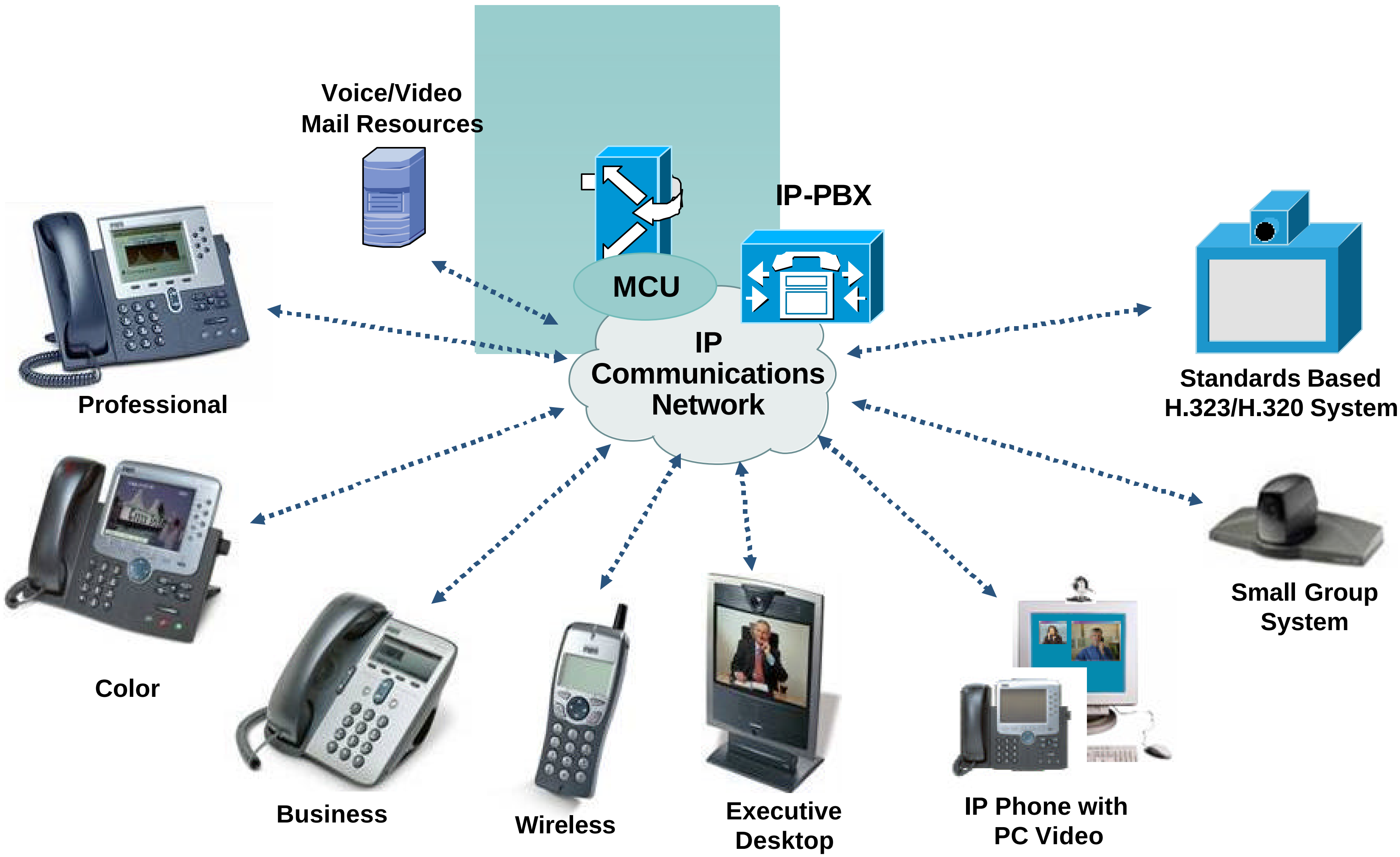


User Experience: Transfer



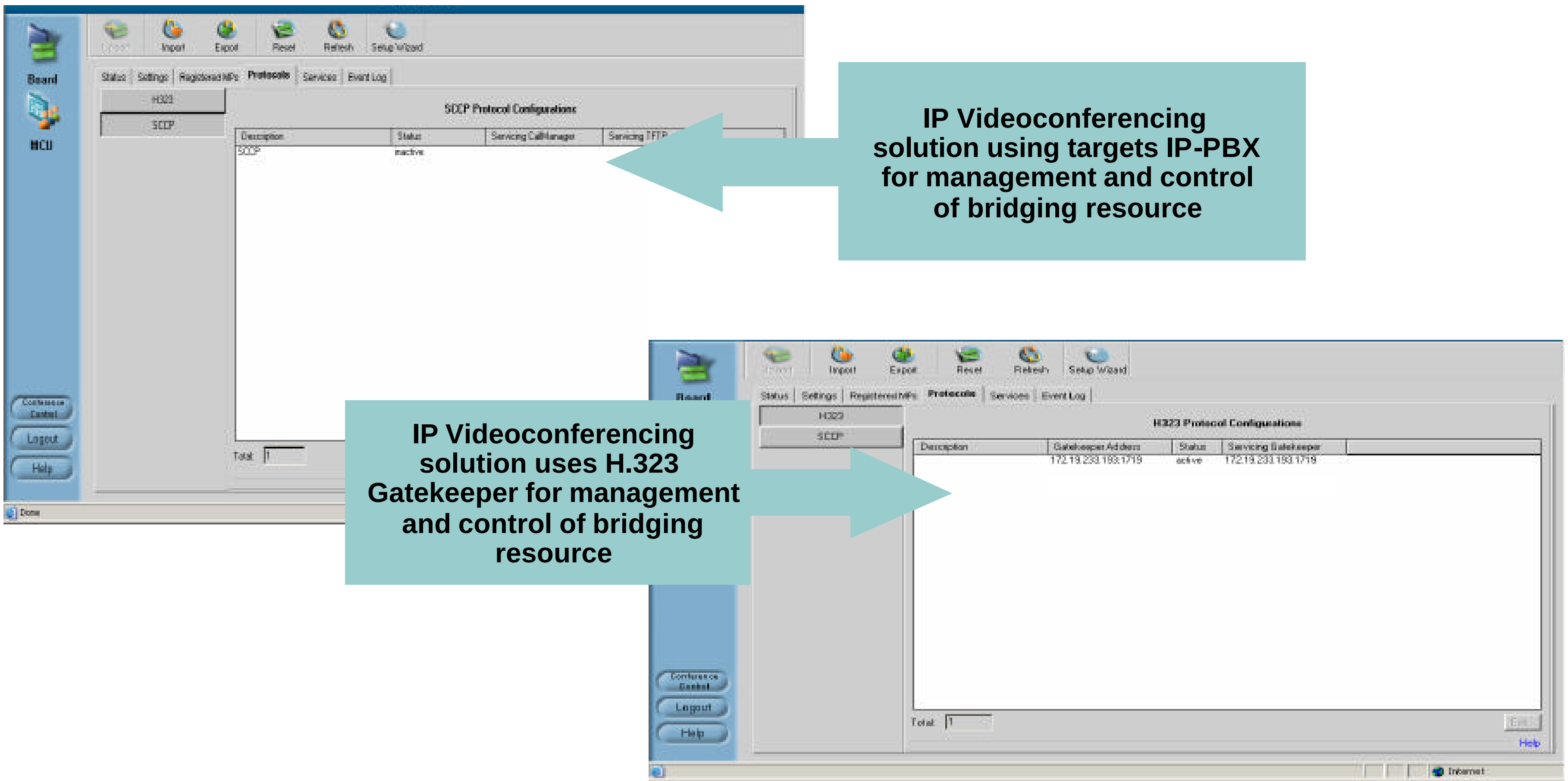
Elements of IP Video Telephony

Cisco.com



IP-PBX vs. H.323 Gatekeeper Control

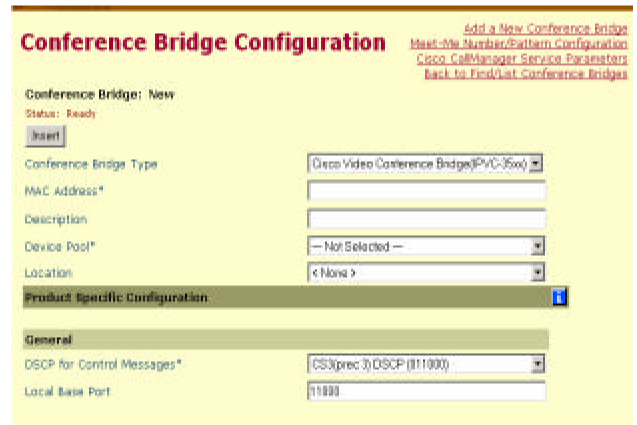
Cisco.com

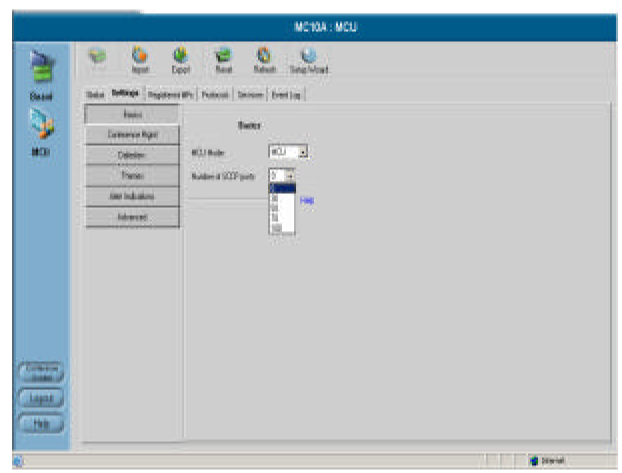


Multipoint Conference Unit

Cisco.com

- **IP-PBX has direct control of video MCU resource**
- **Configured in the IP-PBX as a Conferencing Resource**
- **Identify Media Resource Group (MRG) will help define endpoint video capabilities**
- **Automatically invoked when a video-capable device hits the conference soft key**
    - **Allows additional participants to be added to the conference**
- **Enables ad-hoc videoconferencing**





How Is “Ad-Hoc” Videoconferencing Enabled?

- Allows one to create point-point calls then seamlessly expand into videoconference format
- Same video telephony experience through soft key:

Confr

In Call Feature

- Point to Point call
- To add participant
- Push ‘Confr’ button
- Get dial tone
- Dial participant’s number

(repeat as needed)

MeetMe

Pre Call Feature

Pick up phone
- Push ‘Meet Me’ button
- Enter assigned number
- Notify participants via IM, e-mail, phone, etc.
- Everyone dials in

(Max 64 participants)

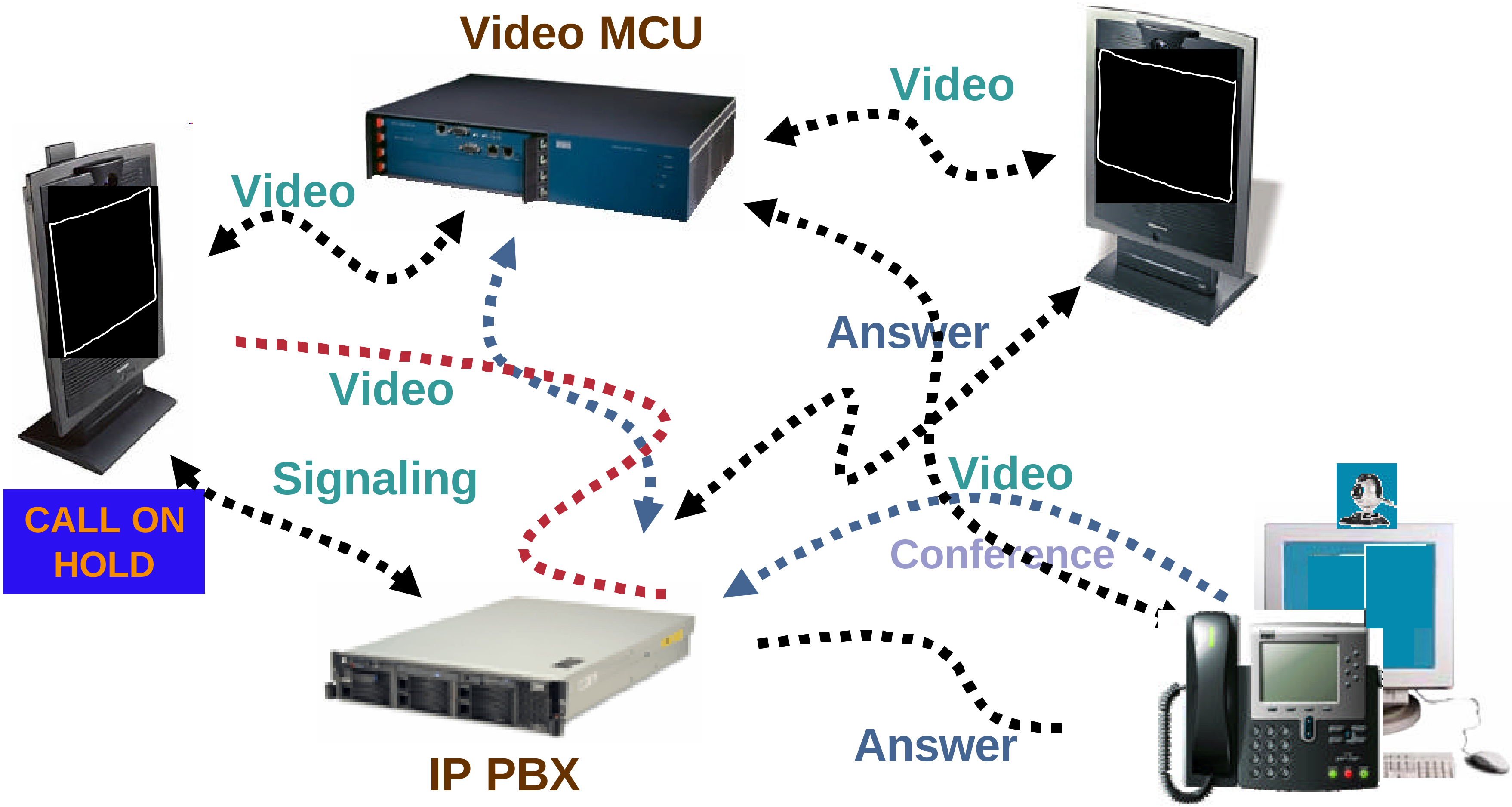
Join

In Call Feature

- Point to Point call
- Receive incoming call
- Place first call on hold
- Pickup second call
- Press ‘Join’ button
- Incoming caller joins existing call

User Experience: Ad-Hoc Conferencing

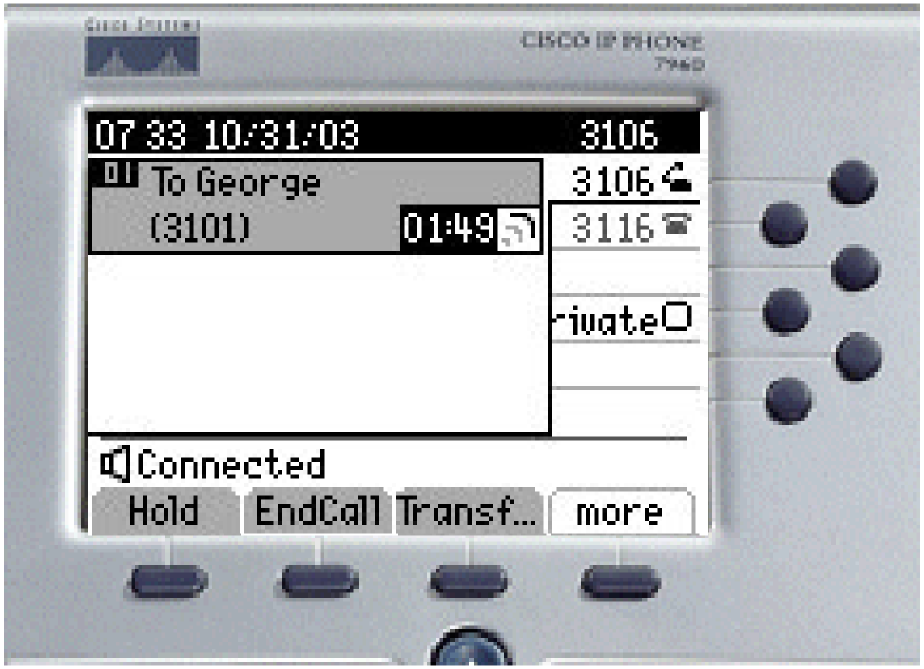
Cisco.com



Ad-Hoc Conference Features

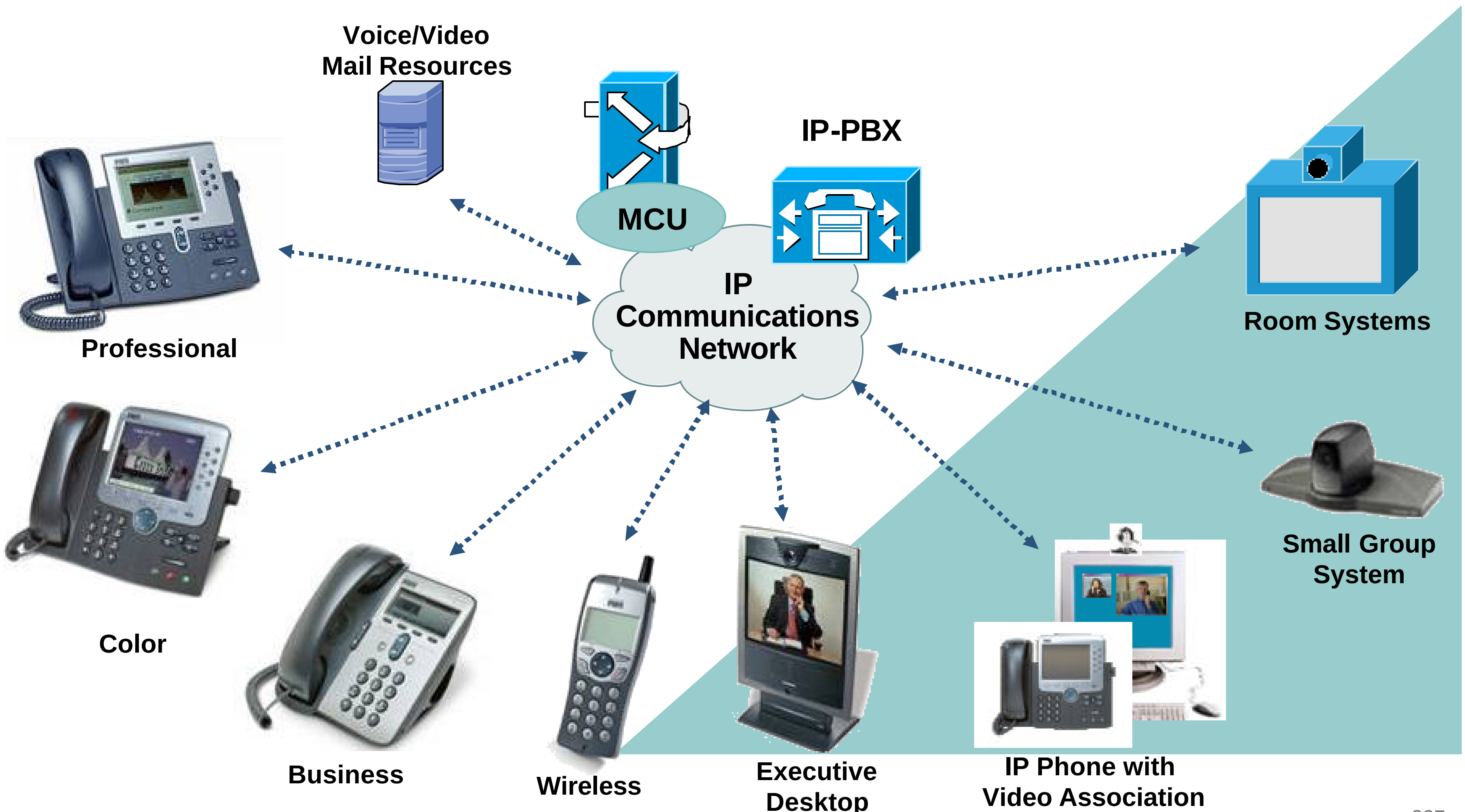
Cisco.com

- When only two participants remain in conference, conference will terminate and the two remaining participants are reconnected directly as a point to point call
- Example: Mary, George, and Sam are in a Conference
- Mary Hangs up
- George and Sam are in a point to point call
- The Conference Bridge Resource is released



Elements of IP Video Telephony

Cisco.com

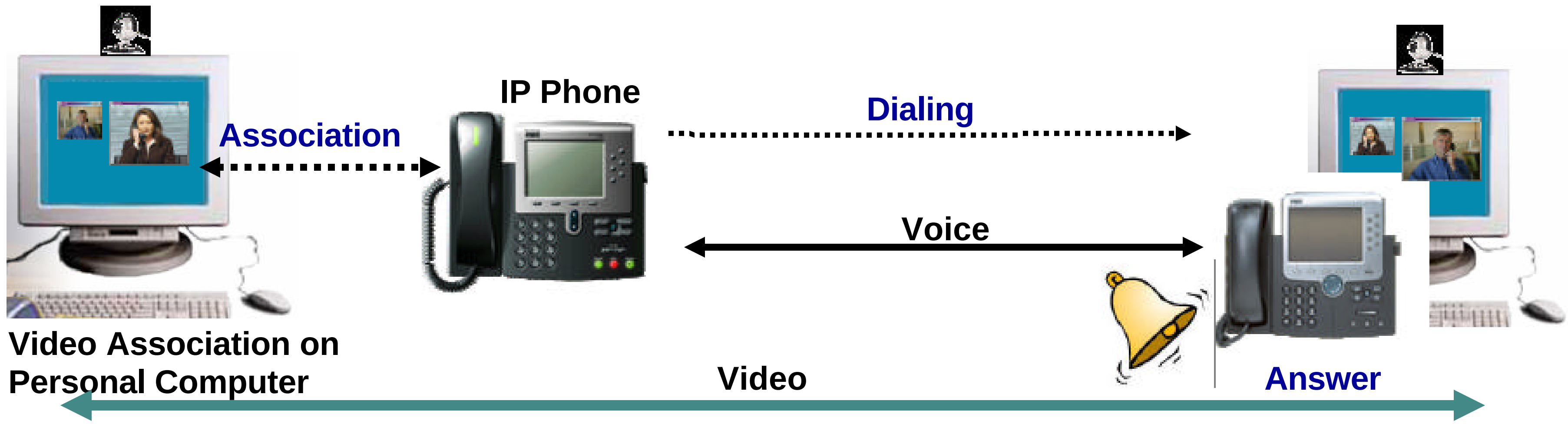


Introducing Cisco Video Telephony Advantage

- **Cisco VT Advantage enhances a phone call by automatically adding person-to-person video**
- **Uses phone features to enable users to transfer, conference, mute, forward, or put on hold the video-enabled phone call**
- **Cost-effectively integrates the simplicity of the phone call with the human element and personal effectiveness of video**

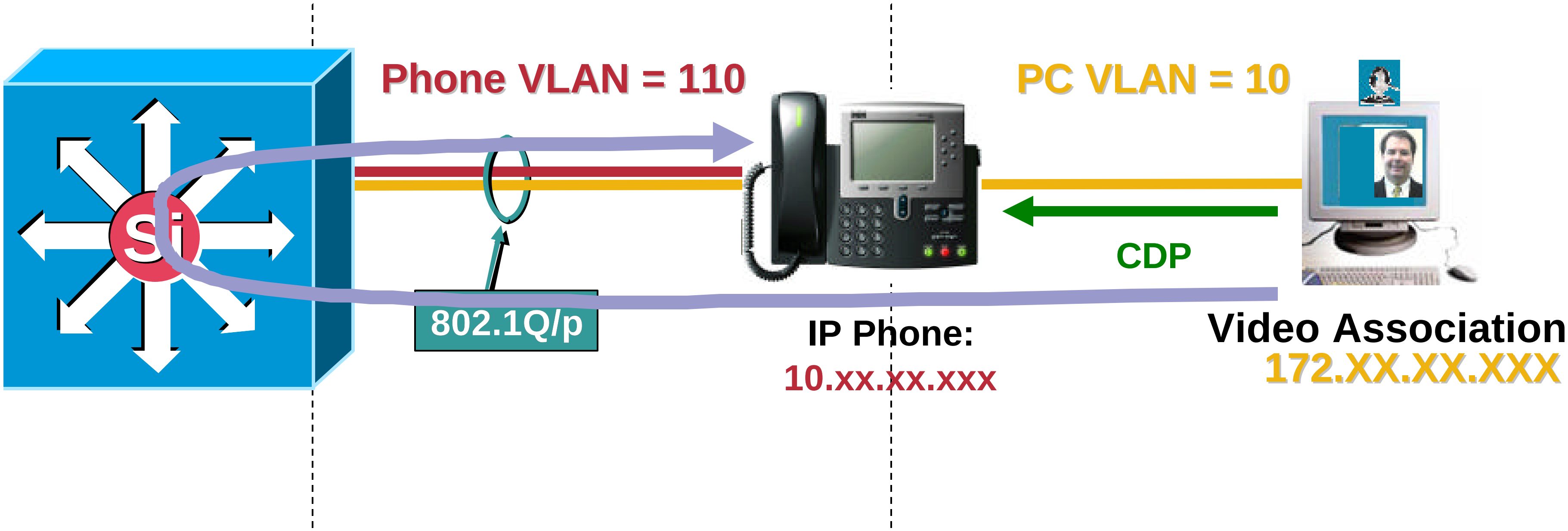
Video Association

Cisco.com



- **Personal Computer associates with IP phone**
- **Phone registers as a video capable phone**
- **Initiate Voice/Video Call from IP phone**
  - **Audio on the Phone**
  - **Video on the Personal Computer**

Video Association

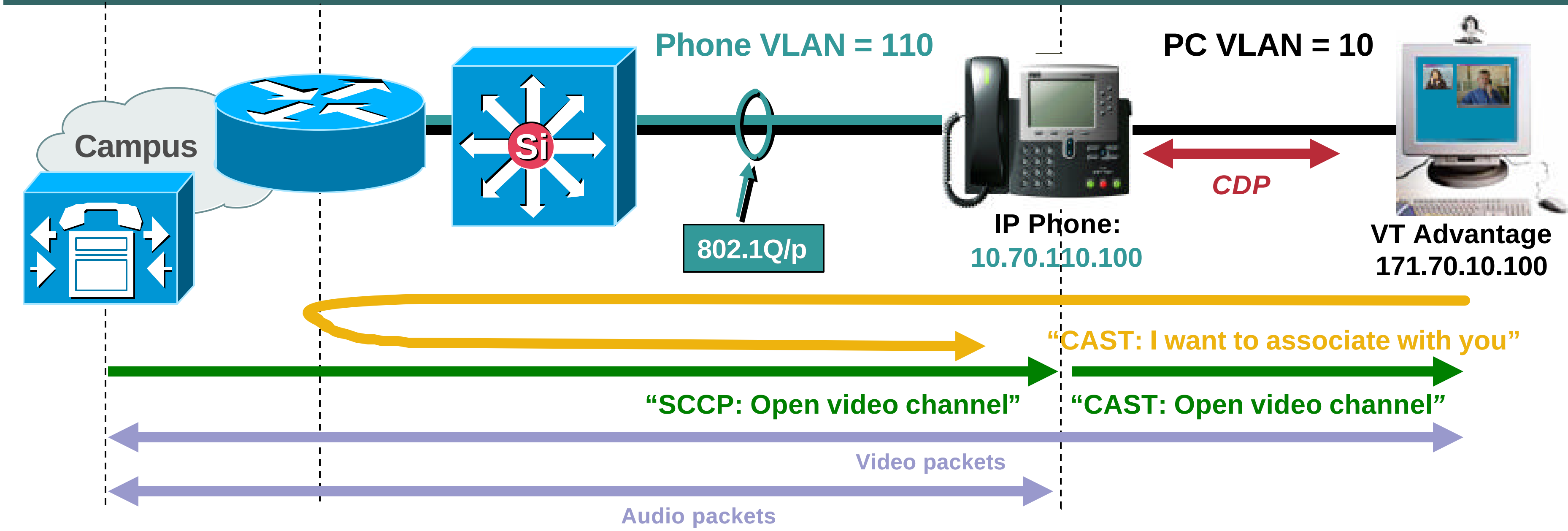


1. Phone traffic is placed on Voice VLAN
2. PC traffic is placed on Data VLAN
3. Phone and PC exchange CDP messages to discover each others IP addresses. Phone begins listening for messages from PC
4. PC sends messages to Phone over Layer-3 (IP)

SCCP Endpoints

How VT Advantage Works

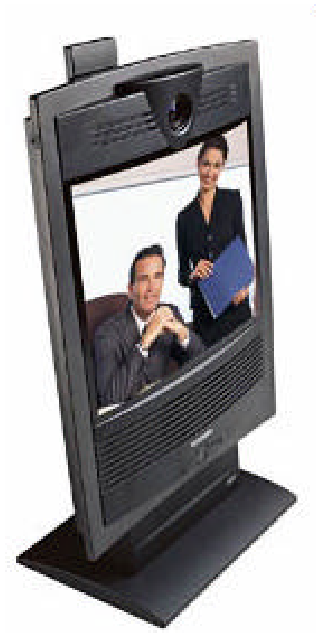
Cisco.com



1. Phone and PC exchange CDP. Phone begins listening for CAST messages on TCP port 4224 from IP address of CDP neighbor
2. PC initiates CAST messages to phone over TCP/IP. CAST packets are routed up to layer-3 boundary between VLANs. Firewalls and/or ACLs must permit TCP port 4224
3. Phone acts as SCCP proxy between VT Advantage and CallManager. CallManager tells phone to open video channels per call. Phone proxies those messages to PC via CAST protocol
4. Phone sends/receives audio. PC sends/receives video. Audio and video marked DSCP AF41. Switch port must be set to trust DSCP (or use an ACL) instead of trust COS or else VT Advantage packets will be rewritten to DSCP 0

Executive Desktop/Small Group Systems

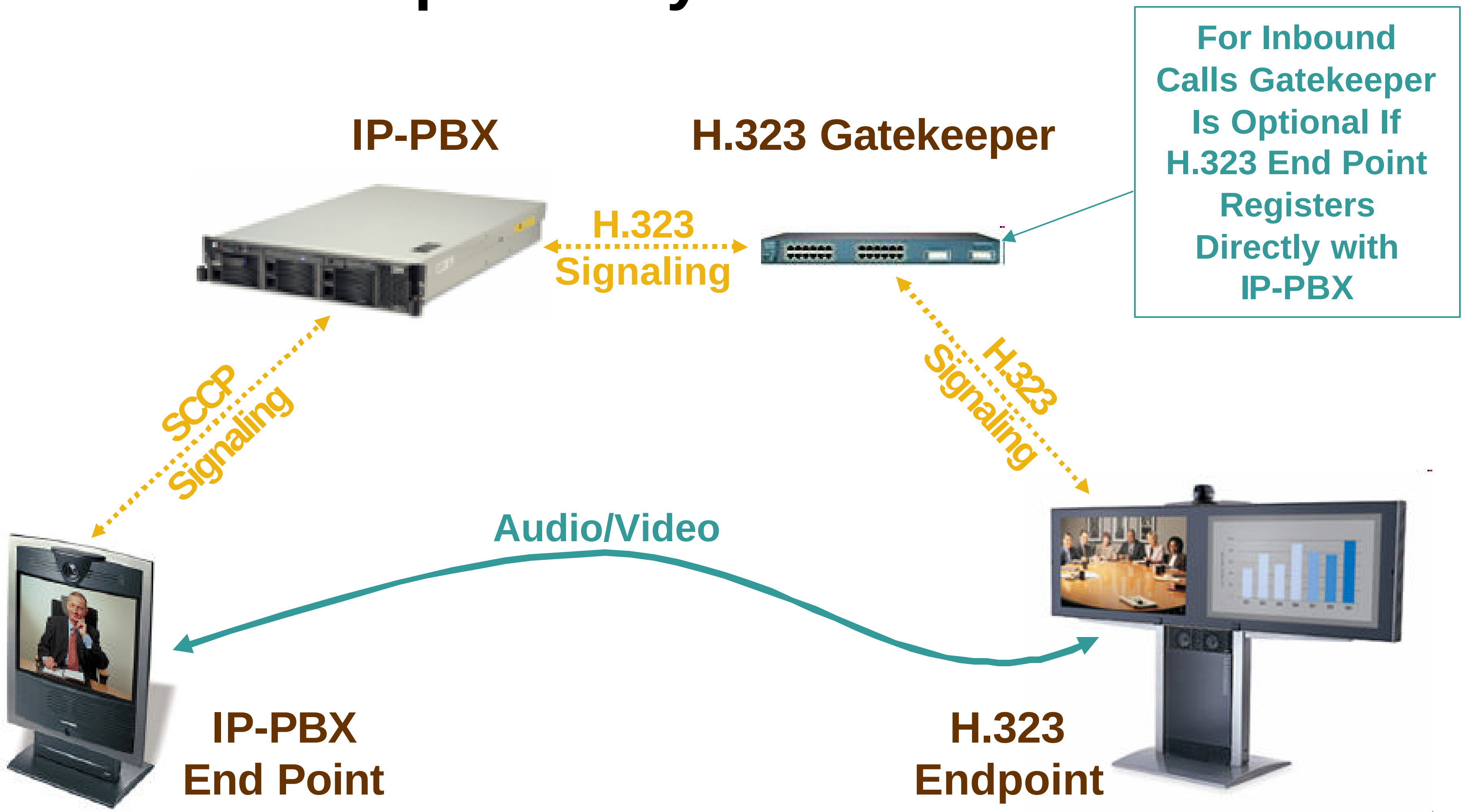
- **Videoconferencing systems communicate through same control protocol as IP-PBX**
- **Administration and management identical to existing IP telephony end points**
- **IP-PBX feature benefits extended to meeting room**



Room Systems

Cisco.com

H.323 Interoperability



H.323 End Points

- **Call Routing features are supported**

  Common Dialing, Call Forwarding, Shared Lines, Hunt Groups

- **H.323 endpoint initiation of Supplementary Features is not supported**

- **H.323 end points can be subject to Supplementary Features depending on their support of Empty Capability Set**

H.323 Empty Capability Sets

- **H.323 end points can be subject to Supplementary Features depending on their support of Empty Capability Set (ECS)**

‘

Without ECS Implementation

Unsupported Features

- Supplemental Features
- Park, Hold, Transfer,
- Conf, Join

Supported Features

- Common Dialing
- Call Forward
- Shared Lines
- Hunt Groups

With Improper ECS Implementation

Limited Features

- Transfer/Conference do not work properly
- No Up-speeding from audio to video

Supported Features

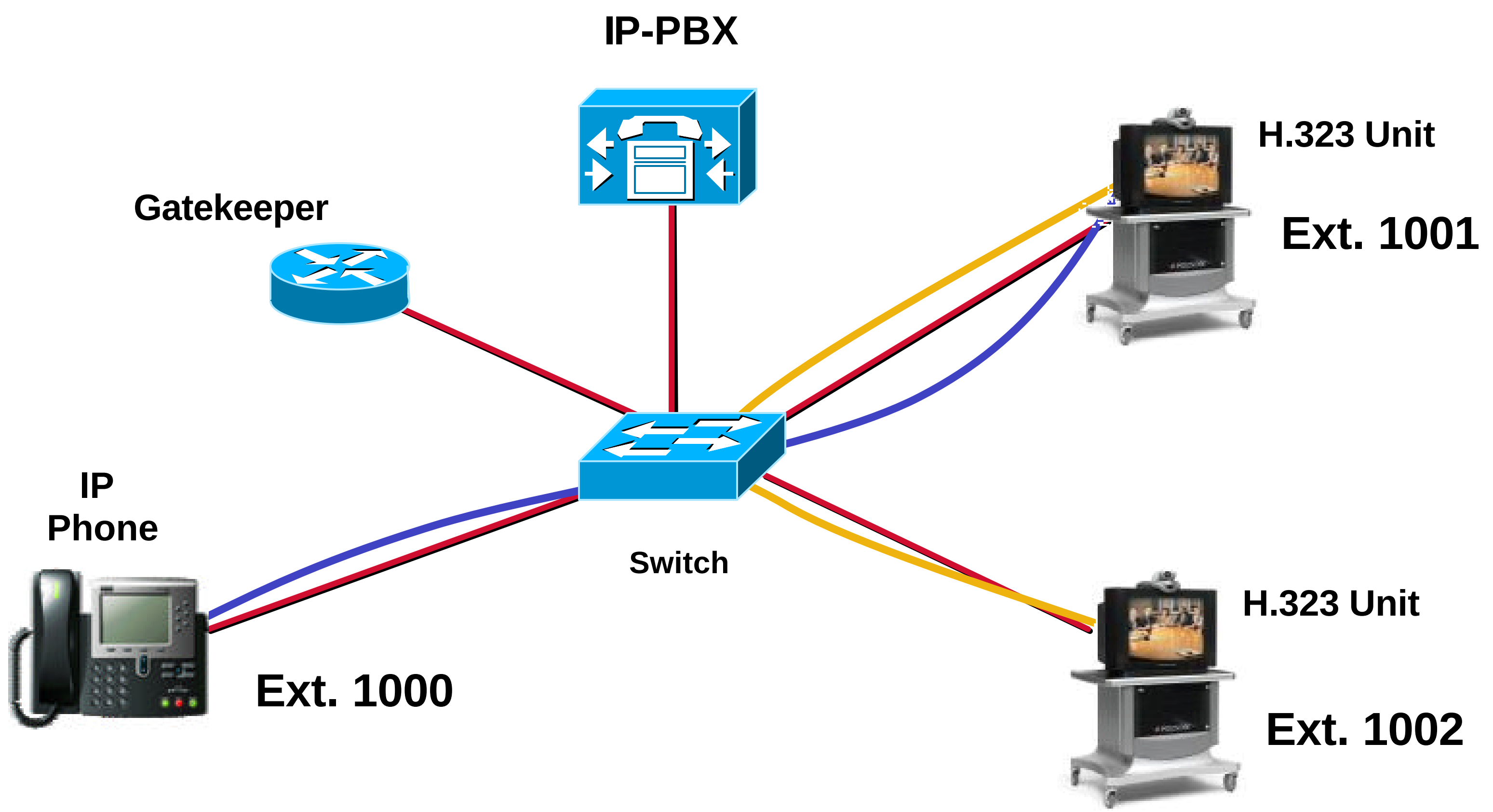
- Down-speeding is okay
- In call features do work Hold, Resume, Park

Proper ECS Implementation

Supported Features

- All Call Supplementary features are supported
- Can be subject to above features, allowing end point react when IP-PBX end point initiates feature request

Transfer for H.323 Endpoints with Proper ECS Implementation

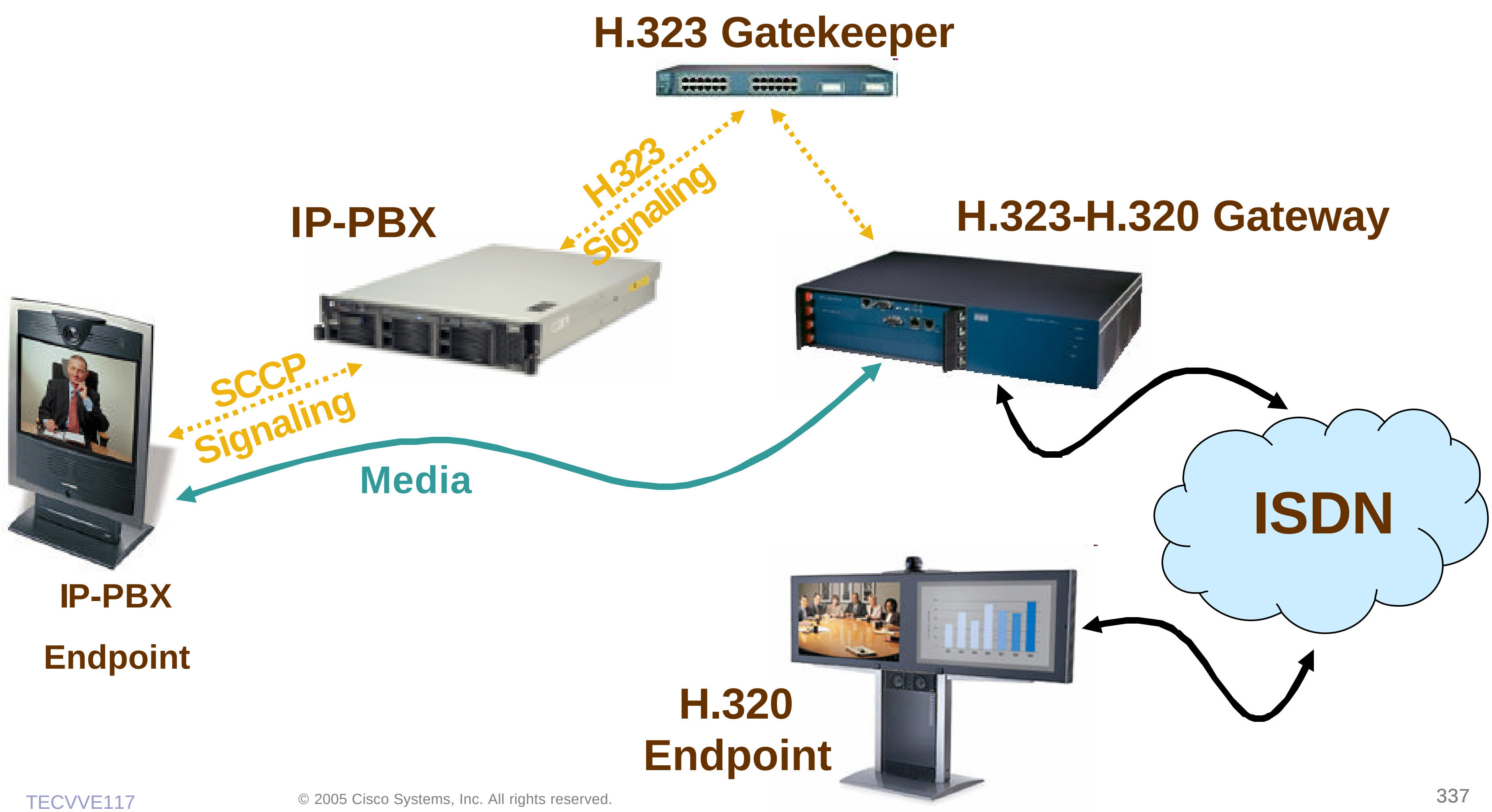


Scenario:

1. Call from IP Phone (ext 1000) talking to H.323 End Point (ext 1001)—voice only
2. IP Phones Transfers ext 1001 to ext 1002—now a video call

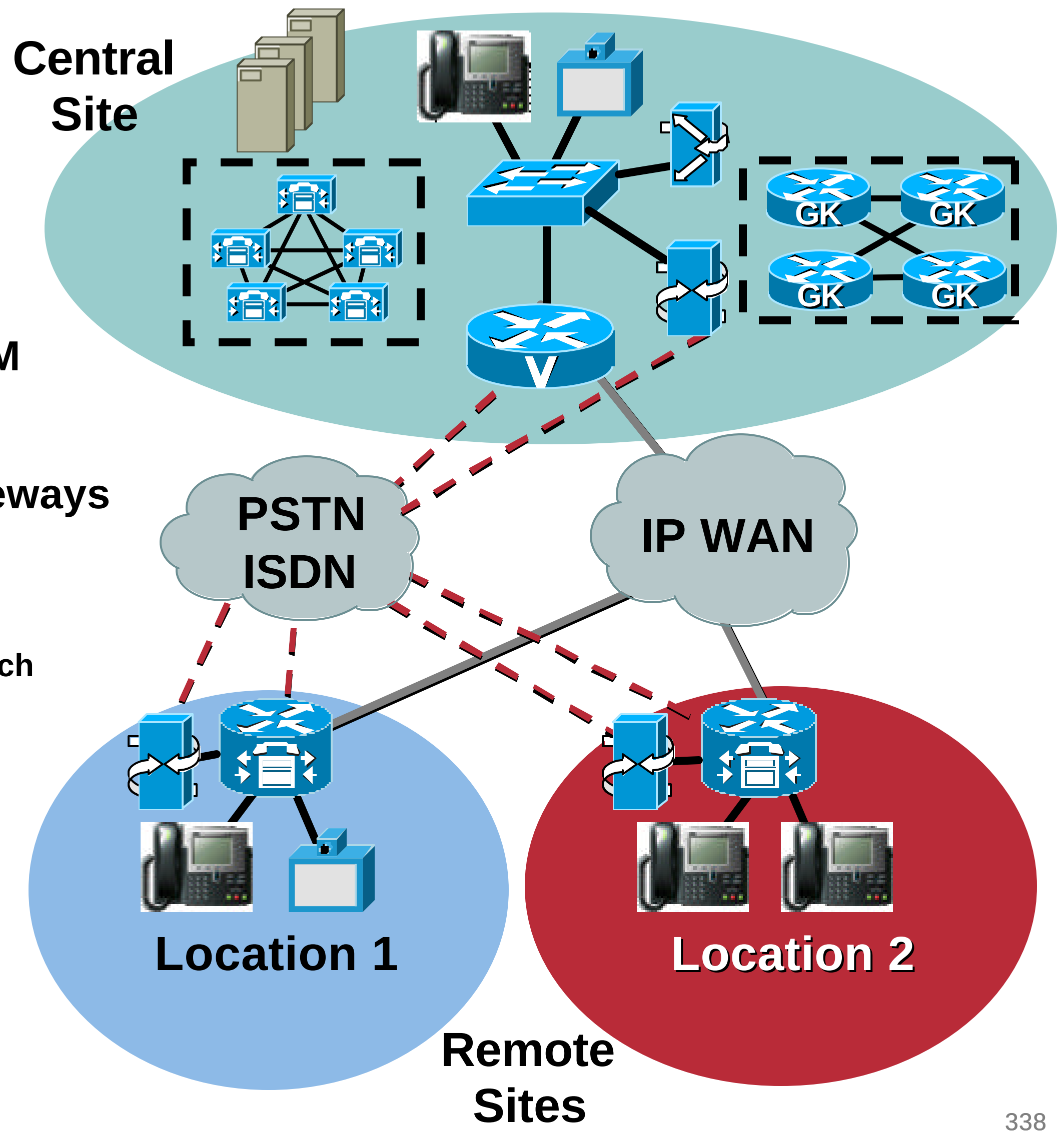
IP Video Telephony with H.320 Interoperability

Cisco.com

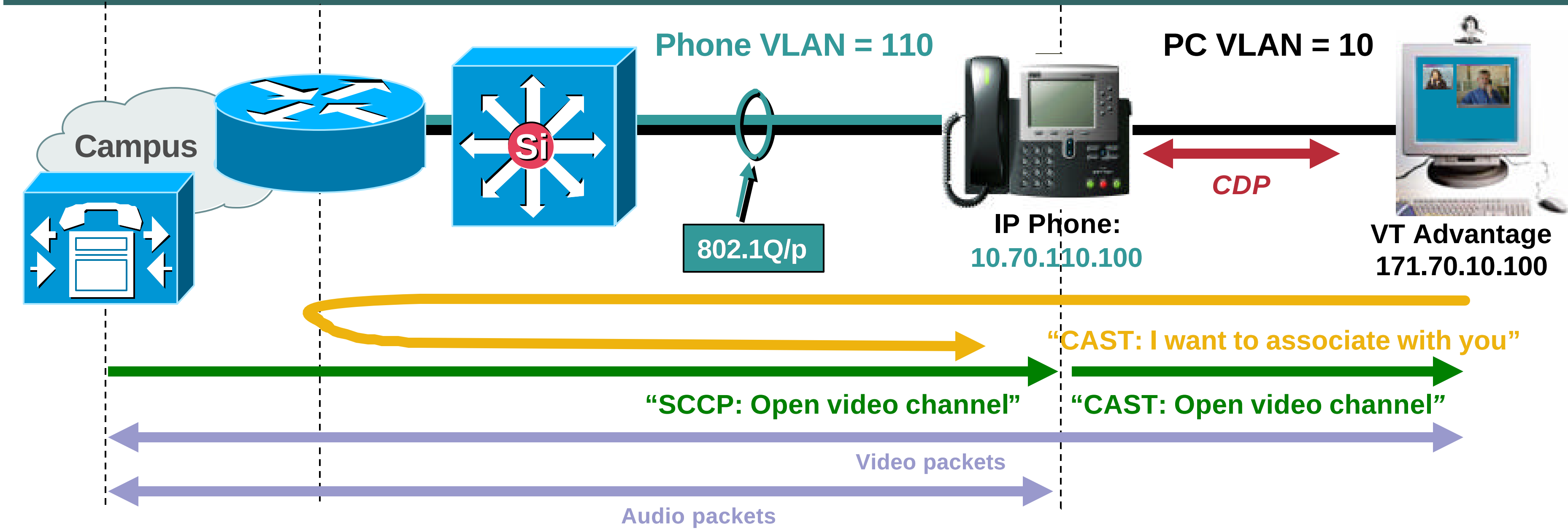


Centralized Call Processing AND Centralized Gatekeeper for H.323 Legacy and SCCP Video

- Cisco CallManager and GK located at single site, endpoints distributed
- H.323 endpoints register to GK or CM
- SCCP endpoints register to CM
- CM locations and region CAC
- Centralized or distributed gateways and MCUs?
- Dial plan design
    - Call routing, partitions, calling search spaces



SCCP Endpoints
How VT Advantage Works



1. Phone and PC exchange CDP. Phone begins listening for CAST messages on TCP port 4224 from IP address of CDP neighbor
2. PC initiates CAST messages to phone over TCP/IP. CAST packets are routed up to layer-3 boundary between VLANs. Firewalls and/or ACLs must permit TCP port 4224
3. Phone acts as SCCP proxy between VT Advantage and CallManager. CallManager tells phone to open video channels per call. Phone proxies those messages to PC via CAST protocol
4. Phone sends/receives audio. PC sends/receives video. Audio and video marked DSCP AF41. Switch port must be set to trust DSCP (or use an ACL) instead of trust COS or else VT Advantage packets will be rewritten to DSCP 0

SCCP Dial Plan

Cisco.com

CM utilizes the same logic for class of service, call routing, etc., for video as it does for audio

- Shared Line Appearances

  SCCP devices can share lines with full features

  H.323 devices can share lines, but loss of features such as hold, etc, which require specific interface features not found on H.323 devices

- Call Forwarding

  Across regions can be difficult, depending on H.245 and H.225 caps exchanges

  H.323 devices must be on but not answered, or CF fails

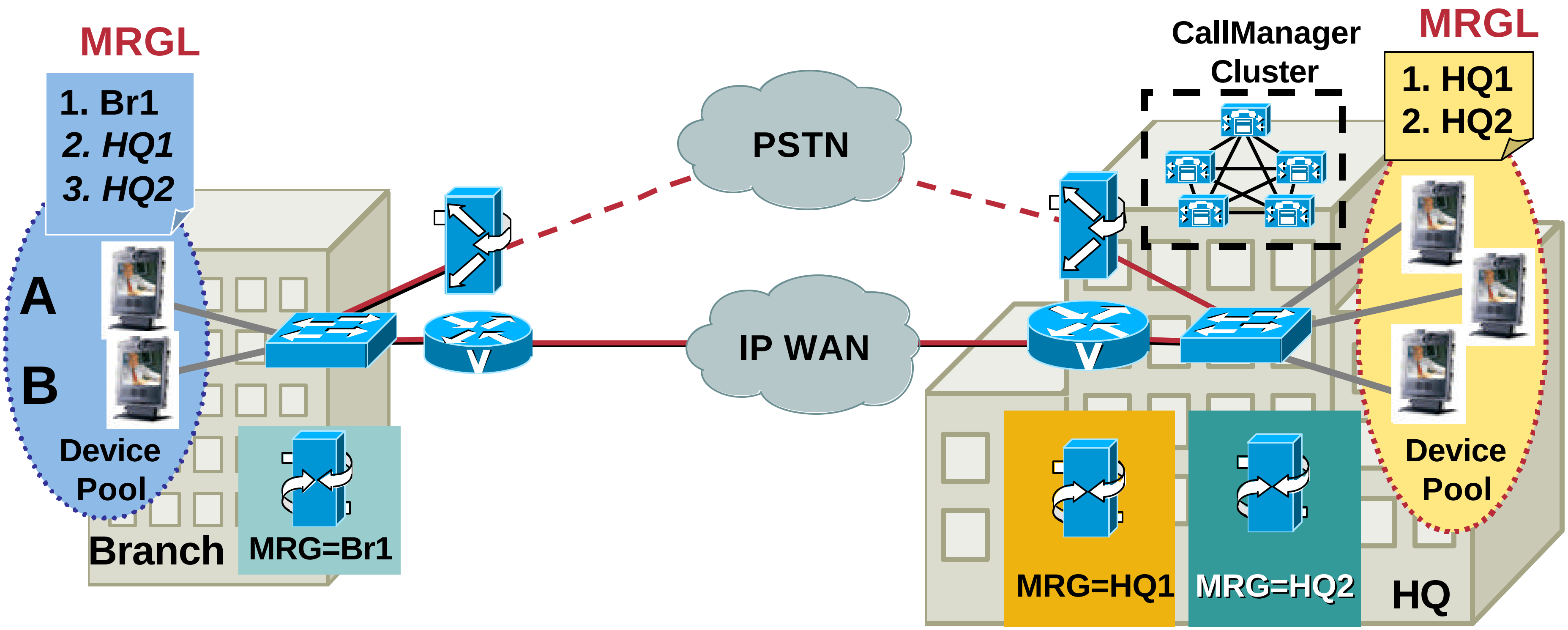
- Hunt Groups

  SCCP and H.323 devices can be in a hunt group

  If H323 device is in hunt, but is OFF, hunt terminates - use ‘broadcast’ to avoid this condition

SCCP Media Resources
Distributed Conferencing Resources

Cisco.com



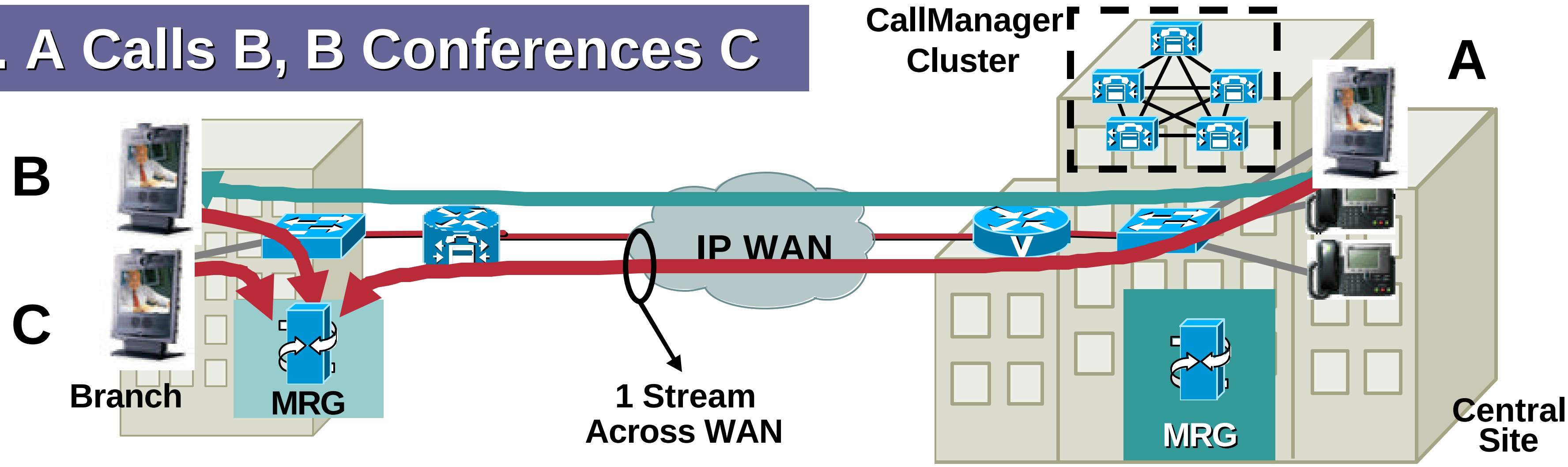
- Conference between A, B —no video across WAN
- MCU, Gateway resources at branch
- Transcoding/Transrating resources are ‘owned’ and managed by the MCU
- No conferencing during WAN failures

MRG = Media Resource Group
MRGL = Media Resource Group List

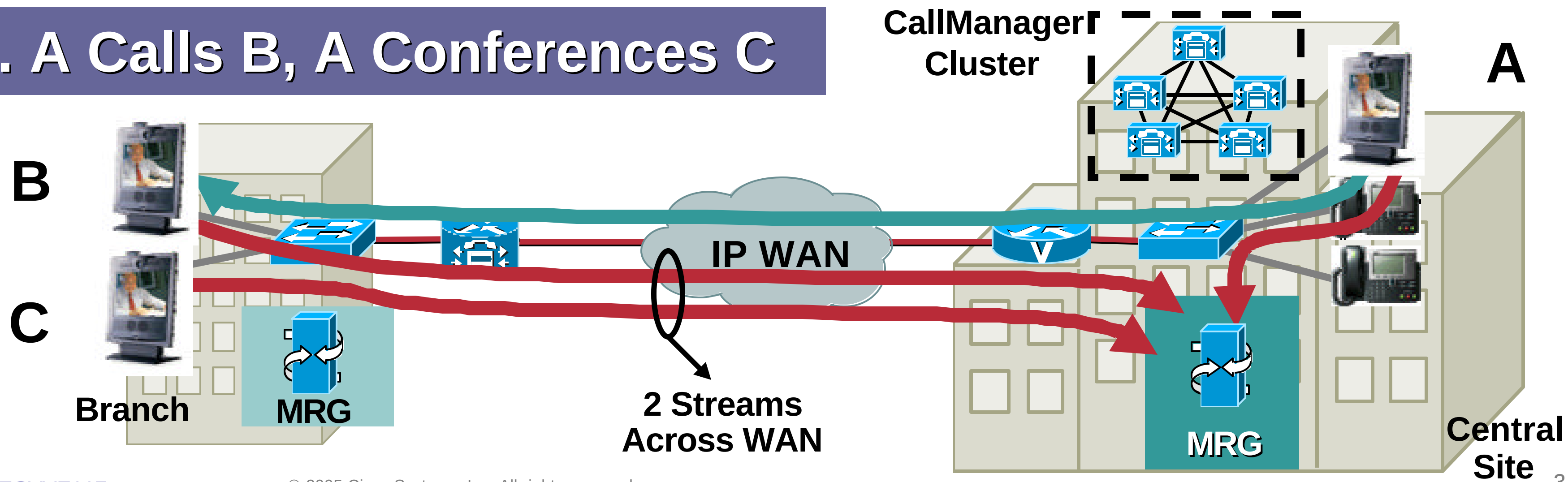
SCCP Media Resources "Conference Initiator" Concept

Overprovision WAN to Allow for This…

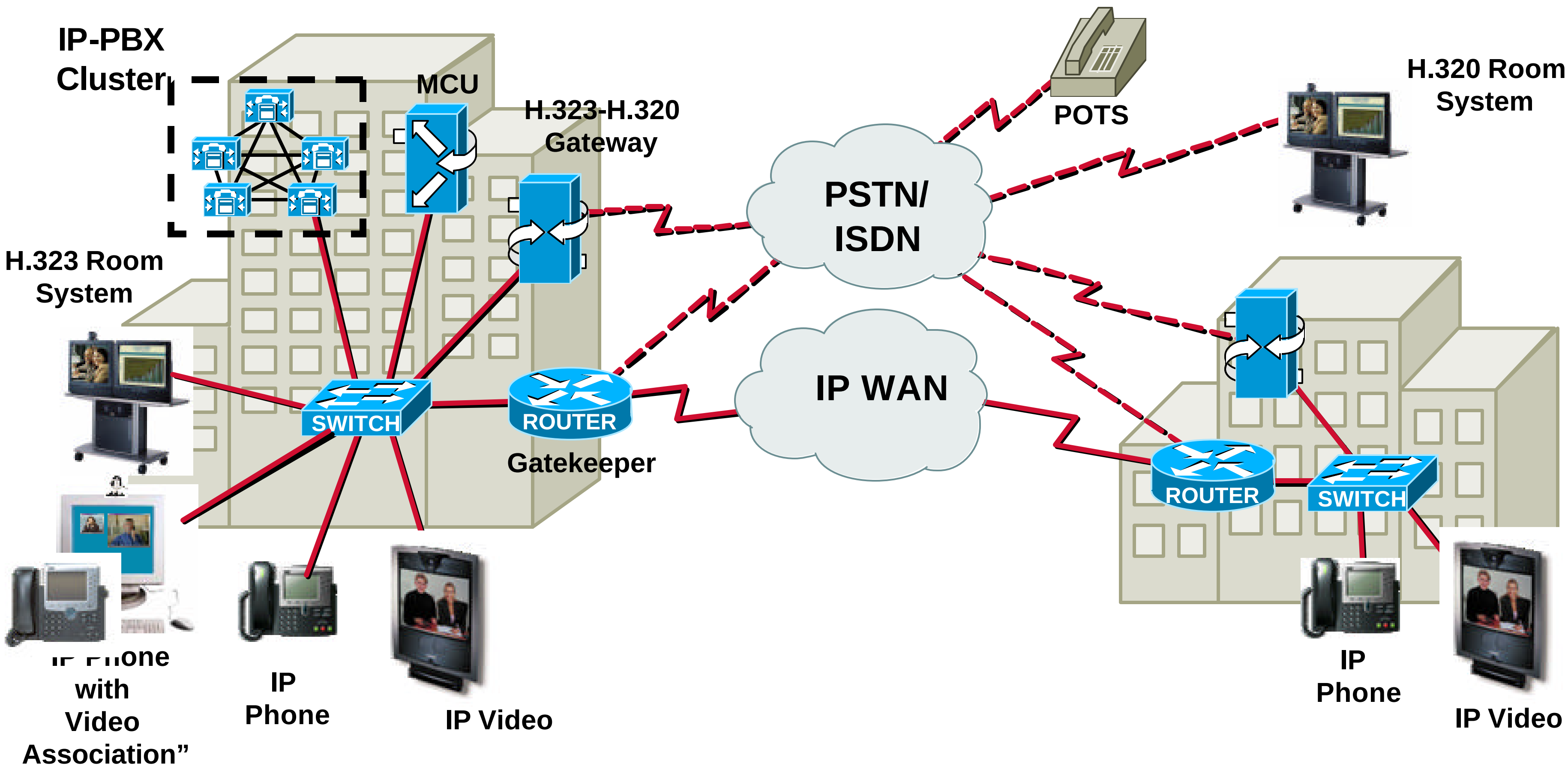
1. A Calls B, B Conferences C



2. A Calls B, A Conferences C



Bringing It All Together



Telephony Infrastructure Agenda (2/2)

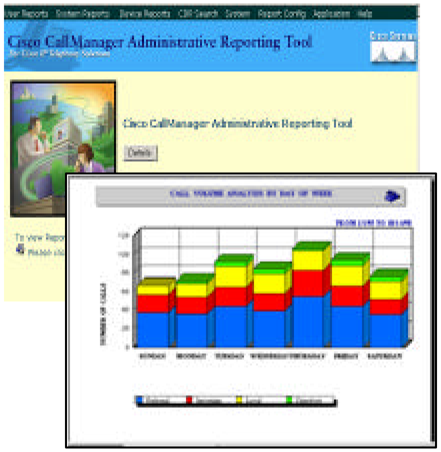
Cisco.com

- Call Admission Control
- Survivable Remote Site Telephony
- Call Manager Express
- Dial Plan
- Voice Mail Integration
- Security
- Video Telephony
- Management
- LDAP Directories

Management

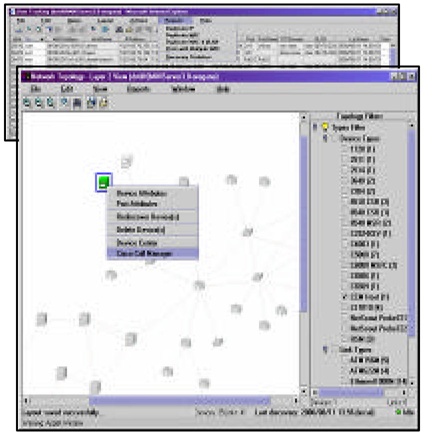
Cisco.com

Provisioning and Reporting



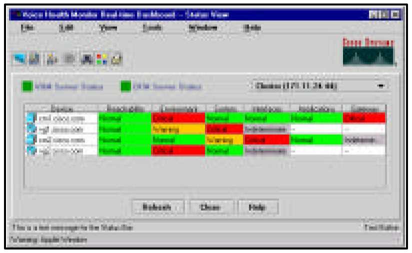
- **Provisioning:** BAT (IP phones), CVM (network), QPM PRO (QoS)
- **Reporting:** CAR

Element Management



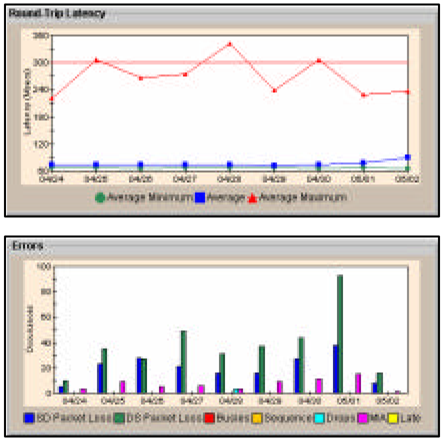
- CW2000: RME 3.2, Campus Mgr 3.1
- In-line powered switches, CCM
- Handset tracking
- CCM topology display

Fault Detection



- IP Telephony Manager (ITEM)
- Pro-active fault detection
- Real-time status reports on CCM, GWs, Apps

Performance Analysis



- IPM 2.2
- Real-time data on delay, jitter,…
- Generate alarms based on perf. thresholds

Telephony Infrastructure Agenda (2/2)

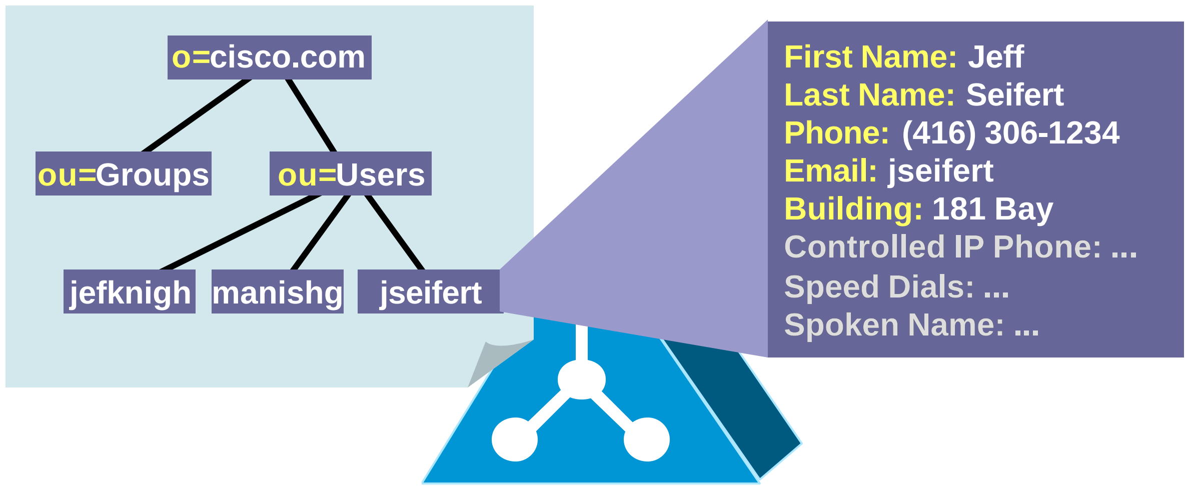
- Call Admission Control
- Survivable Remote Site Telephony
- Call Manager Express
- Dial Plan
- Voice Mail Integration
- Security
- Video Telephony
- Management
- LDAP Directories

LDAP Directories

What Is a Directory? What Is a Schema? What Is LDAP?

Cisco.com

DIRECTORY:
A Specialized Database Used to Store User Information



DIRECTORY SCHEMA:
Dictates Rules and Types of Objects That Can Be Stored in the Directory

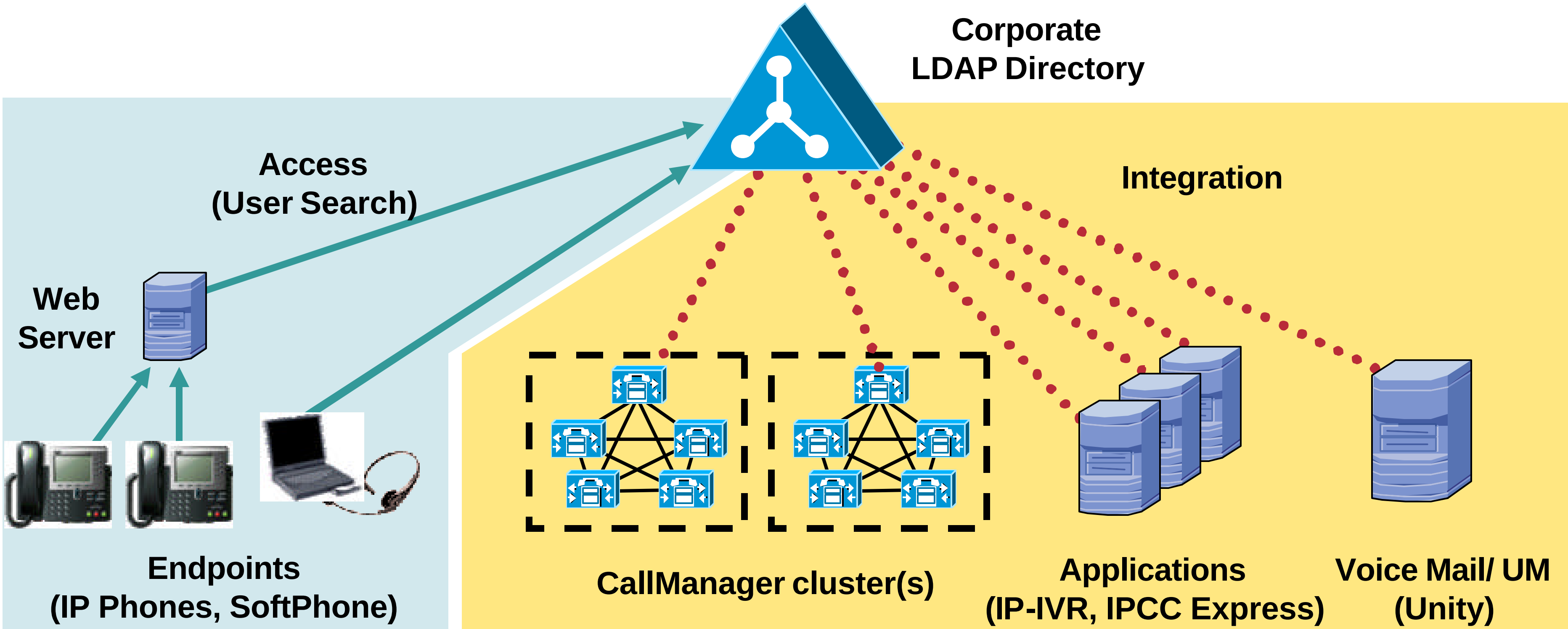
LDAP:
Lightweight Directory Access Protocol, a Standard Protocol Used to Access Directories

IP Phone

User PC

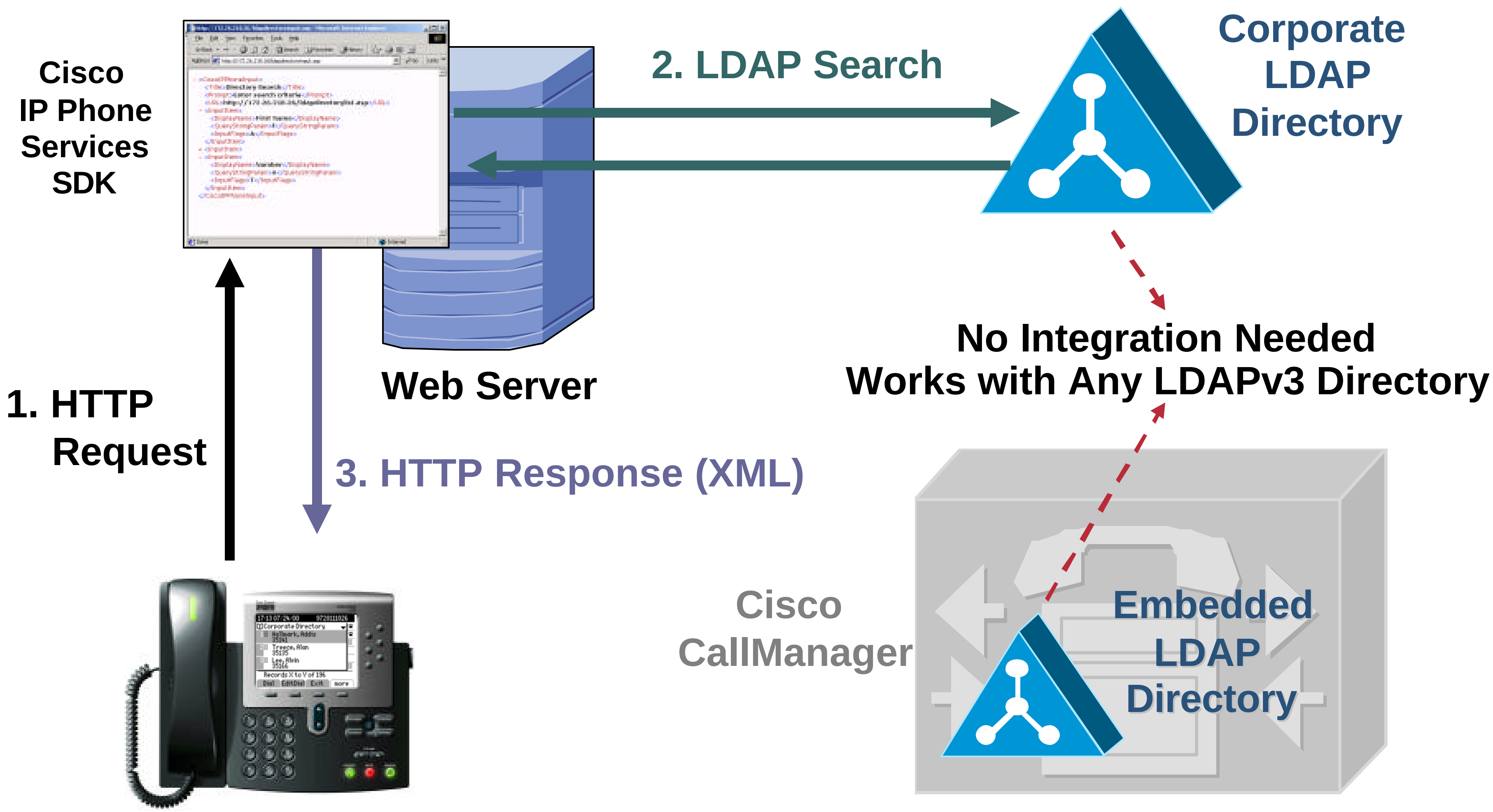
Directory-Enabled Application

LDAP Directories
Directory Access and Integration

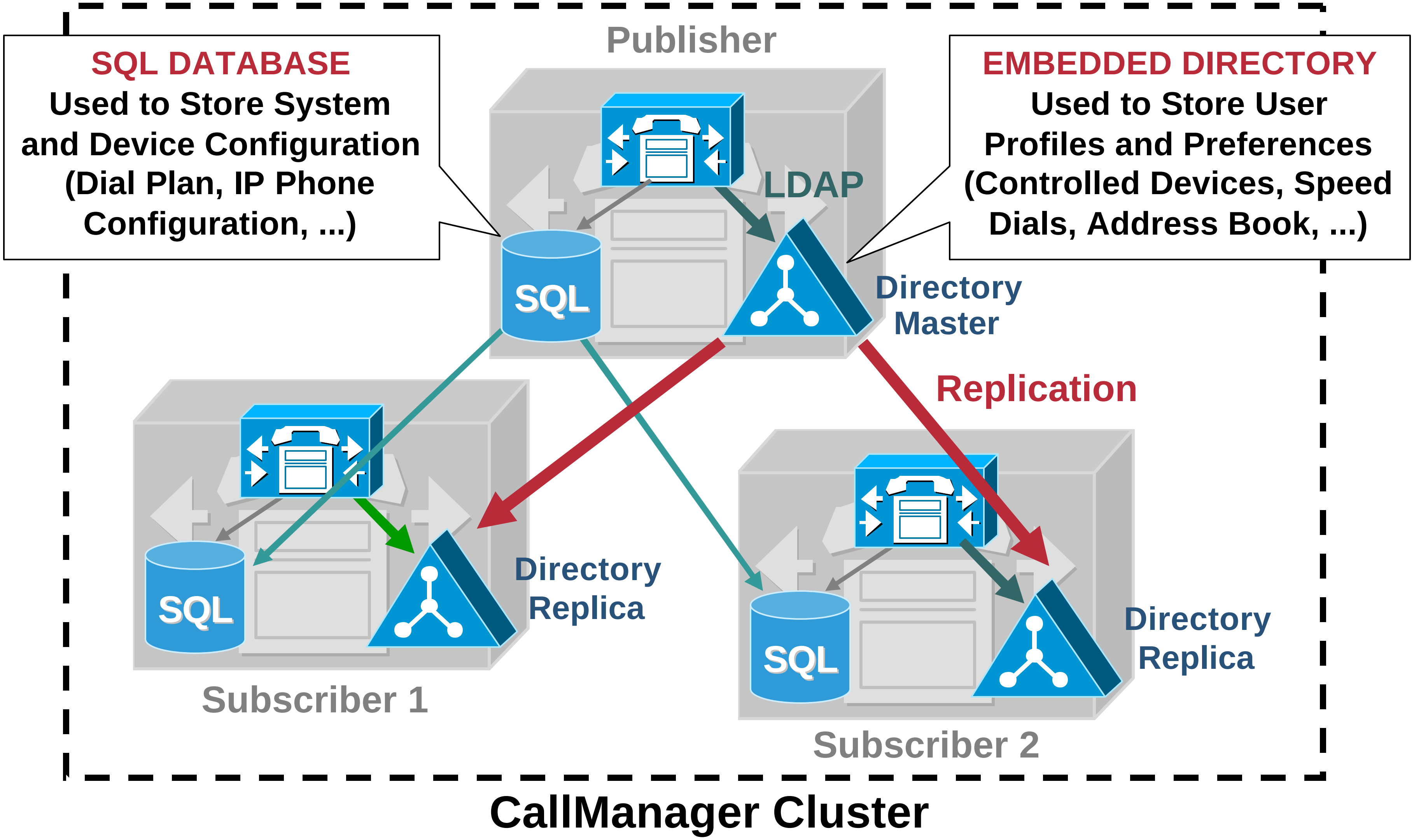


- **Directory Access**: Endpoints enabled to search corporate directory
- **Directory Integration**: User profile stored in a single repository—single point of user authentication

LDAP Directories
Directory Access for IP Phones

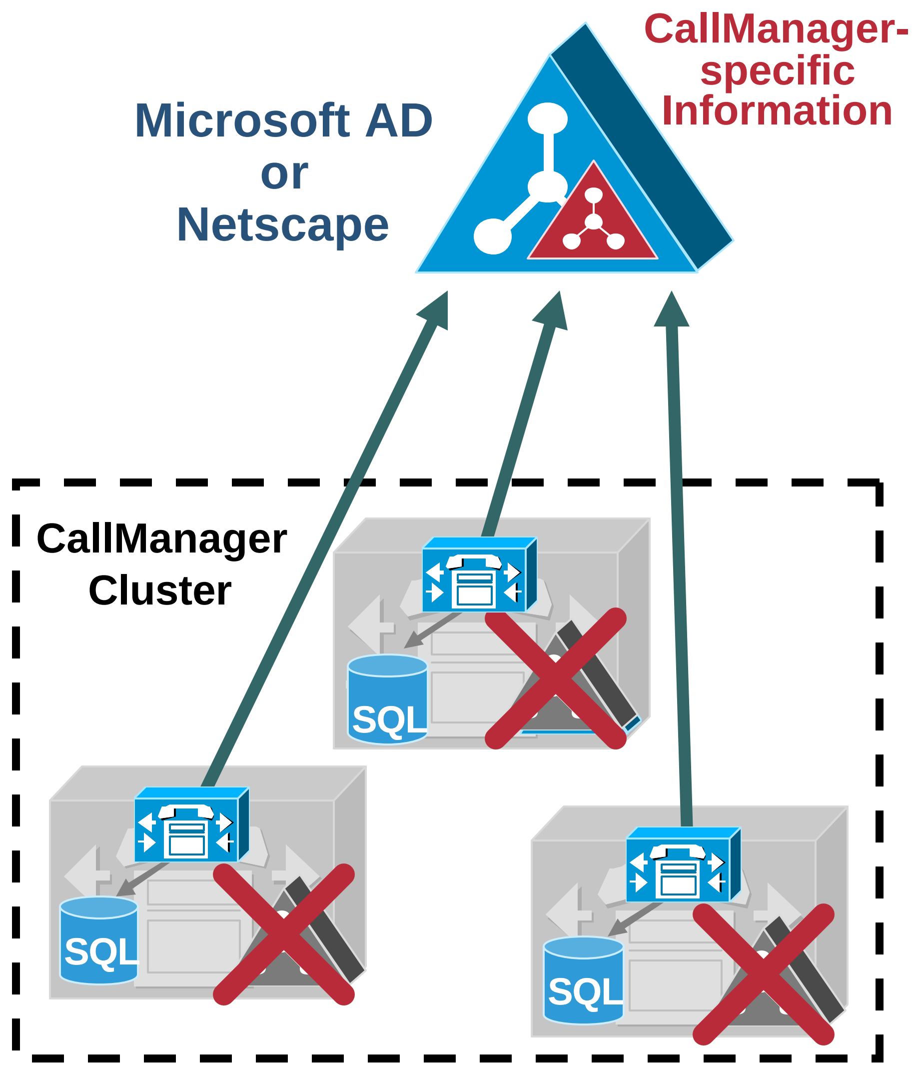


LDAP Directories
CallManager Directory Architecture



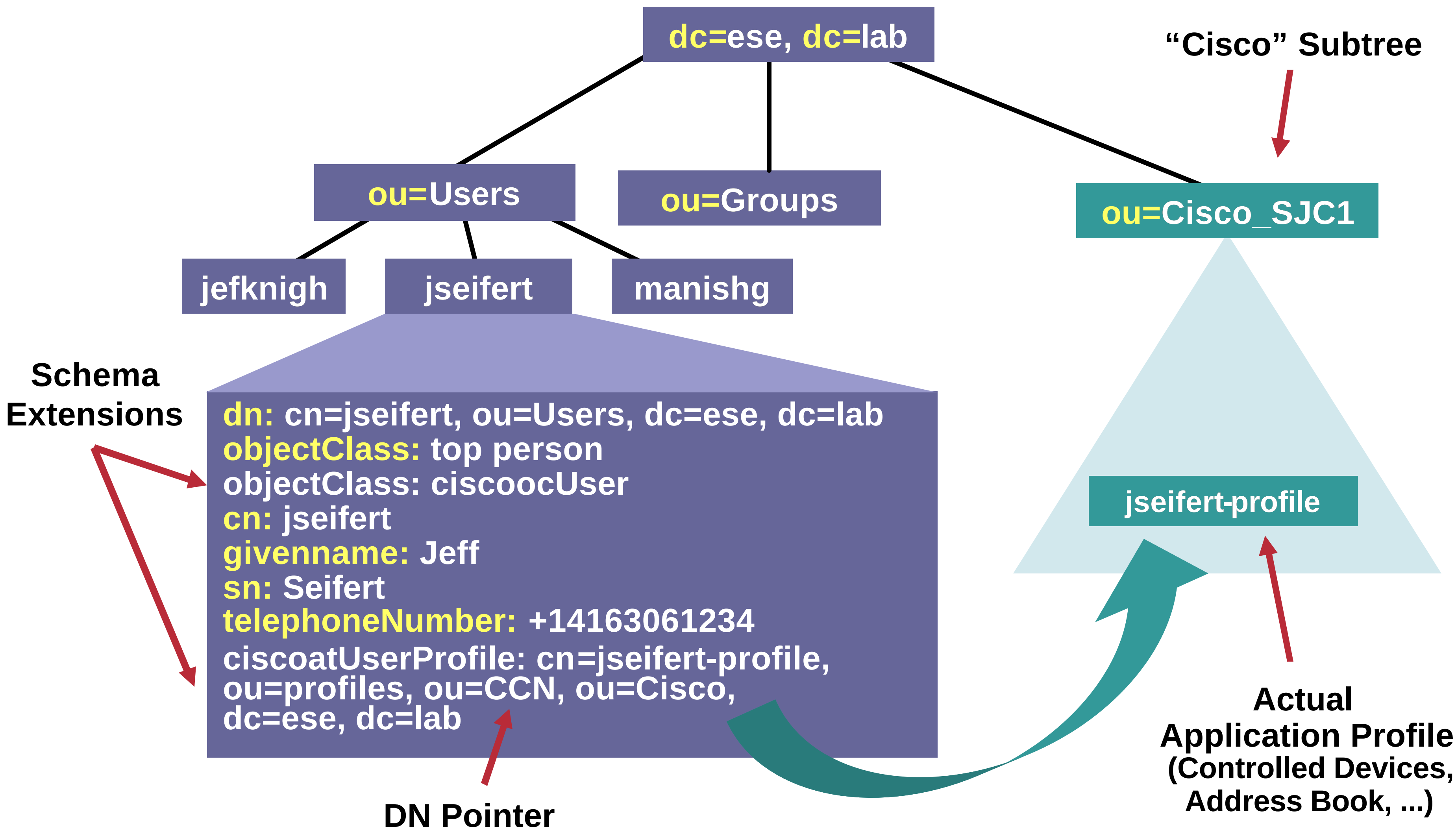
LDAP Directories
Integrating with a Corporate Directory

- Embedded directory is no longer used (stop DC Directory service)
- Need to extend the corporate directory schema to store application-specific info
- No standard for schema extension process
- Supported directories: Microsoft AD, Netscape



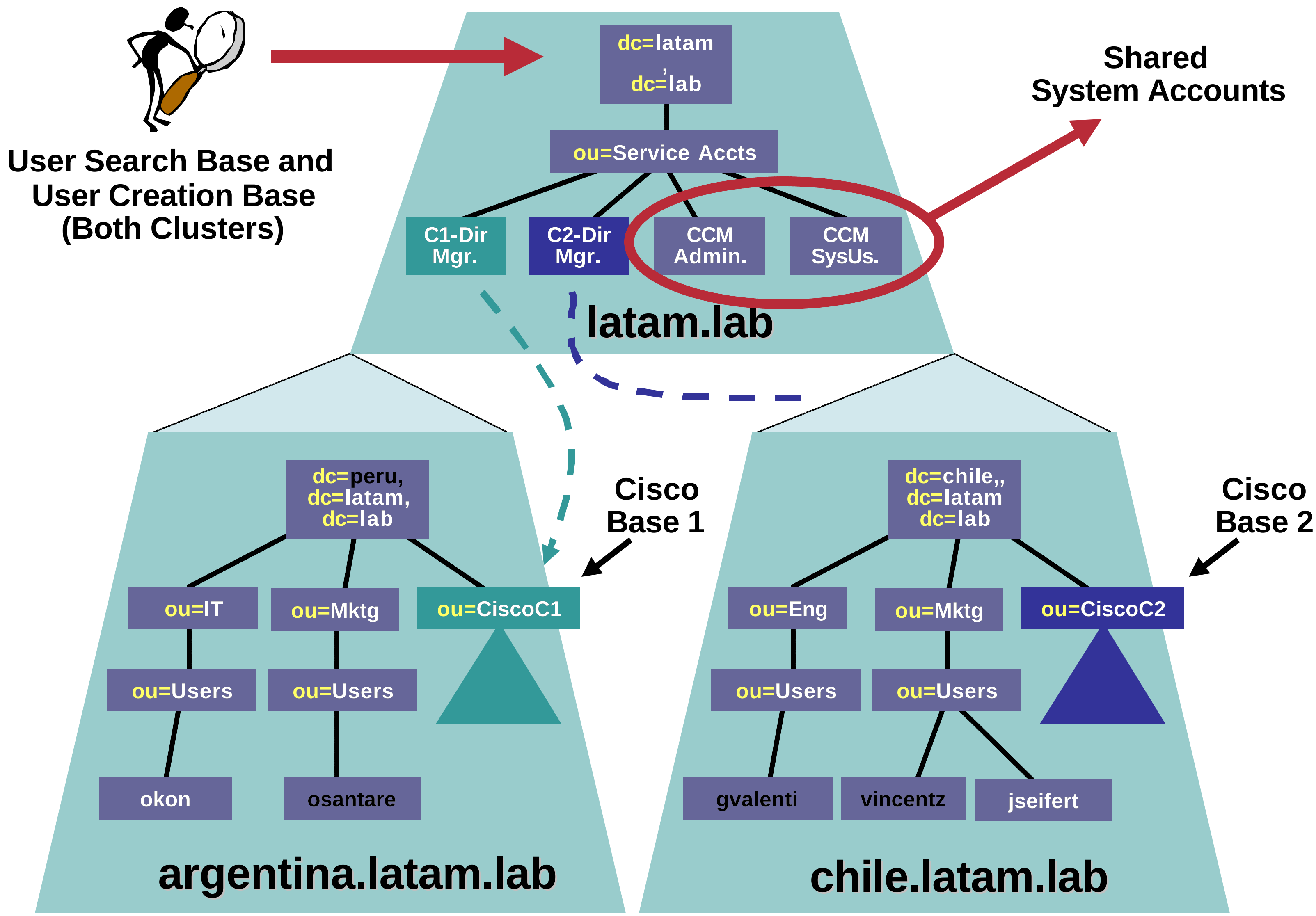
LDAP Directories
Directory Hierarchy Structure

Cisco.com



LDAP Directories
Multiple CCM Clusters Integration (3.3(3) Needed)

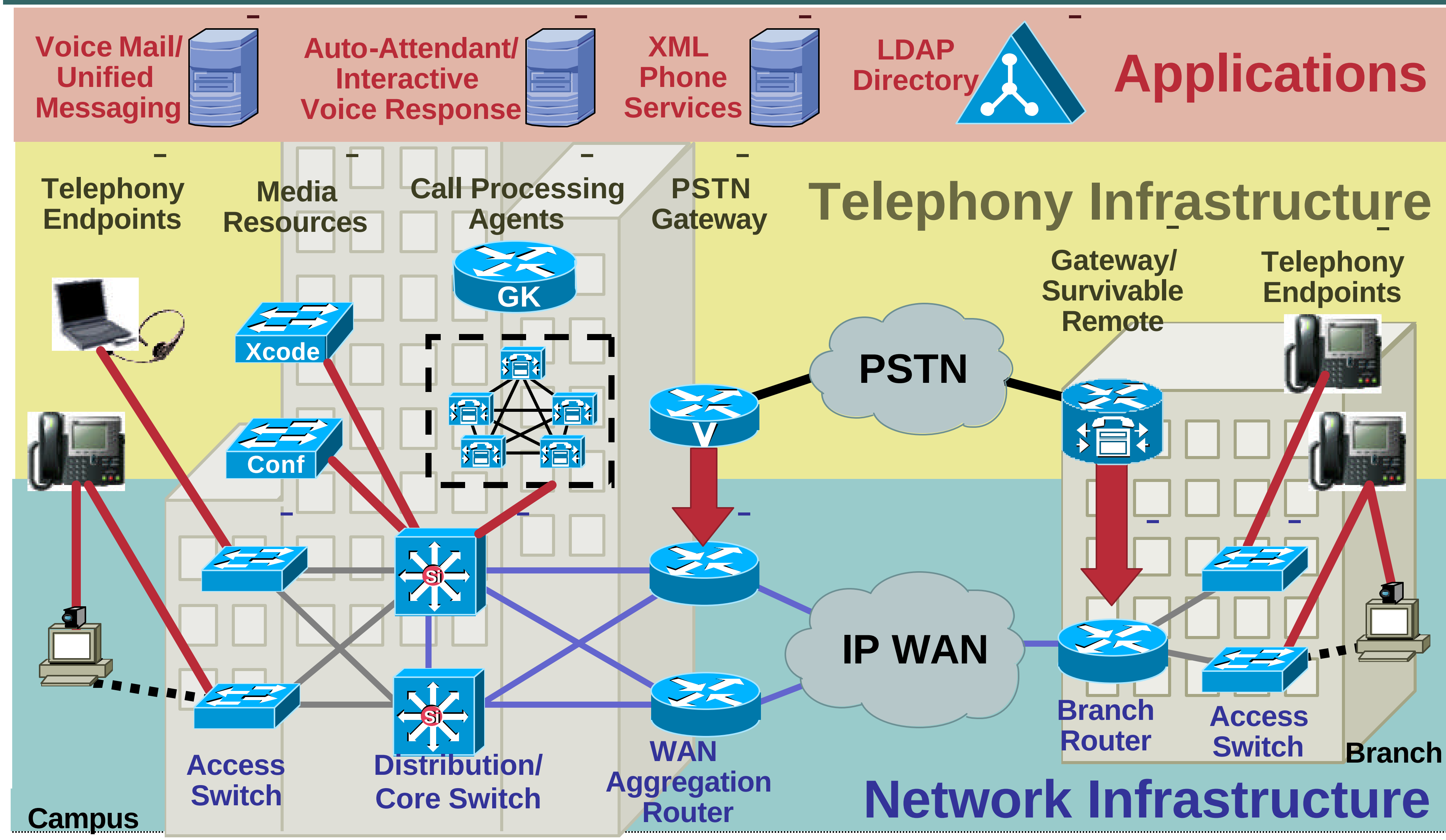
Cisco.com



LDAP Directories
Integration Best Practices

- Ensure that the integration is planned and implemented by your organization's AD experts
- Before integration, test in a lab setup against an exact replica of the production AD
- Back up the AD forest prior to integration
- Use DNS-resolvable domain names instead of specific AD server names in the Plugin configuration (for HA and load balancing)
- Use IOS SLB on a Cat6K if DNS load balancing is not available

What We Have Built So Far



Agenda

Cisco.com

- Introduction
- Network Infrastructure
- Telephony Infrastructure
- Legacy Migration and Integration

Legacy Migration and Integration

Agenda

- Flash Cut Migrations

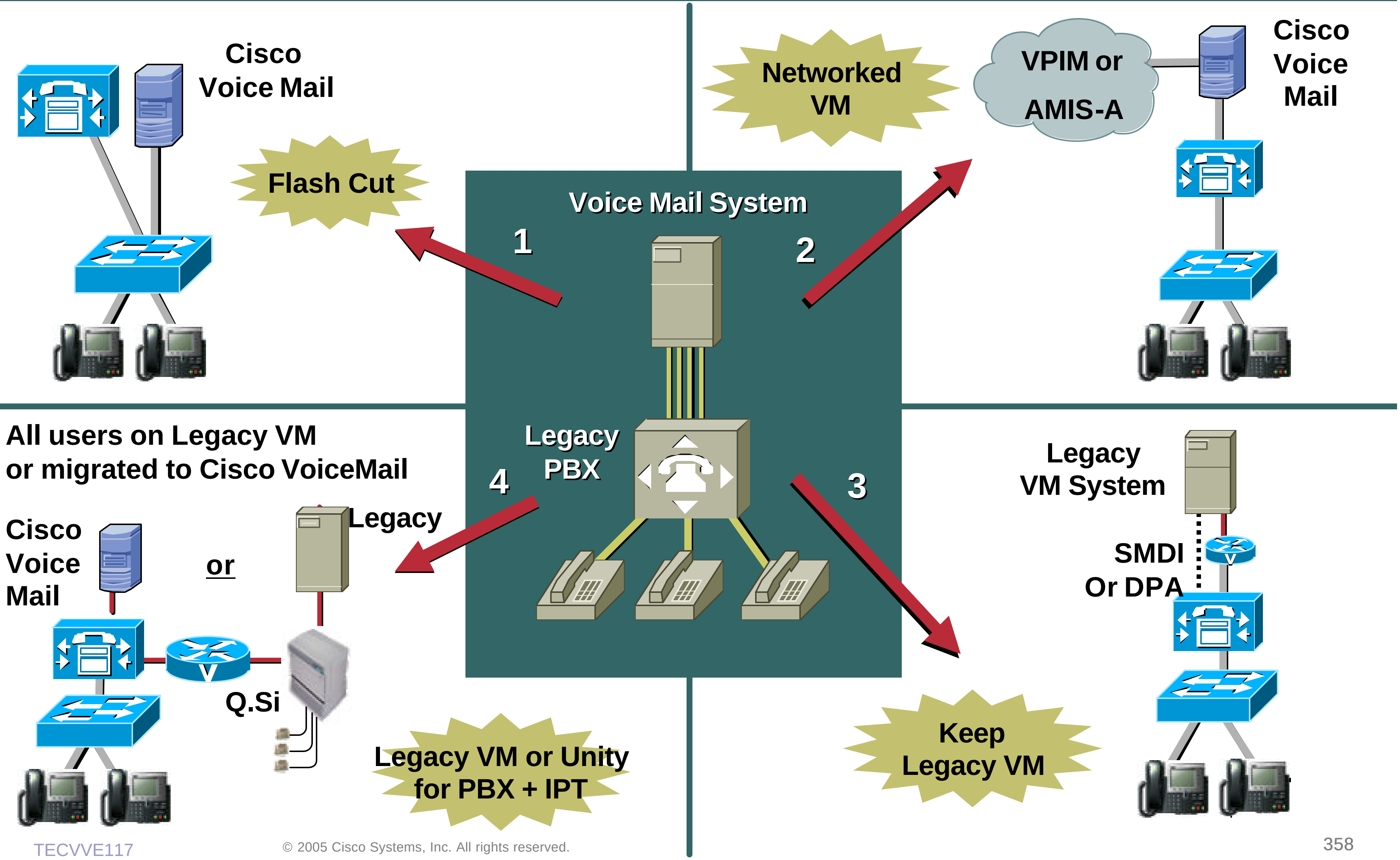
    Pull the Band-Aid off Fast

- Slow Migrations (“Shrink and Grow”)

    Pull the Band-Aid off Slow

- Integration Matrices

Flash Cut Migrations
Voice Mail Integration Options



Legacy Migration and Integration

Agenda

- Flash Cut Migrations

  Pull the Band-Aid off Fast

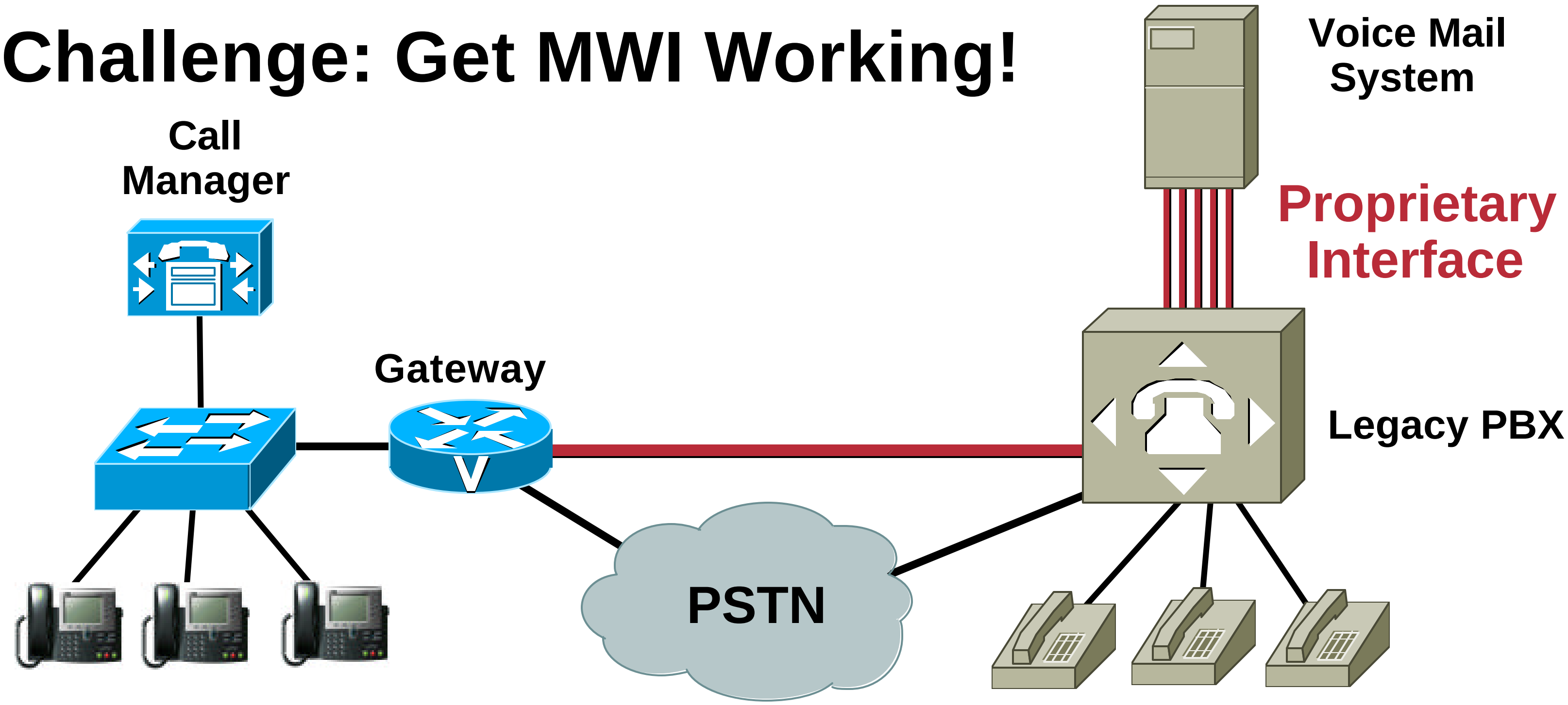
- Slow Migrations ("Shrink and Grow")

  Pull the Band-Aid off Slow

- Integration Matrices

Slow Migrations

Challenge: Get MWI Working!



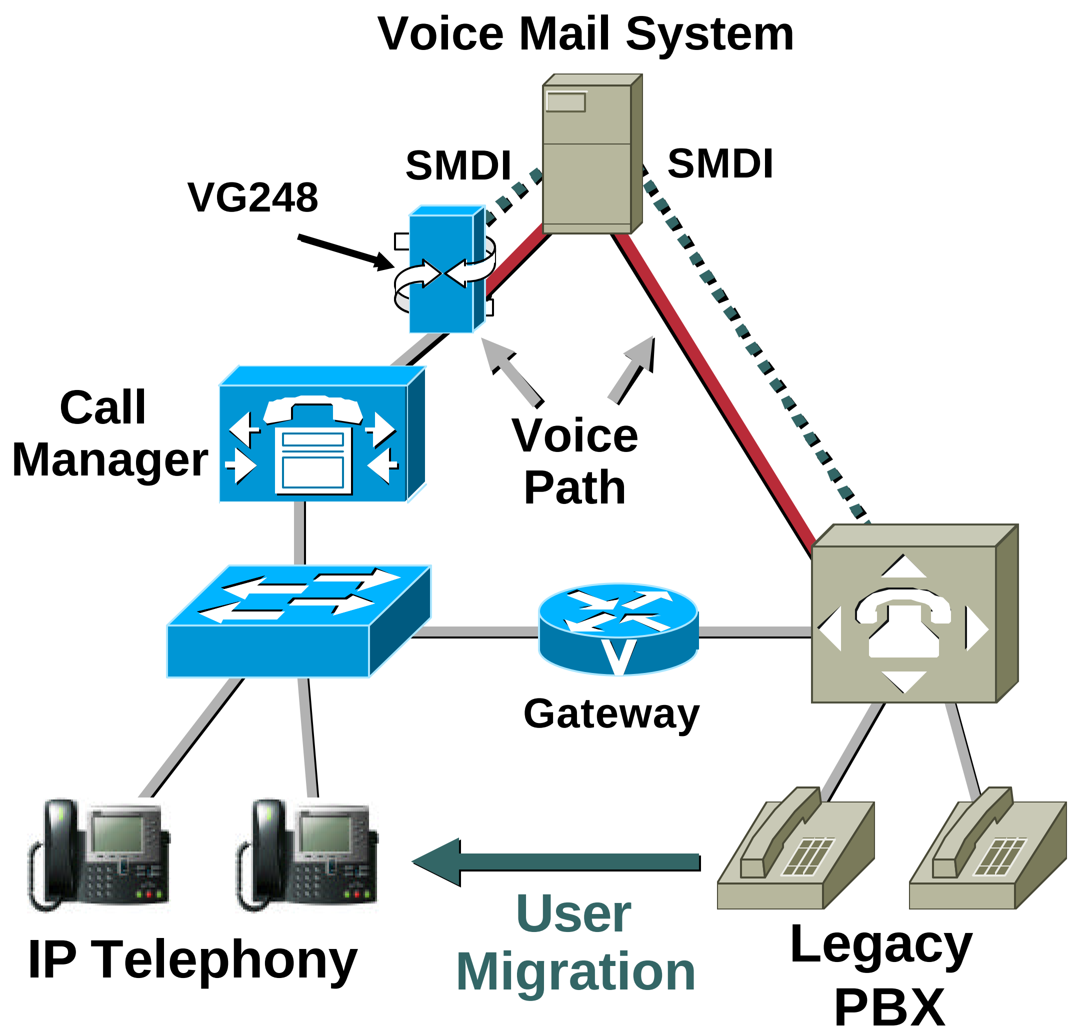
- **IF PBX-Voice Mail Integration Is Done through Proprietary Interface:**

IP Phones Do Not Have Transparent Voice Mail

Slow Migrations
Dual SMDI Integration from Voice Mail System

Supported
Voice Mail Systems:
Avaya Octel 250/350
Avaya Intuity

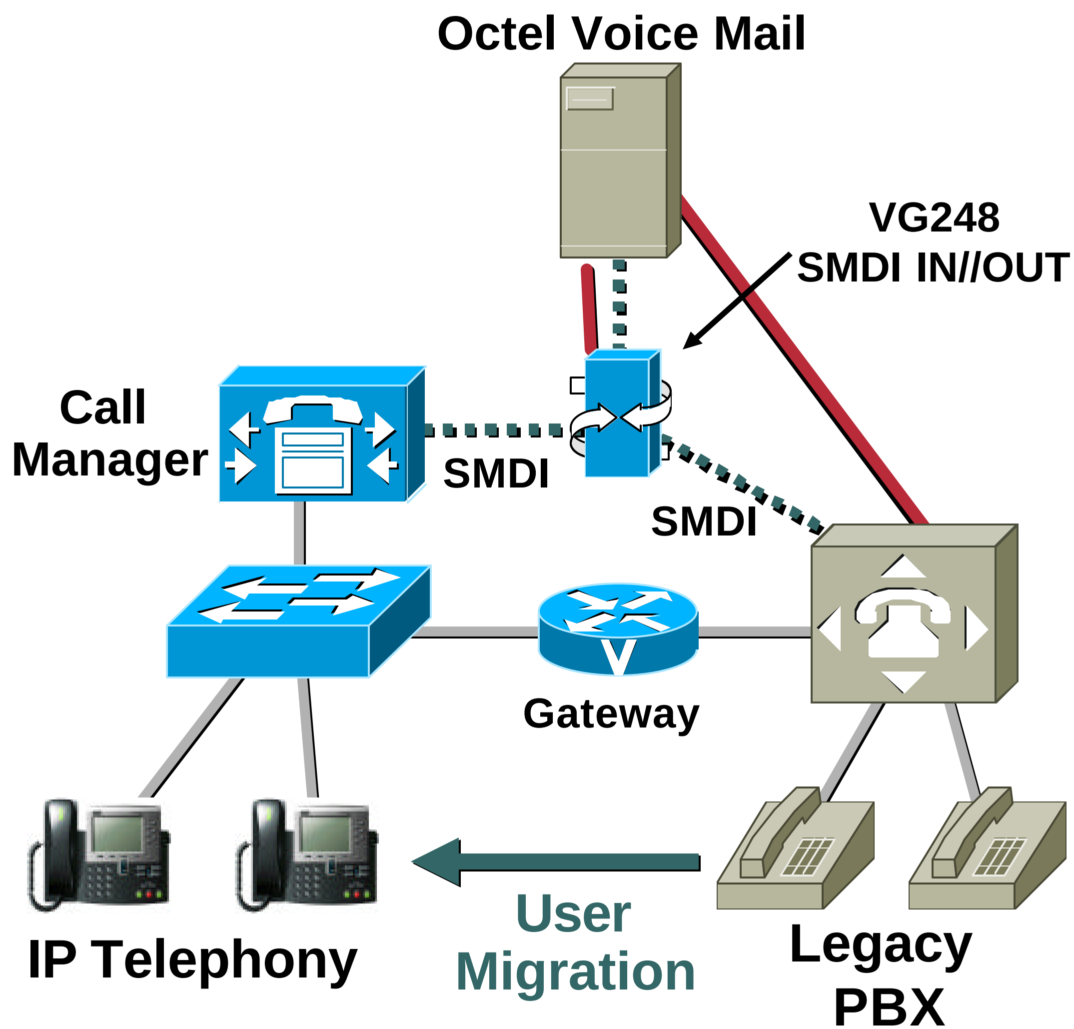
NOTE:
Assumes PBX
– VM integration
via analog/SMDI



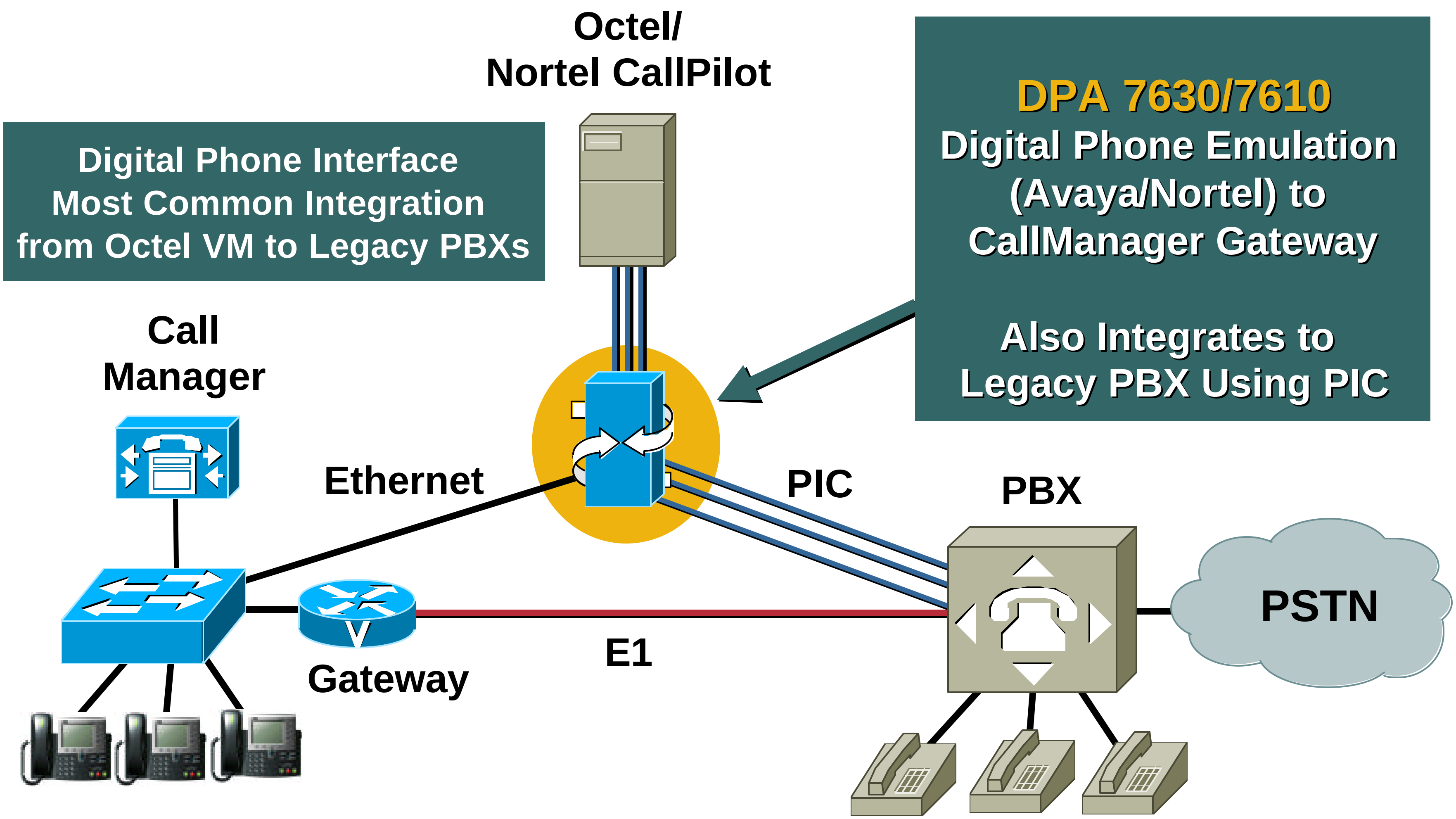
Slow Migrations
Single SMDI Integration from Voice Mail System

Needed if only Single SMDI RS-232 Supported on Voice Mail Systems:
Avaya Octel 200/300
Siemens Phone Mail
or if serial ports unavailable

NOTE:
Assumes PBX – VM integration via analog/SMDI

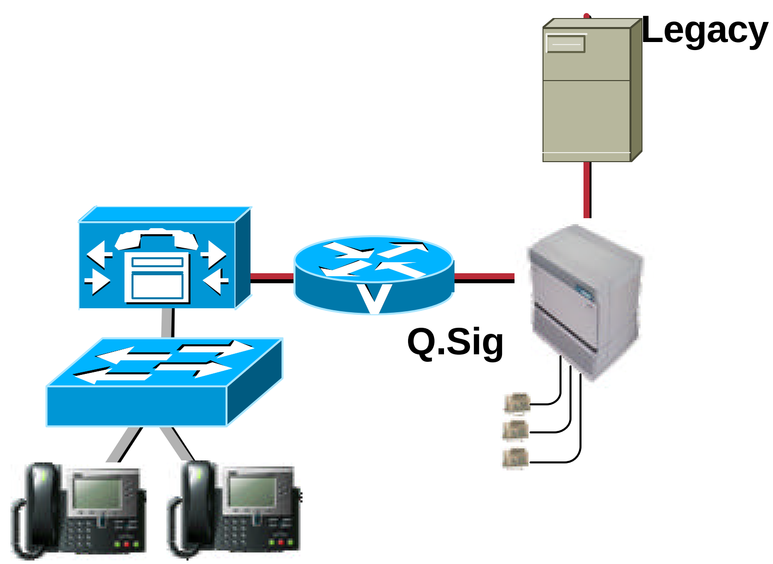


Slow Migrations
CallManager-Octel-PBX Integration via DPA



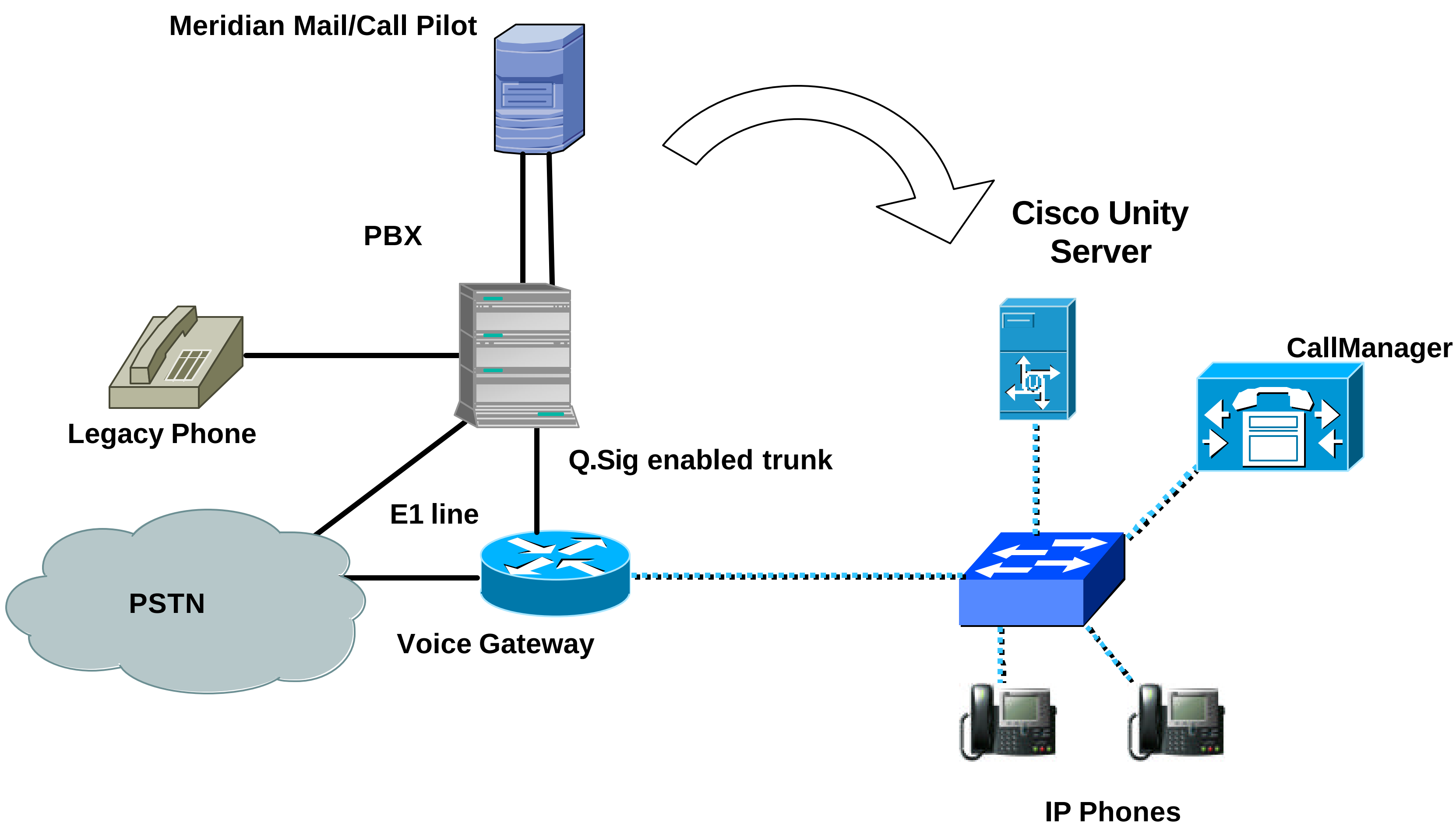
Slow Migrations: Cisco IP phones share other voicemail system

- Some voicemail systems do not support SMDI or digital emulation or are embedded in PBX (eg. Meridian Mail)
- Q.Sig allows IP phones to work with legacy VM



Slow Migrations: Legacy VM end of life, flash cut users to new VM/UM, migrate phones over time

Cisco.com

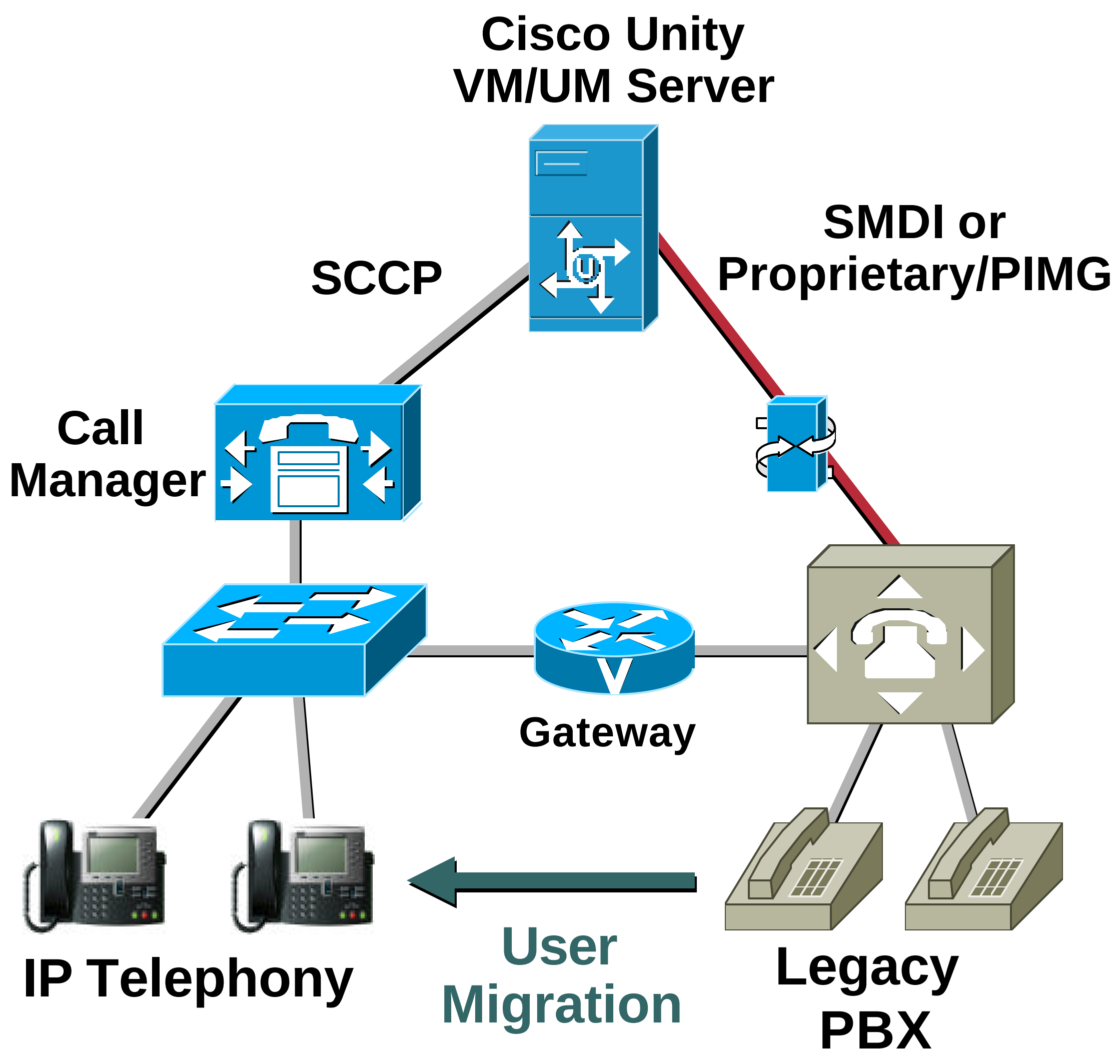


Slow Migrations
Dual Integration with Cisco Unity

Cisco.com

PBX Prerequisites:
SMDI Support
or
Lucent/Avaya *
Nortel *
NEC *…

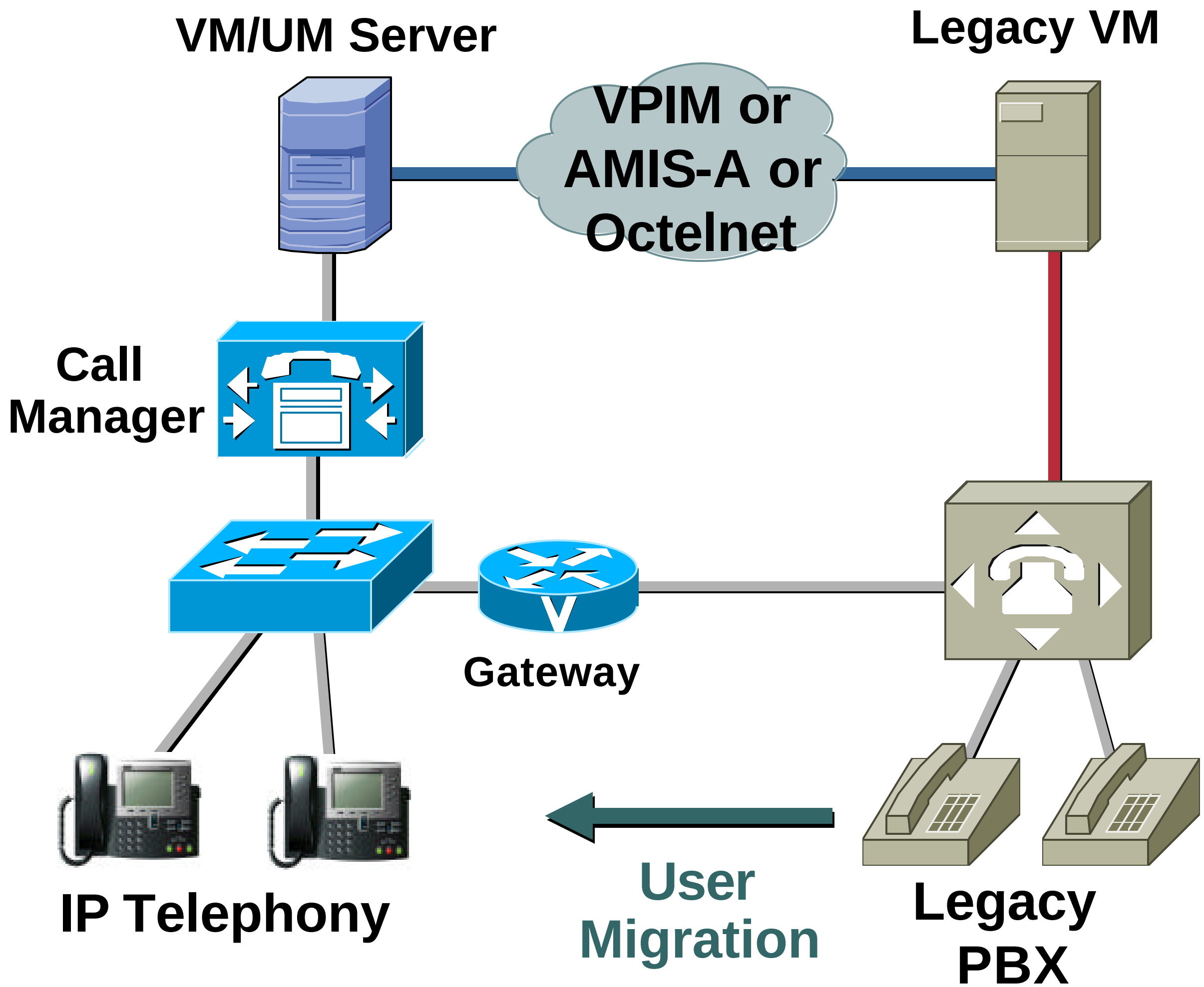
*** NOTE:**
Cisco Unity supports several proprietary PBX interfaces



Slow Migrations
Voice Mail Networking (No SMDI on Legacy VM)

Cisco.com

NOTE:
Depends on VM Support of a Common Networking Protocol (VPIM or AMIS-A)



Agenda

- **Flash Cut Migrations**

  Pull the Band-Aid off Fast

- **Slow Migrations ("Shrink and Grow")**

  Pull the Band-Aid off Slow

- **Integration Matrices**

Integration Matrices
PBX Integration (Across All Platforms)

Cisco.com

	Analog	H.323 PRI	MGCP PRI	Q.SIG PRI
Avaya Definity G3	Yes	Yes	Yes	Yes
Nortel Meridian 1	Yes	Yes	Yes	Yes
Siemens Hicom 300 E	Yes	Yes	Yes	Yes
Ericsson MD110	Yes	Yes	Yes	Yes
Alcatel 4400	Yes	Yes	Yes	Yes
Intertel Keysystem	Yes	Yes	Yes	N/A
Fujitsu F9600ES	Yes	Yes	Yes	Future
NEC 2400	Yes	Yes	Yes	Yes

Integration Matrices
Voice Mail Integration

Cisco.com

	SMDI	Dual SMDI Support	VPIM Support	Cisco DPA
Avaya Octel 250/350	Yes	Yes	No	Yes
Avaya Octel 200/300	Yes	No	No	Yes
Avaya Intuity	Yes	No	No	No
Nortel CallPilot	Yes	No	Yes	Yes
Siemens PhoneMail	Yes	No	No	No
AVT/Captaris	Yes	No	Yes	No
Interactive Intelligence	Yes	Yes	No	No
Lyrix	Yes	Yes	No	No

Summary

- What are the key components and requirements of an IP telephony solution
- How to build it:
  - Network infrastructure
  - Telephony infrastructure
  - Applications
- What are the design guidelines and recommendations

Conclusions

- IP Telephony is mainstream technology
- Key advantages are cost, flexibility and applications
- To learn more about IP Telephony design:

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

Recommended Reading

- **Cisco CallManager Fundamentals**

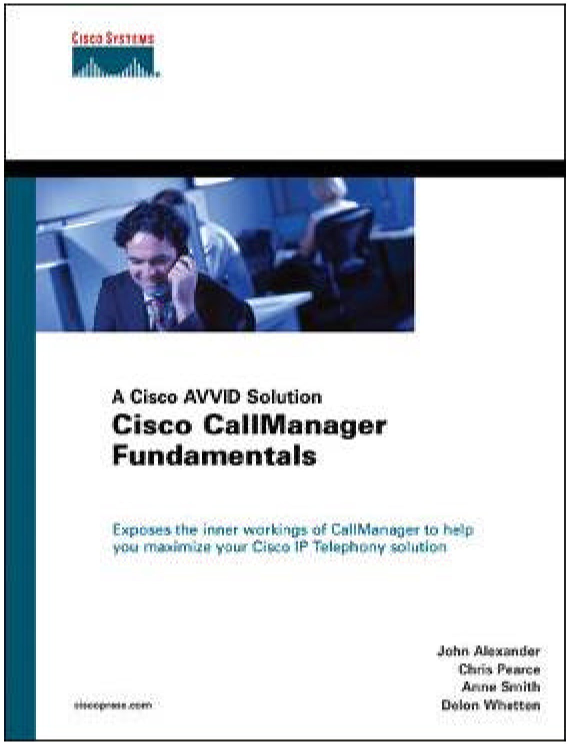
  ISBN: 1587050080

- **Voice-Enabling the Data Network: H.323, MGCP, SIP, QoS, SLAs, and Security**

  ISBN: 1587050145

- **Voice over IP Fundamentals**

  ISBN: 1578701686



Available Onsite at the Cisco Company Store

Recommended Reading

Cisco.com

- **Cisco IP Telephony**

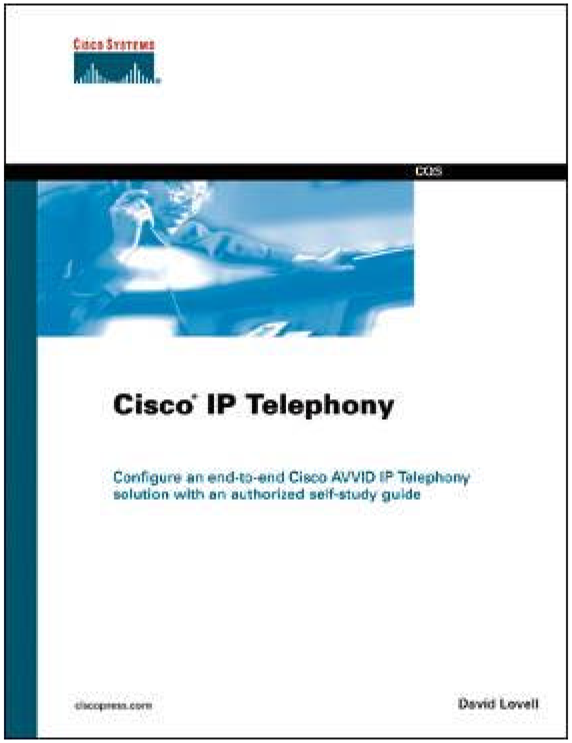
  ISBN: 1587050501

- **Cisco Voice over Frame Relay, ATM, and IP**

  ISBN: 1578702275

- **IP Telephony Unveiled**

  ISBN: 1587200759



Available Onsite at the Cisco Company Store

Complete Your Session Evaluation Form

Muchas Gracias por asistir a esta sesión.

Por favor, complete y entregue a la salida la evaluación suministrada.

¡Gracias!